The Purpose and Use of NIST

BY: RAELYN JORDAN
PRINCIPLES OF CYBERSECURITY

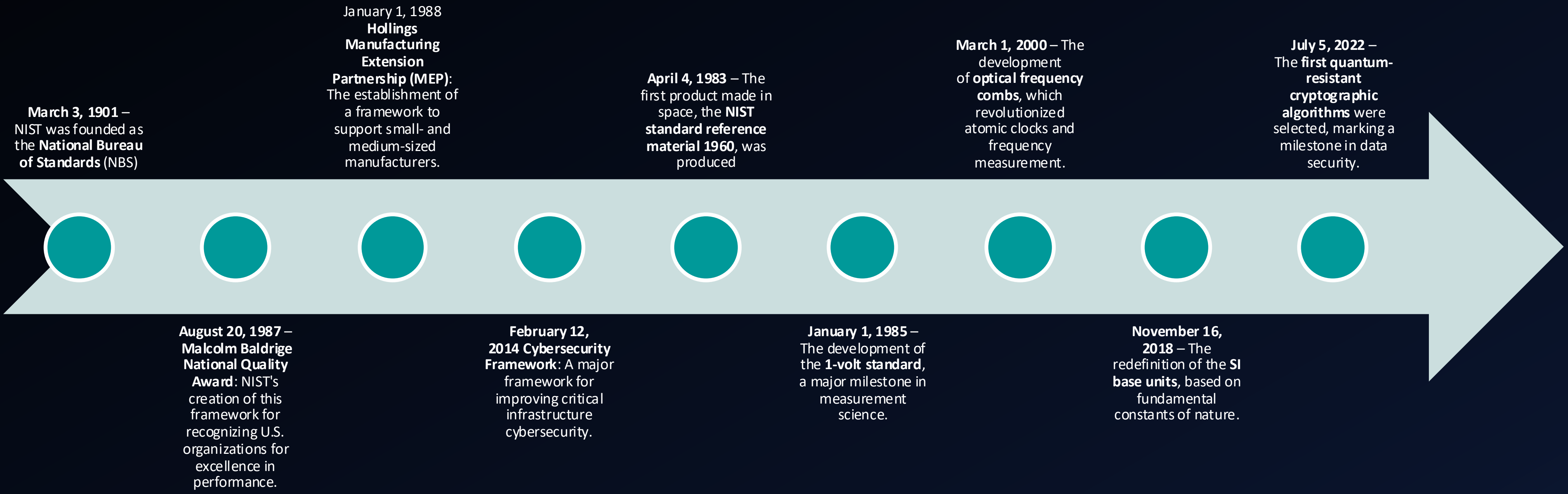
National Institute of Standards and Technology

- Founded in 1901, now part of the U.S. Department of Commerce
- Originally created to improve U.S. competitiveness through better measurement standards
- Impacts industries like tech, healthcare, and construction
- Many organizations are are at risk and their systems need protection, NIST plays a key role by providing trusted guidelines for cybersecurity (National Institute of Standards and Technology, n.d.).

What is NIST?

- Provides guidelines and standards for technology related matters and how to safely protect against vulnerabilities
- NIST mission is to support U.S. innovation and improve the quality of life (National Institute of Standards and Technology, n.d.).

NIST Timeline



March 3, 1901 – NIST was founded as the **National Bureau of Standards** (NBS)

August 20, 1987 – Malcolm Baldrige National Quality Award: NIST's creation of this framework for recognizing U.S. organizations for excellence in performance.

January 1, 1988 **Hollings Manufacturing Extension Partnership (MEP)**: The establishment of a framework to support small- and medium-sized manufacturers.

February 12, 2014 Cybersecurity Framework: A major framework for improving critical infrastructure cybersecurity.

April 4, 1983 – The first product made in space, the **NIST standard reference material 1960**, was produced

January 1, 1985 – The development of the **1-volt standard**, a major milestone in measurement science.

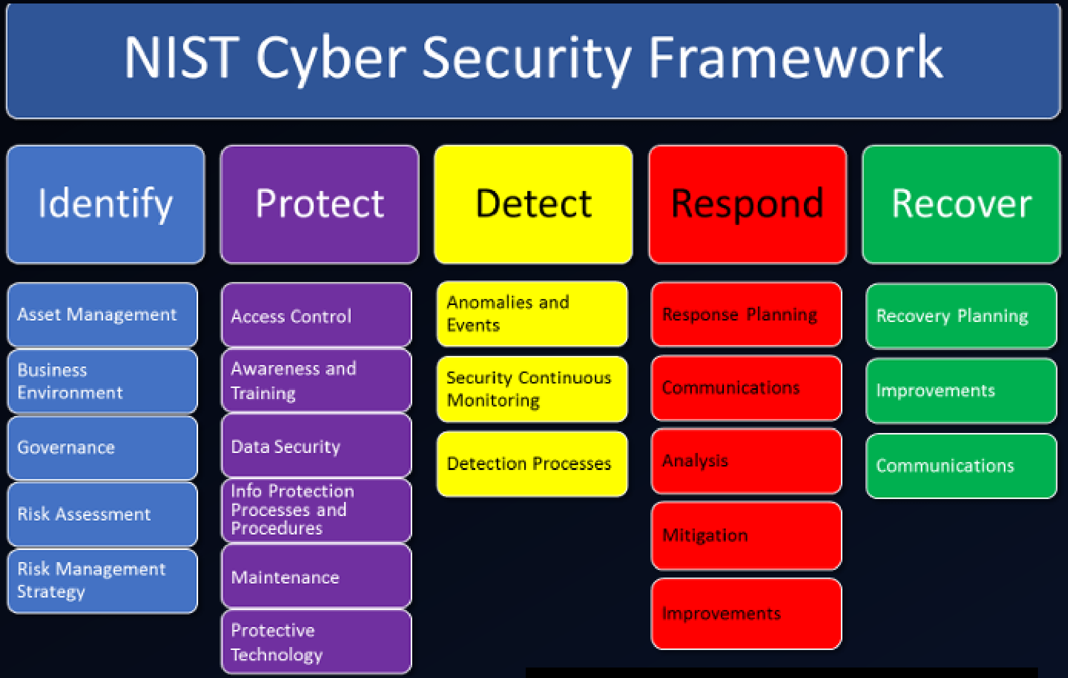
March 1, 2000 – The development of **optical frequency combs**, which revolutionized atomic clocks and frequency measurement.

November 16, 2018 – The redefinition of the **SI base units**, based on fundamental constants of nature.

July 5, 2022 – The **first quantum-resistant cryptographic algorithms** were selected, marking a milestone in data security.

NIST CYBERSECURITY FRAMEWORK

NIST provides a flexible outline of best practices and guides where to focus resources *(Federal Trade Commission, n.d.)*.



NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

- Identify – understand what you need to protect ie: equipment software, data
- Protect – Secure your systems, control access, and protect sensitive data
- Detect – Monitor for threats and unauthorized activity
- Respond– Have a plan in place to respond to and recover from attacks
- Recover – Restore operations and keep proper patrons informed

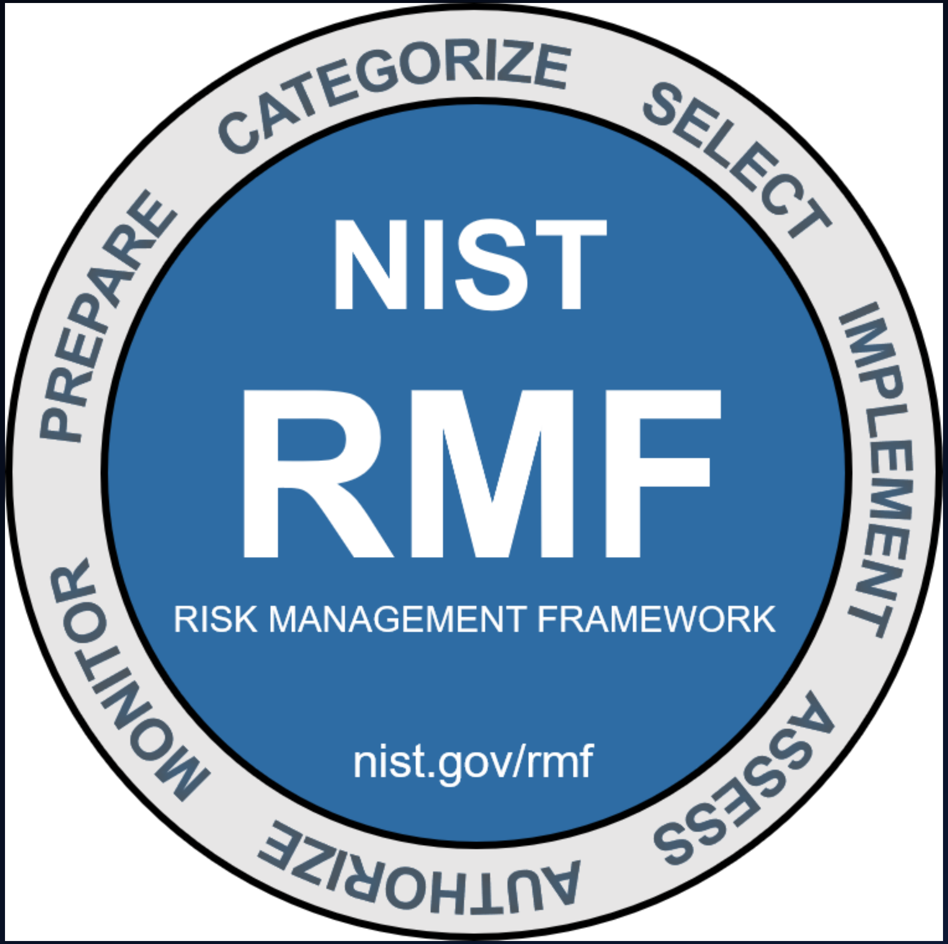
NIST and Risk Management

- The Risk Management Framework (RMF) is a flexible, risk-based approach that integrates security, privacy, and cyber supply chain risk management into the system development life cycle *(National Institute of Standards and Technology, n.d.)*.

The RMF process include 7 steps:

1. **Prepare** the organization to manage security and privacy risks
2. **Categorize** the system and its data based on impact
3. **Select** controls from NIST SP 800-53 to protect the system
4. **Implement** controls and document how they're deployed
5. **Assess** controls to ensure they're effective and operating as intended
6. **Authorize** the system for operation based on risk
7. **Monitor** continuously to track risks and control effectiveness

The RMF applies to both new and legacy systems, across all organizations, regardless of size.



IMPLEMENTING NIST FRAMEWORKS

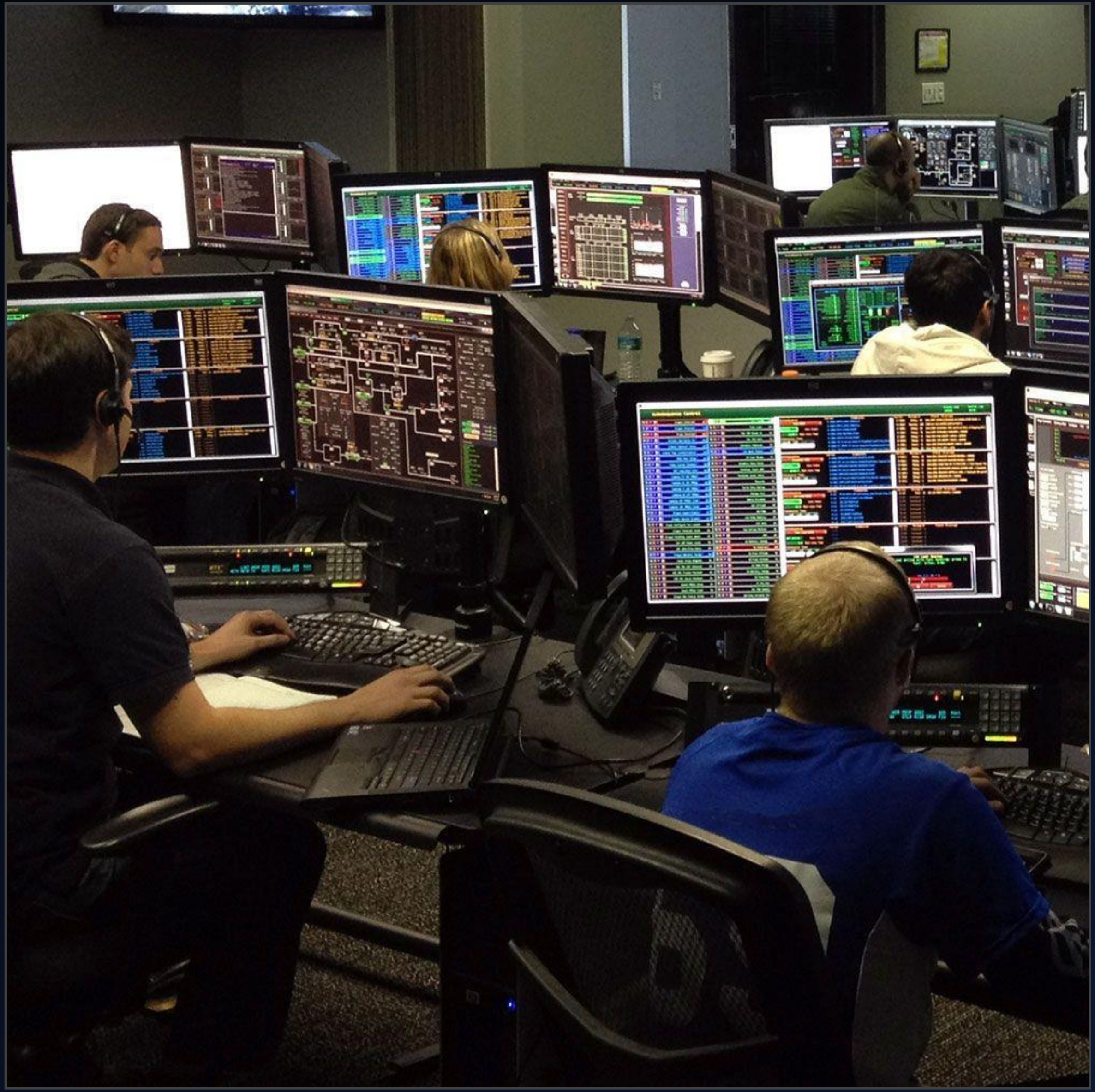
NIST frameworks, such as the RMF, have been adopted by many businesses and organizations for security, privacy, and risk management purposes. Here are some key examples showing the use of NIST:

- Federal Agencies: Agencies have undertaken RMF compliance to certify the cybersecurity of federal IT assets.
- Private Sector: Corporations use NIST Standards for the protection of classified information like cyber security and encrypting.
- Critical Infrastructure: NIST frameworks help in the defense of infrastructure of any nation from cyber-attacks.

Real-World Examples:

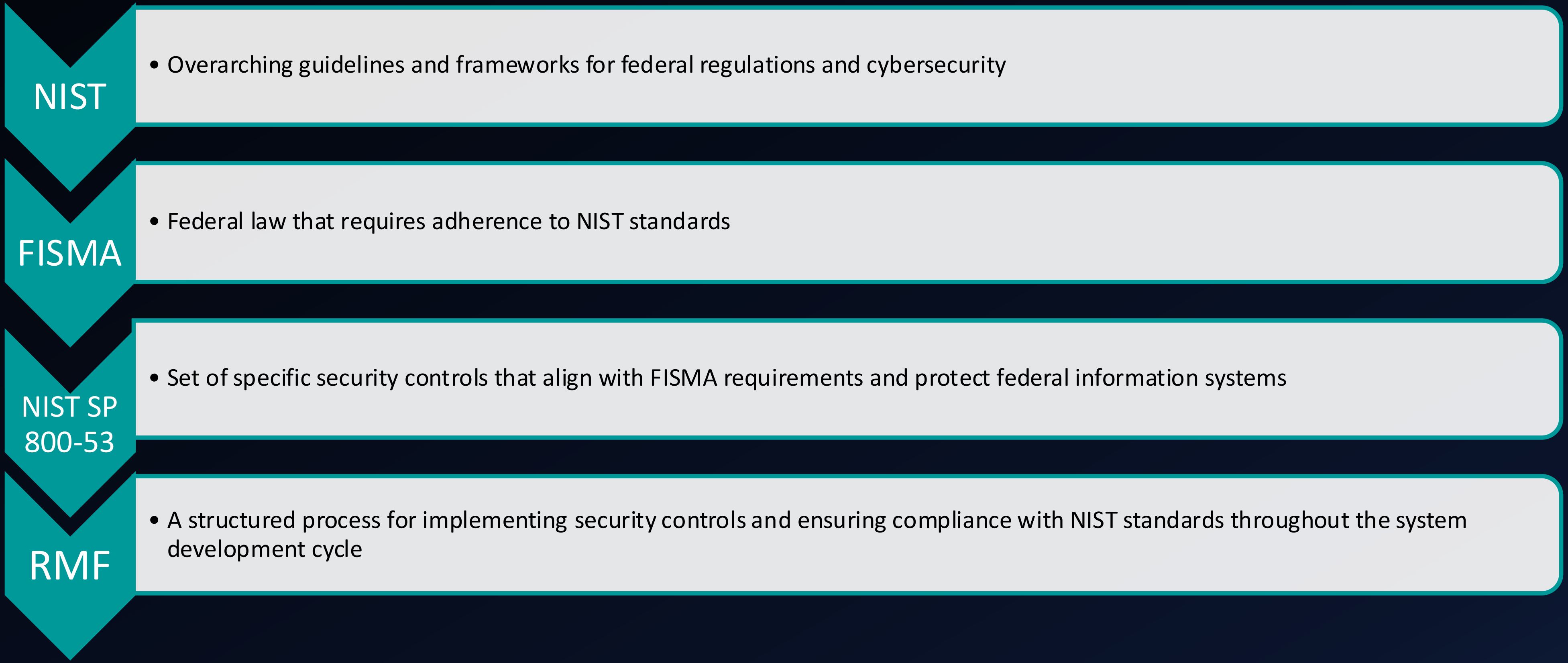
- The Cybersecurity Framework (NIST CSF) is used throughout the private and public sectors.
- Supply Chain Risk Management (SCRM) frameworks aid firms in mitigating the risks associated with third-party vendors.

Outcome: Uniformity, confidence, and effective risk mitigation are achieved at all levels due to the NIST standards.



NIST and Federal Regulations

NIST'S GUIDELINES AND FRAMEWORKS ALIGN WITH FEDERAL CYBERSECURITY REGULATIONS AND STANDARDS TO ENSURE THE PROTECTION OF THE FEDERAL GOVERNMENT



NIST
- Overarching guidelines and frameworks for federal regulations and cybersecurity

FISMA
- Federal law that requires adherence to NIST standards

NIST SP 800-53
- Set of specific security controls that align with FISMA requirements and protect federal information systems

RMF
- A structured process for implementing security controls and ensuring compliance with NIST standards throughout the system development cycle

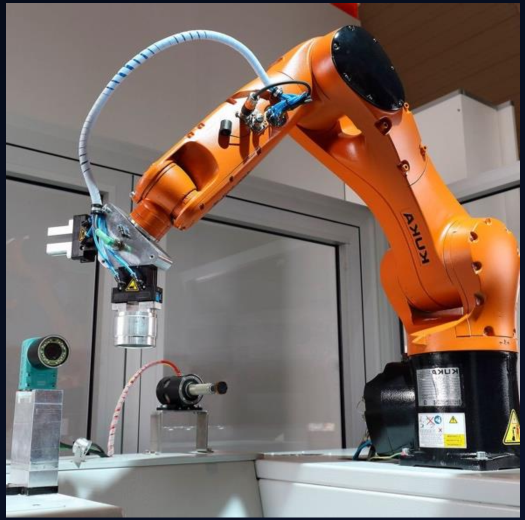
NIST’S Impact of Industry

Healthcare

NIST impacts healthcare by assisting with HIPPA compliance. It also secures electronic health records against cyber threats.

It helps financial institutes meet GLBA compliance and protects sensitive data using the Cybersecurity Framework

Manufacturing



Ensures cybersecurity resilience in operational technology and protects critical infrastructure with NIST’s Cybersecurity Framework and Risk Management Framework

NIST’s Global Influence

- NIST works with a select group of foreign partners through Standards Developing Organizations (SDOs) to help develop and interrelate cybersecurity frameworks worldwide.

- NIST takes part in global initiatives, including the RSA Conference, Israel Cyber Week, International Cybersecurity Challenge (ICC), and many other activities with Brazil for the cooperation and exchange of information in cybersecurity.

- NIST Cybersecurity Framework (CSF), Privacy Framework, and Workforce Framework are well accepted the world over, having been translated into several languages, thus promoting global cybersecurity harmony (National Institute of Standards and Technology, 2025).

- NIST’s works enhances and enables the development of other international standards with other collaborators such as ISO, ENISA, and APEC.

BENEFITS OF NIST FRAMEWORK

- Enhanced Cybersecurity Posture: Boosts protection and resiliency at the same time to contending cybersecurity innovations constraints.
- More Effective Risk Control: Helps organizations identify and prioritize cybersecurity risks.
- Cultivated Communication and Collaboration: Provides a common language for cybersecurity discussions.
- Regulatory Compliance: Aids in meeting specified regulatory expectations.
- Flexibility : Adjusts for the different organizational or overall company's needs.
- Trust and Reputation: Increases business goodwill and builds trust with customers and business partners.
- Business Survival: Guarantees survival or recoverability of an organization after events of incidents.
- Improved efficiency: Reduces mitigation expenses incurred from expensive cyber attacks and their consequences(AuditPeak, n.d.)

CHALLENGES OF IMPLEMENTING NIST

- Limited Resources
  - Small businesses tend to have issues in relation to time, money, and human resource investments.
- Technical Challenges
  - In the absence of proper infrastructure, applying the framework can be overwhelming.
- Resistance to Change
  - New processes and/or additional tasks can lead to employee resistance.
- Insufficient Internal Capabilities
  - Inability to comprehend and apply the framework may arise due to insufficient in-house expertise.
- Evolving Threats
  - The development of cyber threats occur at a faster pace and thus, constant updates are essential.

Overcoming Challenges:

Practitioners have largely acknowledged that addressing these difficulties would involve a commitment towards management, staff professional development, gaining expertise from outside the organization and making continual updates in order to accommodate the framework and the changes in the field of cybersecurity (AuditPeak, n.d.).

Conclusion

- NIST's Role in Cybersecurity
  - NIST furnishes a comprehensive framework for the governance and mitigation of cybersecurity risks.
- Key Benefits
  - Strengthens increased risks posture, improves risk processes, and promotes collaboration at the same time.
- Challenges
  - Achieving implementation is not easy but achieving it will result in security benefits in the longer run.
- Final Thought
  - Allows an organization’s continued ease of operations while persistently guarding against new cyber threats and vulnerabilities.

References

Computer Security Division, I. T. L. (2025, January 29). *About the RMF - NIST risk management framework: CSRC*. CSRC. https://csrc.nist.gov/projects/risk-management/about-rmf

Mahn, A. (2022, September 6). *NIST's expanding international engagement on Cybersecurity*. NIST. https://www.nist.gov/blogs/cybersecurity-insights/nists-expanding-international-engagement-cybersecurity

National Institute of Standards and Technology (NIST). (1901, March 3). *NIST timeline*. NIST. https://www.nist.gov/timelinelist

National Institute of Standards and Technology (NIST). (2022, January 11). *About Nist*. NIST. https://www.nist.gov/about-nist

Nguyen, S. T. (2022, October 6). *Understanding the NIST cybersecurity framework*. Federal Trade Commission. https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework

Peak, A. (2024, December 20). *Benefits and challenges in implementing NIST CSF*. Audit Peak | Cybersecurity & Advisory Services. https://www.auditpeak.com/challenges-in-implementing-nist-csf/