NIST Cybersecurity Framework

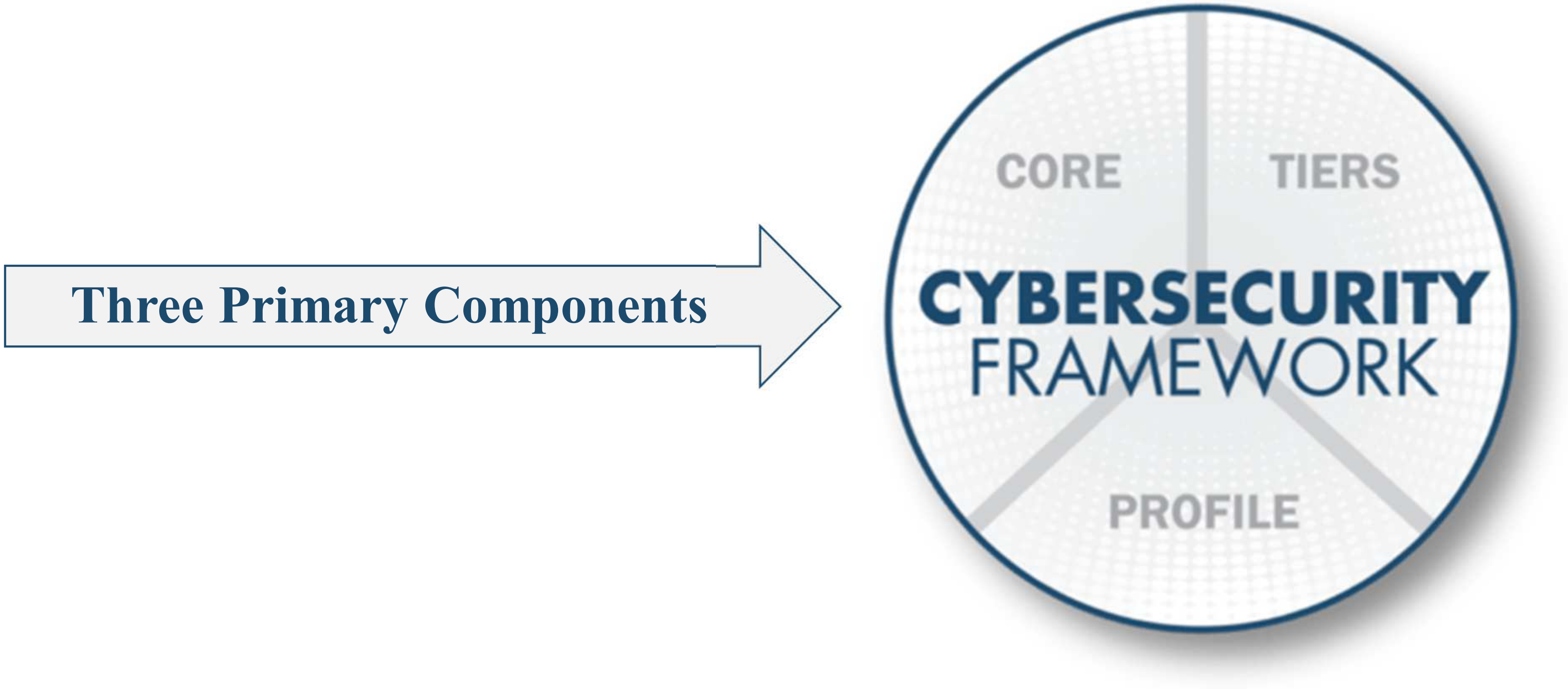
Shweta A. Chawla
Founder & Investigator
SC Cyber Solutions

NIST Cybersecurity Framework

- Published by the US National Institute of Standards and Technology (NIST)
- Primarily designed keeping US critical infrastructure in mind
  - Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
- Mitigates organization level cyber security risks

- The framework is guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk
- Facilitates communication between internal and external stakeholders
- The framework is not industry specific
- Current version 1.1
- Release date: 16 April 2018

The Cybersecurity Framework



Three Primary Components

The Cybersecurity Framework

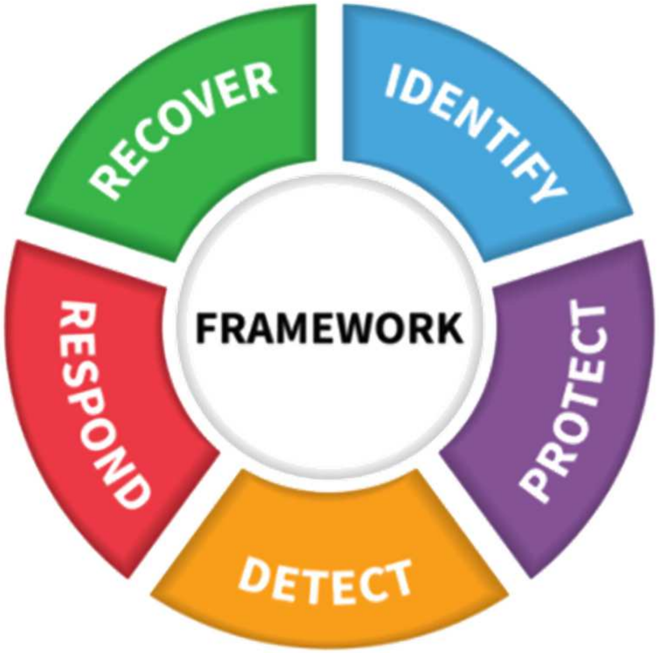
- Core
  - Contains activities, outcomes and references about aspects and approaches to cybersecurity
  - Desired cybersecurity outcomes organized in a hierarchy and aligned to more detailed guidance and controls
  - Presents industry standards, guidelines and practices
  - 5 function > 23 categories > 108 subcategories

- Profiles
  - Alignment of an organization’s requirements and objectives, risk appetite and resources using the desired outcomes of the Framework Core
  - Provides a list of outcomes based on business needs
  - Comparing current profile with target profile
  - Profile created using business requirements with risk assessment to prioritise tasks

- Implementation Tiers
  - Helps clarify cyber risk, processes and risk threshold
  - A qualitative measure of organizational cybersecurity risk management practices that provides guidance
  - Characterise practices over a range – Tier 1 (Partial) to Tier 4 (Adaptive)
    - Informal practices to flexible, risk informed, structured practices
  - Tier selection based on
    - current risk management practices
    - threat environment
    - legal and regulatory requirements
    - business/mission objectives
    - organizational constraints

Key Framework Attributes

- Principles of Current and Future Versions of the Framework
  - Common and accessible language
  - Adaptable to many technologies, lifecycle phases, sectors and uses
  - Risk-based
  - Based on international standards
  - Living document
  - Guided by many perspectives – private sector, academia, public sector



The Framework Core

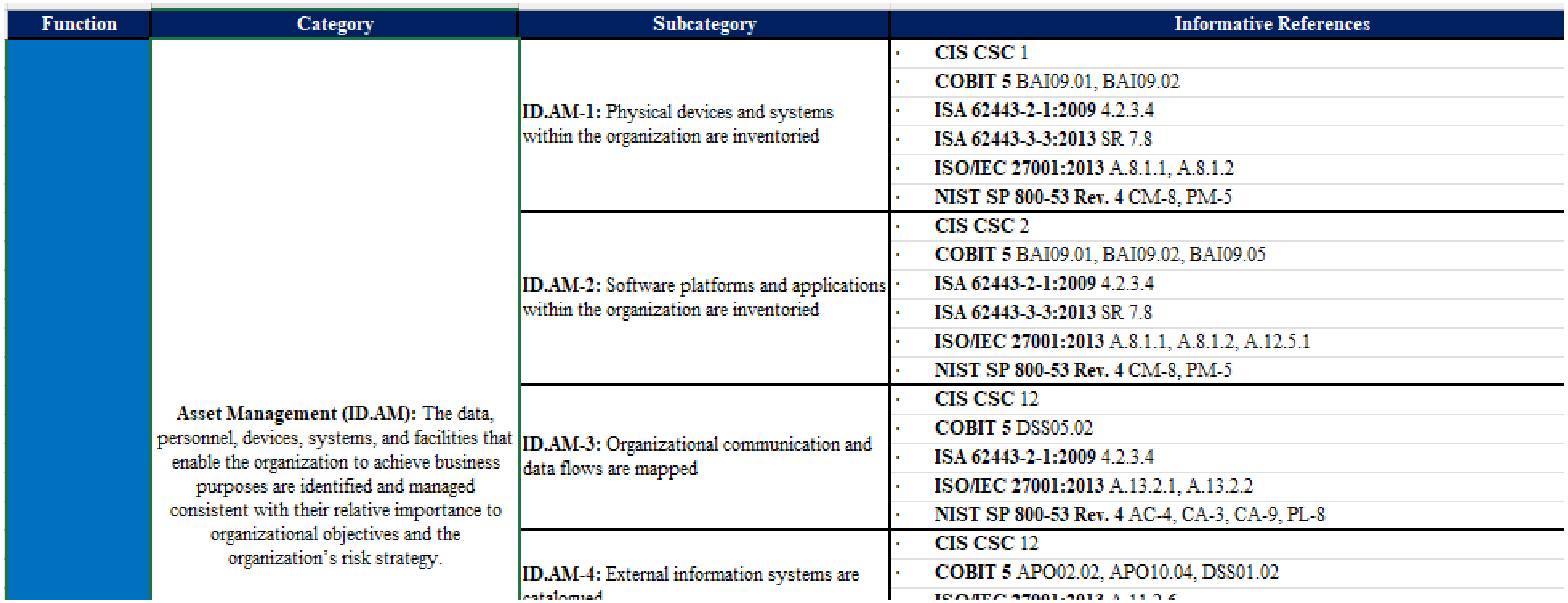
Establishes a Common Language

- Describes desired outcomes
- Understandable by everyone
- Applies to any type of risk management
- Defines the entire breadth of cybersecurity
- Spans both prevention and reaction

Function
Identify
Protect
Detect
Respond
Recover

SC
Cyber Solutions

NIST Framework Core

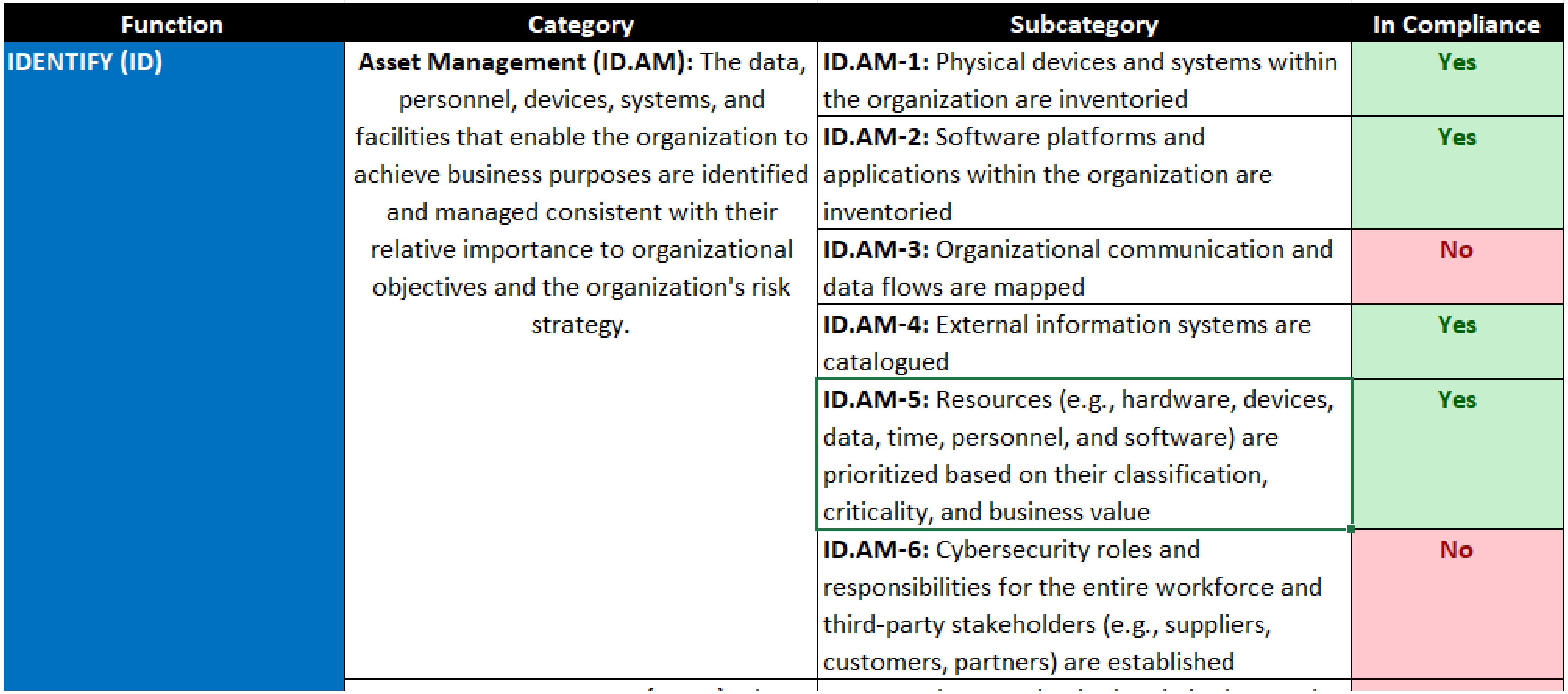


Function	Category	Subcategory	Informative References
	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	· **CIS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	· **CIS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 · **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	· **CIS CSC** 12 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	· **CIS CSC** 12 · **COBIT 5** APO02.02, APO10.04, DSS01.02 · **ISO/IEC 27001:2013** A.11.2.6

- The framework provides guidance
- Does not provide a checklist
- Organisations are required to build customized checklists based on their threats, vulnerabilities and risk tolerance

SC
Cyber Solutions

NIST Auditor Checklist



Function	Category	Subcategory	In Compliance
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	Yes
		ID.AM-2: Software platforms and applications within the organization are inventoried	Yes
		ID.AM-3: Organizational communication and data flows are mapped	No
		ID.AM-4: External information systems are catalogued	Yes
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	Yes
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	No

Thank You!

Contact details:
Mob: +91 98230 80864
shweta@sccybersolutions.com
www.sccybersolutions.com
@sccs1300