Survey of the NIST Framework
Part 1 of 2



Speakers:

Eric Adams, CISO/SVP, MX

Dheeraj Gurugubelli, Senior Director, EY-Parthenon

(c) 2022 Lexeprint Inc. All Rights Reserved.

Disclaimer



This is not legal advice, nor should it be considered legal advice.



This presentation and the comments contained therein represent only the personal views of the participants, and do not reflect those of their employers or clients.



This presentation is offered for educational and informational uses only.

(c) 2022 Lexeprint Inc. All Rights Reserved.

Speakers



Eric Adams
CISO/SVP
MX



Dheeraj Gurugubelli
Senior Director
EY-Parthenon

(c) 2022 Lexeprint Inc. All Rights Reserved

Agenda

- National Institute of Standards and Technology Cybersecurity (NIST) Framework
- Part 1: NIST Cybersecurity Framework Core
- Part 2: NIST Cybersecurity Framework Implementation Tiers

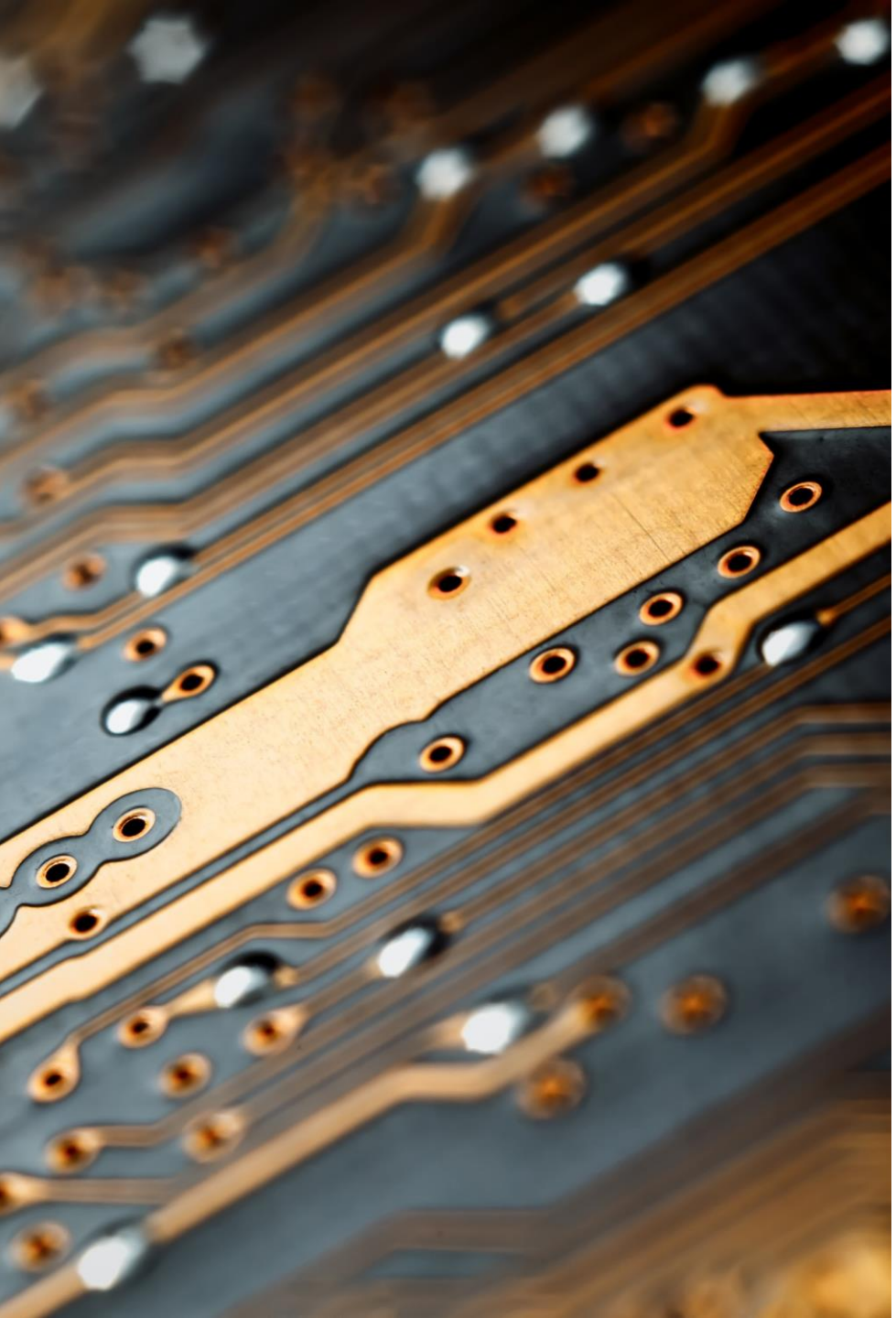
(c) 2022 Lexeprint Inc. All Rights Reserved.



National Institute of Standards and Technology Cybersecurity Framework

(c) 2022 Lexeprint Inc. All Rights Reserved.

This Photo by Unknown Author is licensed under CC BY-ND



What is NIST?

- The National Institute of Standards and Technology (NIST) is a non-regulatory government agency founded in 1901 to "promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology" to enhance American economic security.*
- Officially, NIST functions as a network of laboratories in various technology and science sectors but, today, one of NISTs core missions is to implement practical cybersecurity and privacy standards.

Source: *https://www.nist.gov/about-nist*

(c) 2022 Lexeprint Inc. All Rights Reserved.



What is NIST? (cont.)

- As part of this effort, NIST is responsible for producing guidelines and standards to help federal agencies comply with the Federal Information Security Management Act (FISMA).
- One of the most widely adopted NIST standards is the NIST Cybersecurity Framework for Critical Infrastructure, a framework designed for federal agencies and programs to protect critical data and manage cybersecurity.

(c) 2022 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-SA-NC

History of NIST Cybersecurity Framework

- In February 2013, President Obama issued EO 13636, *Improving Critical Infrastructure Cybersecurity.*
- The EO established the "policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity."*
- As such, the order called on NIST to develop a voluntary risk-based set of industry standards to help organizations identify, assess, and manage cybersecurity risks.

** Executive Order 13636, Improving Critical Infrastructure Cybersecurity*

(c) 2022 Lexeprint Inc. All Rights Reserved.



History of NIST Cybersecurity Framework

- The EO directed NIST to work with industry leaders to develop the Framework --- leading to a year-long, collaborative process in which NIST served as a convener for industry, academia, and government stakeholders.
- As a result, the NIST Cybersecurity Framework was released in early 2014.

(c) 2022 Lexeprint Inc. All Rights Reserved.



What is the NIST Cybersecurity Framework?

- The Framework outlines a set of risk-based guidelines to help organizations "identify, implement and improve" cybersecurity practices.*
- Rather than introducing new standards, the Framework integrates existing cybersecurity practices developed by organizations like NIST and the International Standardization Organization (ISO) to create a comprehensive guide.

*Source: https://www.ftc.gov/business-guidance/blog/2016/08/nist-cybersecurity-framework-and-ftc

(c) 2022 Lexeprint Inc. All Rights Reserved.



NIST is Voluntary Not Required

It is important to note that the Framework is a *voluntary guidance.*

(c) 2022 Lexeprint Inc. All Rights Reserved.

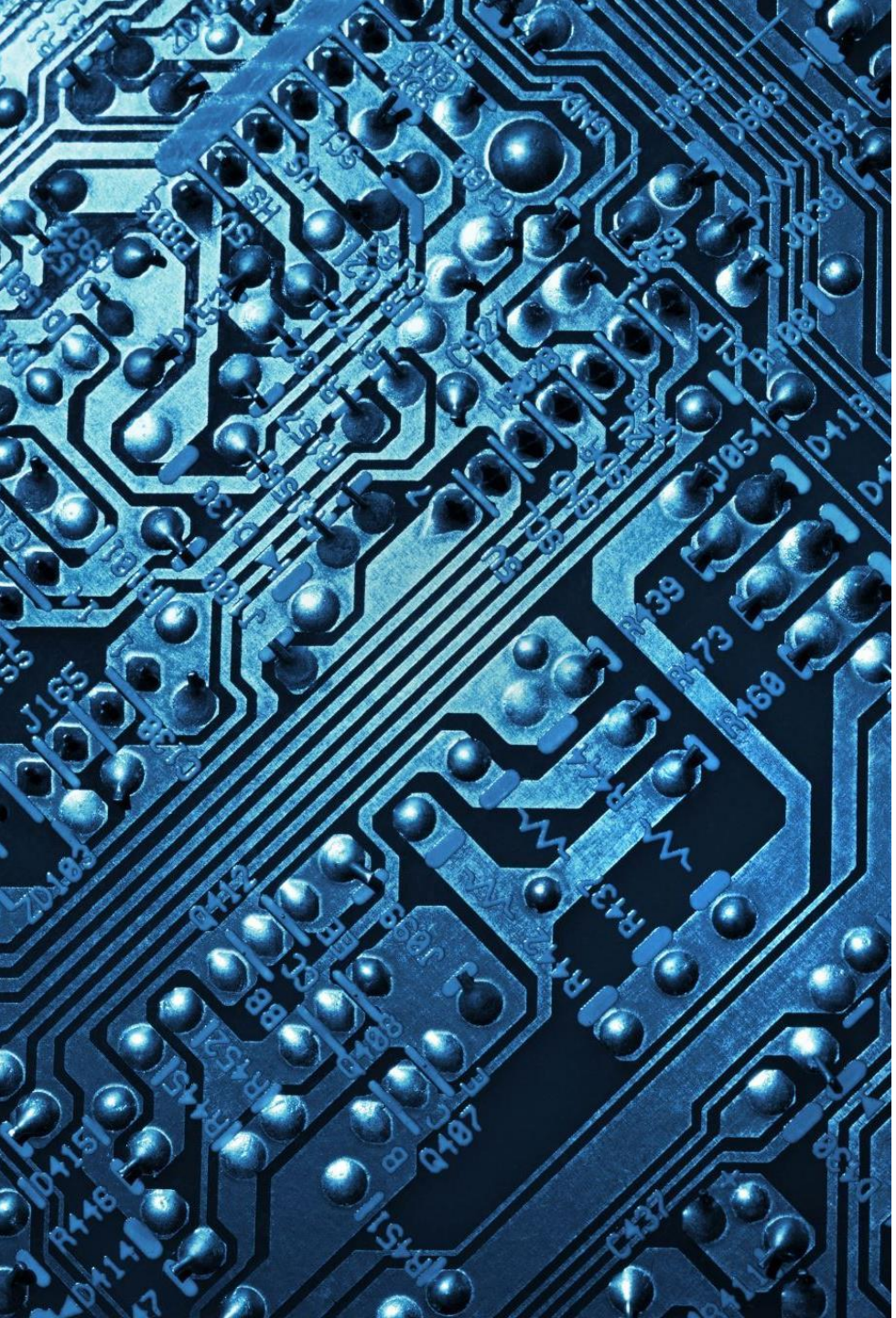


Who uses the NIST Framework?

- The Framework was designed specifically for companies classified as part of the U.S. critical infrastructure; however, many other private and public sector organizations use the Framework as cybersecurity guidance.
- Critical infrastructure, for the purposes of this Framework is defined in Presidential Policy Directive 21 as "systems and assets so vital to the United States that the incapacity or destruction of such would have a debilitating impact on security, national economic security or national public health or safety". *
    - Examples: utilities providing energy and water, transportation, financial services, communications, healthcare and public health, food and agriculture, etc...

* *Presidential Policy Directive 21 (2013)*

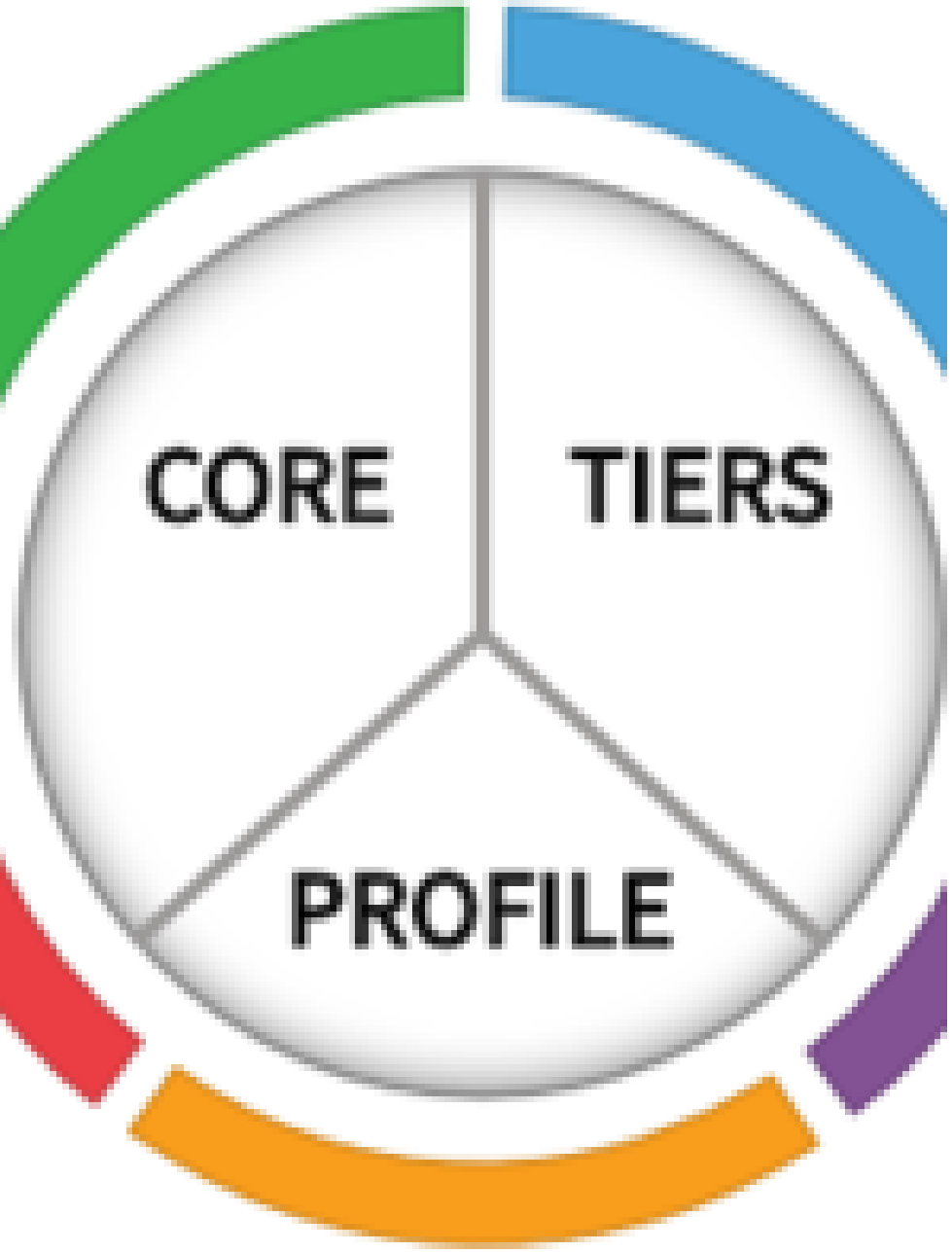
(c) 2022 Lexeprint Inc. All Rights Reserved.



What are the Benefits of the Framework?

- Adhering to the Framework provides an organization with guidelines to:
  - Better understanding of its cybersecurity risks;
  - Determine which cyber-activities are most important to assure critical operations to help with prioritizing investments and reducing cost; and
  - Standardize a "common language" to address cybersecurity risk management to enhance an organization's internal and external communication.

(c) 2022 Lexeprint Inc. All Rights Reserved.



What is the Structure of the Framework?

- The Cybersecurity Framework consists of three main components:
  - (1) The Framework Core
  - (2) Implementation Tiers
  - (3) Profiles

Image taken from https://www.nist.gov/cyberframework/online-learning/components-framework)

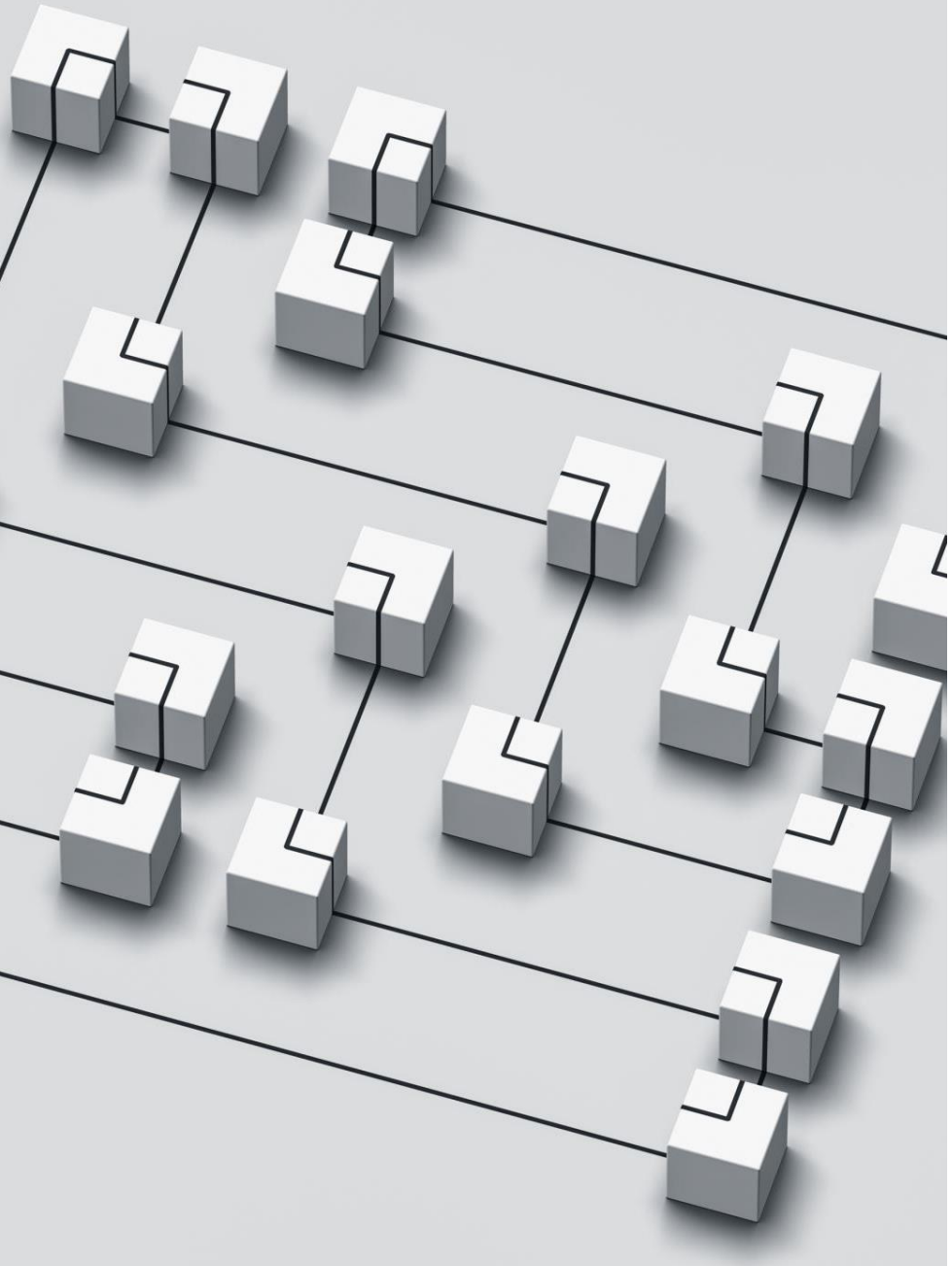
(c) 2022 Lexeprint Inc. All Rights Reserved.



Part 1: NIST Cybersecurity Framework Core

(c) 2022 Lexeprint Inc. All Rights Reserved.

This Photo by Unknown Author is licensed under CC BY-SA-NC



What is the Framework Core?

- The Framework Core is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors.
- The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities from the executive level to the implementation and operations level.

(c) 2022 Lexeprint Inc. All Rights Reserved.

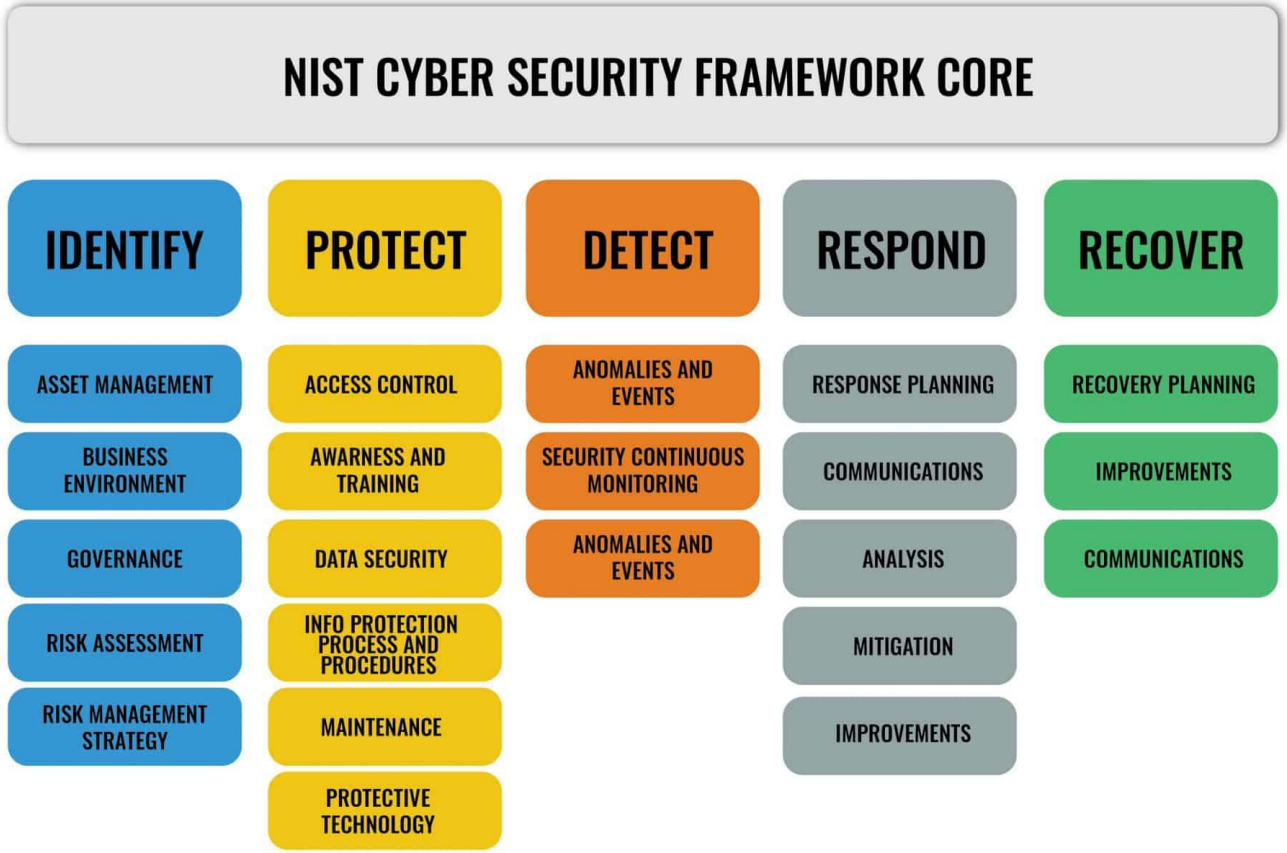
NIST Cybersecurity Framework Components

- The Core is separated into three parts:
  - Functions,
  - Categories, and
  - Subcategories.
- Within these parts, the Core includes 23 Categories across the five functions:
  - Identify,
  - Protect,
  - Detect,
  - Respond, and
  - Recover.

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

(c) 2022 Lexeprint Inc. All Rights Reserved.

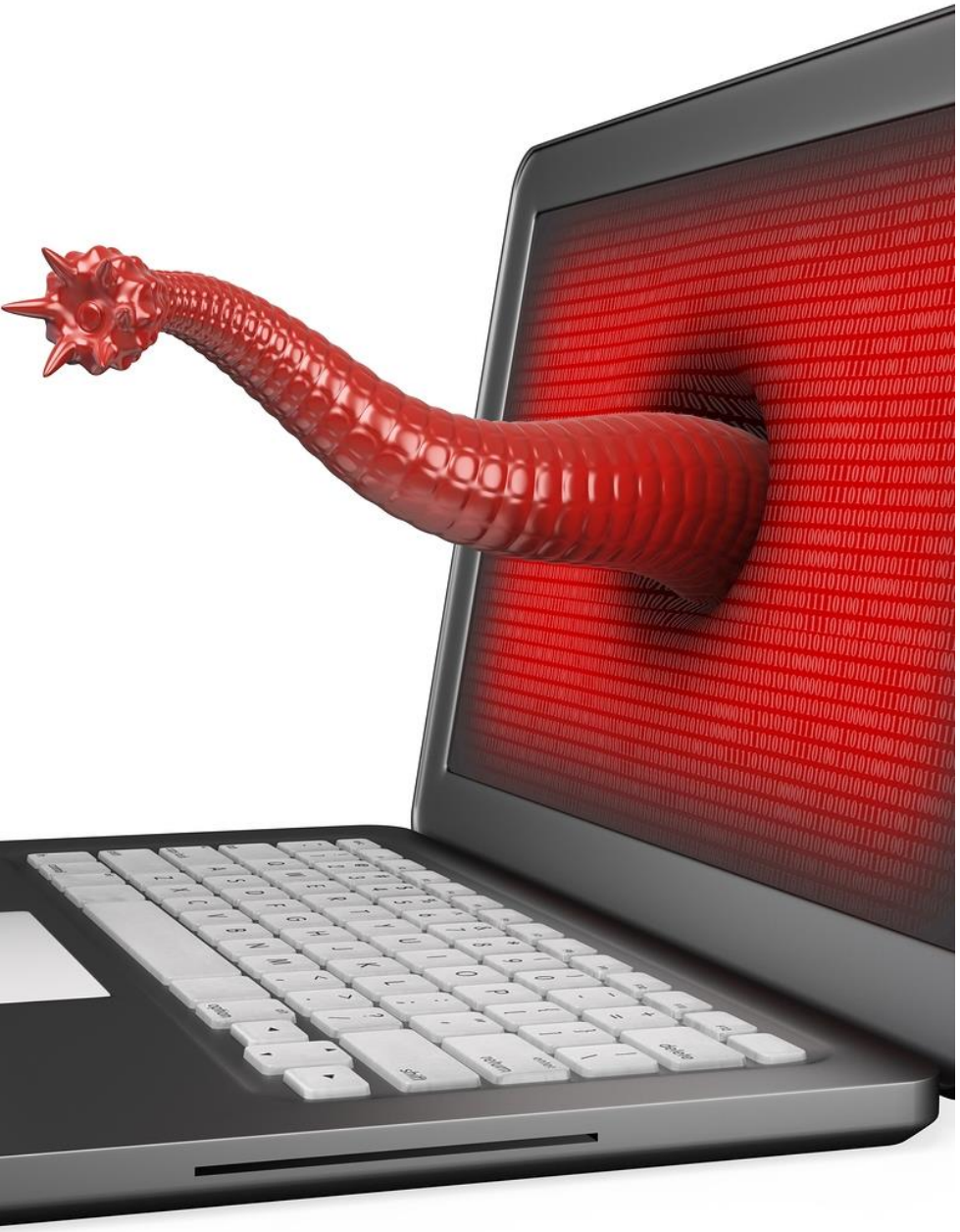
Framework Core



(c) 2022 Lexeprint Inc. All Rights Reserved.

Identify

Identify helps organizations gain an understanding of how to manage cybersecurity risks to systems, assets, data, and capabilities. This category focuses on identifying:



This Photo by Unknown Author is licensed under CC BY-SA-NC

Protect

- **Protect** helps organizations develop the controls and safeguards necessary to protect against or deter cybersecurity threats.
- This category focuses on:
  - Protecting for identity management and access control within the organization;
  - empowering staff through awareness and training; and
  - Establishing data security protection consistent with the organization's specific risk strategy.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Detect

- **Detect** are the steps organizations should consider taking to provide proactive and real-time alerts of cybersecurity-related events.
- This category focuses on:
  - Ensuring anomalies and events are detected and understood;
  - Implementing security continuous monitoring capabilities to verify the effectiveness of protective measures; and
  - Maintaining detection processes to provide awareness of anomalous events.

(c) 2022 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown Author is licensed under CC BY-SA-NC

Respond

- **Respond** helps organizations develop effective incident response activities.
- This category focuses on:
  - Ensuring response planning process are executed during *and* after an incident;
  - Managing communications during and after an event with stakeholders, law enforcement and external stakeholders;
  - Supporting forensic analysis strategies to support effective recovery activities; and
  - Performing mitigation activities that prevent the expansion of an event.

(c) 2022 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY

Recover

- **Recover** is the development of continuity plans so organizations can maintain resilience and return to normal operations after a breach.
- This category focuses on:
  - Ensuring the organization implements recovery planning procedures to restore affected systems;
  - Implementing improvements based on lessons learned and reviews of existing strategies; and
  - Coordinating internal and external communications during and following the recovery from a cybersecurity incident.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Part 2: NIST Cybersecurity Framework Implementation Tiers

(c) 2022 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown Author is licensed under CC BY-SA

What are Framework Implementation Tiers?

- Framework Tiers provide:
  - Context on how the organization views cybersecurity risk;
  - An overview of existing processes to manage that risk;
  - Characterization of cybersecurity practices on a 4 Tier scale, from Partial (Tier 1) to Adaptive (Tier 4); and
  - Higher tiers limit cybersecurity risk.
- Businesses can use the implementation tiers to see how their current cybersecurity risk management practices compare to the Framework's ideal standards.

(c) 2022 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-NC

Tier 1: Partial Implementation

- **Risk Management Process:**
  - Not formalized and risk is managed in a non-procedural and sometimes reactive manner.
- **Integrated Risk Management Program:**
  - Limited awareness of cybersecurity risk at the organizational level.
- **External Participation:**
  - The organization does not understand its role in the larger ecosystem about its dependencies or dependents.

(c) 2022 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown Author is licensed under CC BY-SA

Tier 2: Risk Informed

- **Risk Management Process:**
  - Risk management practices are approved by management but cannot be established as an organizational policy.
- **Integrated Risk Management Program:**
  - There is an awareness of cybersecurity risk at the organizational level, but a broad approach to managing this risk has not been established by the organization.
- **External Participation:**
  - Generally, the organization understands its role in the larger ecosystem about its own dependencies or dependents, but not to both.

(c) 2022 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-SA

Tier 3: Repeatable

- **Risk Management Process:**
  - The organization's risk management practices are formally approved and expressed as a policy.
- **Integrated Risk Management Program:**
  - There is an organization-wide approach to managing cybersecurity risks.
- **External Participation:**
  - The organization understands its role, dependencies, and dependents in the larger ecosystem and can contribute to a broader understanding of community risks.

(c) 2022 Lexeprint Inc. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-SA-NC

Tier 4: Adaptive

- **Risk Management Process:**
  - The organization adapts its cybersecurity practices based on past and current cybersecurity activities, including lessons learned and predictive indicators.
- **Integrated Risk Management Program:**
  - There is an organization-wide approach to managing cybersecurity risks that uses informed risk policies, processes, and procedures to address potential cybersecurity events.
- **External Participation:**
  - The organization understands its role, dependencies, and dependents in the larger ecosystem and contributes to a broader understanding of community risks.

(c) 2022 Lexeprint Inc. All Rights Reserved.



(c) 2022 Lexeprint Inc. All Rights Reserved.

Contact Us



Eric Adams
Email: eric2525@gmail.com



Dheeraj Gurugubelli
Email: dheerajsec5@gmail.com

(c) 2022 Lexeprint Inc. All Rights Reserved



Eric Adams
MX – CISO/SVP
Contact:
E: eric2525@gmail.com

Eric Adams is the Chief Information Security Officer (CISO) / SVP joining MX in 2021 in charge of security engineering and security compliance and privacy departments.

Before MX, Eric was previously the CISO / SVP for Kyriba from 2018 to 2021 responsible for security compliance certifications including SWIFT payments systems, SOC1&2, and ISO 27001 and also the overall security of the global SaaS-based treasury management application system and its related business functions.

Before Fintech, Eric successfully completed 20 years of security experience and specifically FedRAMP authorization experience in Federal cloud at HP. He also worked at IBM as a Federal cloud security strategist with Watson AI applications and Blockchain.

At HP, Eric built the first cloud security service approved for federal government use with a FedRAMP JAB authorization for government agencies with authority to operate (ATO) in the cloud. This originated from Eric taking an onsite customer request from a US DOD military customer for scanning using static code security analysis of code in the cloud, which after Eric led the building and Federal authorization now has over 60 US government customers. He was also instrumental in leading IBM to federal cloud authorizations as the federal cloud security strategist.

Eric is a graduate of the Huntsman School of Business at Utah State University and holds an MBA along with CISSP and CSSLP security certifications.

(c) 2022 Lexeprint Inc. All Rights Reserved.



Dheeraj Gurugubelli
EY-Parthenon - Senior Director
Contact:
E: dheerajsec5@gmail.com
URL: https://www.linkedin.com/in/dheerajguru/

Dheeraj (DJ) Gurugubelli is a Senior Director in EY's Transaction Strategy & Execution Group. He is a M&A cybersecurity expert and advises several Fortune 500 and private equity clients on cybersecurity strategy, risk, and security transformation across the capital agenda.

In the past two years, Dheeraj has led more than 200 cybersecurity and data privacy assessments for M&A targets of varying scale globally. He leads a cybersecurity and data privacy team focused on the strategic application of security in the context of capital transactions, including mergers, acquisitions, and divestitures.

He has experience evaluating and transforming security programs for a range of companies including Tier 1 banks, healthcare providers, Fintech's, tele-health, EduTech, smart supply chains, EV charging networks, airliners, gaming, IoT manufacturers, and AI/ML driven data intensive platforms.

Prior to EY, Dheeraj served as a trusted advisor for many Fortune 500 companies on topics spanning cyber risk management, strategy, tactical security operations, and incident response. He served as a security research scholar at Purdue University's Cyber Forensics Lab and has regularly contributed to several publications related to critical infrastructure security.