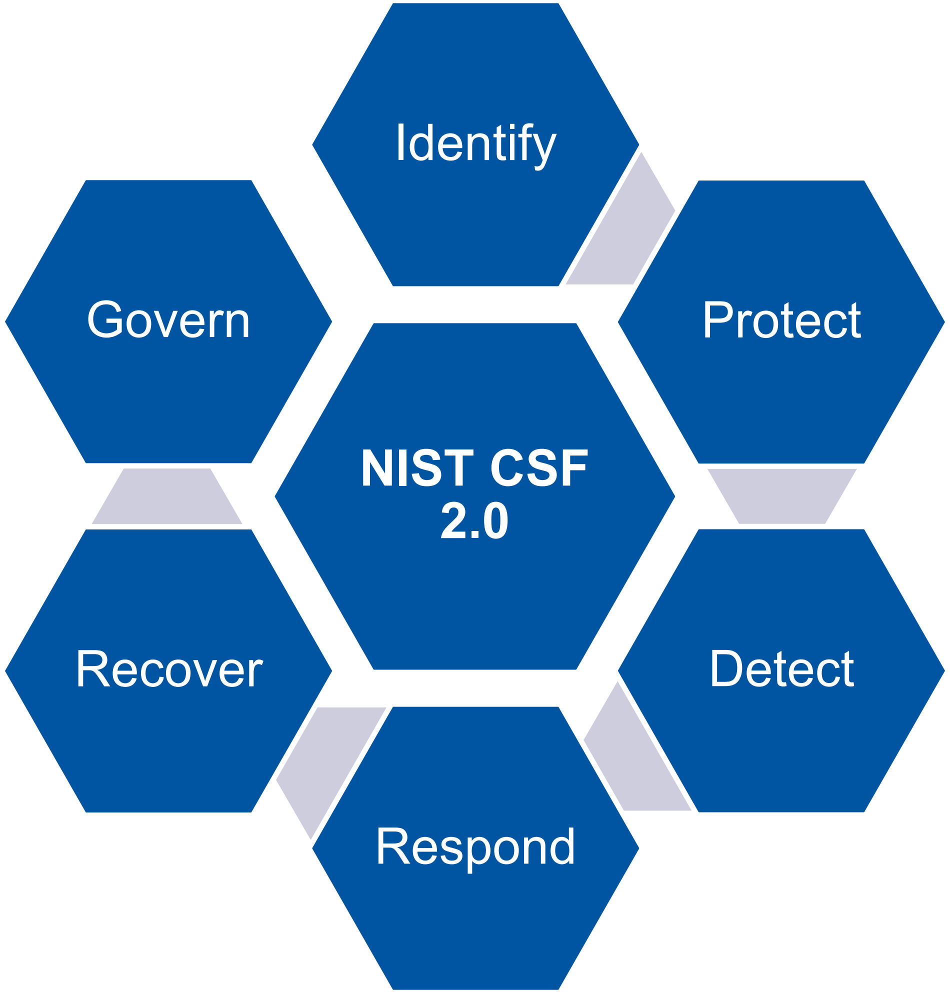
TEXAS RE

National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)

Devin Ferris
Manager, CIP Compliance Monitoring

November 01, 2024

NIST CSF 2.0

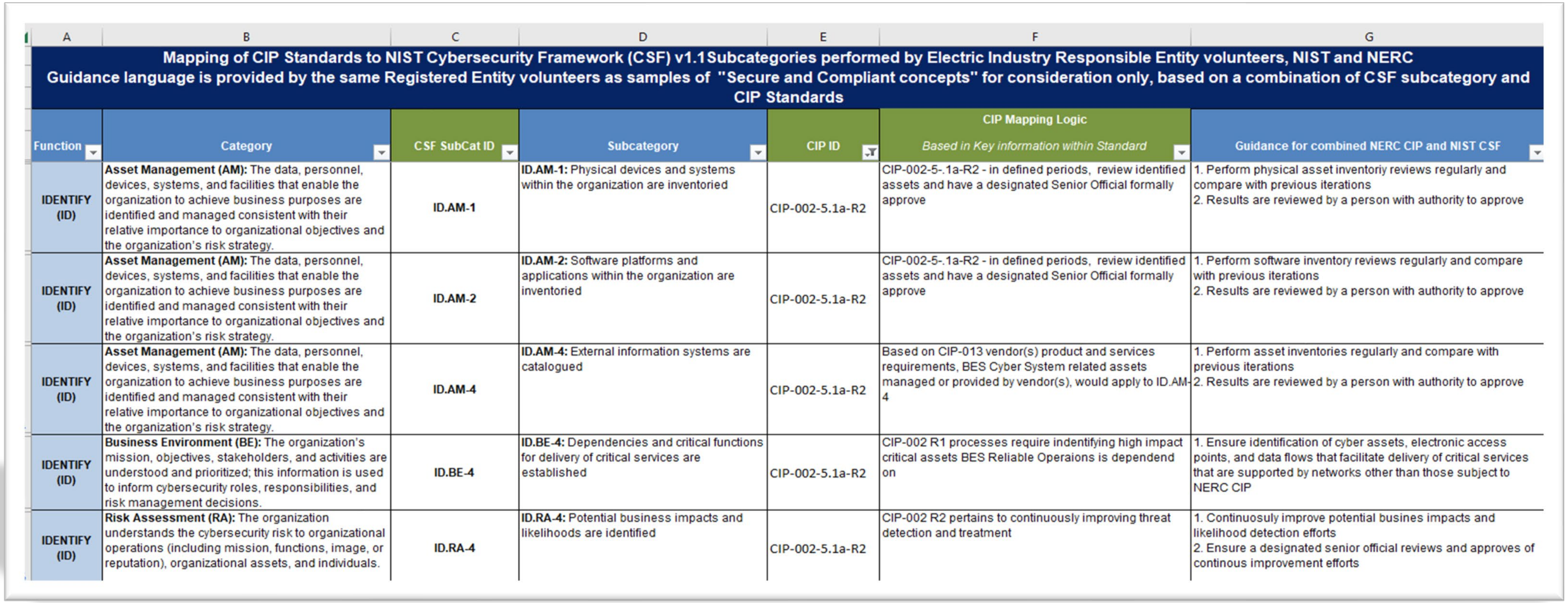

Identify
Protect
Detect
Respond
Recover
Govern
NIST CSF 2.0

NIST CSF 2.0 Resources

NIST CSF 2.0 Resources

- CSF 2.0
- Implementation Examples
- Quick Start Guides
- Mappings

CIP-002-5.1a CSF Mapping Example

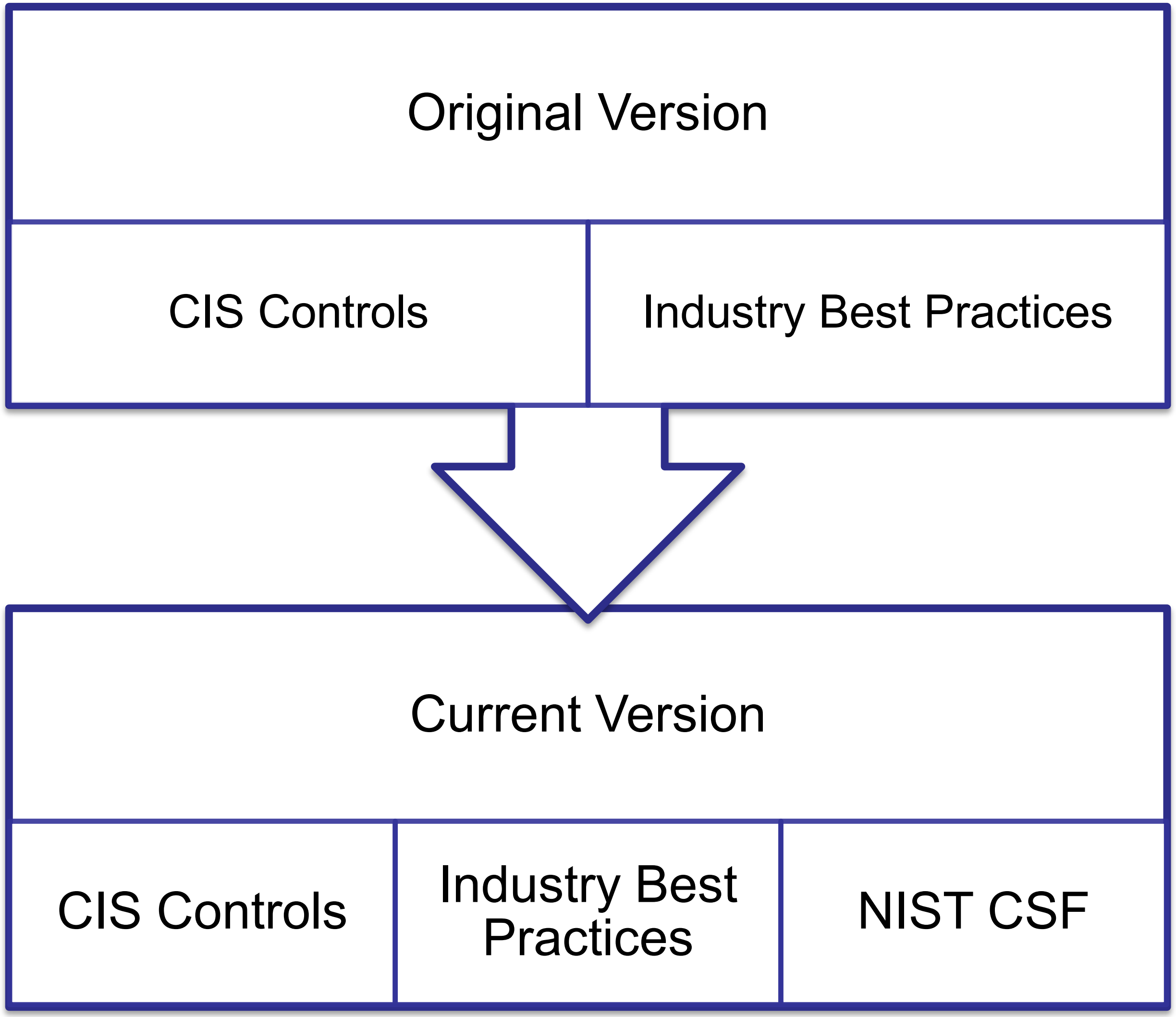


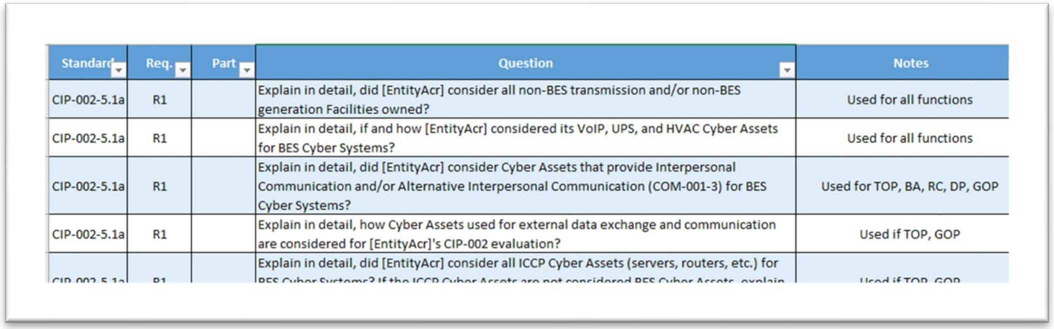
Mapping of CIP Standards to NIST Cybersecurity Framework (CSF) v1.1Subcategories performed by Electric Industry Responsible Entity volunteers, NIST and NERC
Guidance language is provided by the same Registered Entity volunteers as samples of "Secure and Compliant concepts" for consideration only, based on a combination of CSF subcategory and CIP Standards

A	B	C	D	E	F	G
					CIP Mapping Logic	
Function	Category	CSF SubCat ID	Subcategory	CIP ID	*Based in Key information within Standard*	Guidance for combined NERC CIP and NIST CSF
IDENTIFY (ID)	**Asset Management (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	**ID.AM-1:** Physical devices and systems within the organization are inventoried	CIP-002-5.1a-R2	CIP-002-5-.1a-R2 - in defined periods, review identified assets and have a designated Senior Official formally approve	1. Perform physical asset inventoriy reviews regularly and compare with previous iterations 2. Results are reviewed by a person with authority to approve
IDENTIFY (ID)	**Asset Management (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-2	**ID.AM-2:** Software platforms and applications within the organization are inventoried	CIP-002-5.1a-R2	CIP-002-5-.1a-R2 - in defined periods, review identified assets and have a designated Senior Official formally approve	1. Perform software inventory reviews regularly and compare with previous iterations 2. Results are reviewed by a person with authority to approve
IDENTIFY (ID)	**Asset Management (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-4	**ID.AM-4:** External information systems are catalogued	CIP-002-5.1a-R2	Based on CIP-013 vendor(s) product and services requirements, BES Cyber System related assets managed or provided by vendor(s), would apply to ID.AM-4	1. Perform asset inventories regularly and compare with previous iterations 2. Results are reviewed by a person with authority to approve
IDENTIFY (ID)	**Business Environment (BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-4	**ID.BE-4:** Dependencies and critical functions for delivery of critical services are established	CIP-002-5.1a-R2	CIP-002 R1 processes require indentifying high impact critical assets BES Reliable Operaions is dependend on	1. Ensure identification of cyber assets, electronic access points, and data flows that facilitate delivery of critical services that are supported by networks other than those subject to NERC CIP
IDENTIFY (ID)	**Risk Assessment (RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-4	**ID.RA-4:** Potential business impacts and likelihoods are identified	CIP-002-5.1a-R2	CIP-002 R2 pertains to continuously improving threat detection and treatment	1. Continuosuly improve potential busines impacts and likelihood detection efforts 2. Ensure a designated senior official reviews and approves of continous improvement efforts

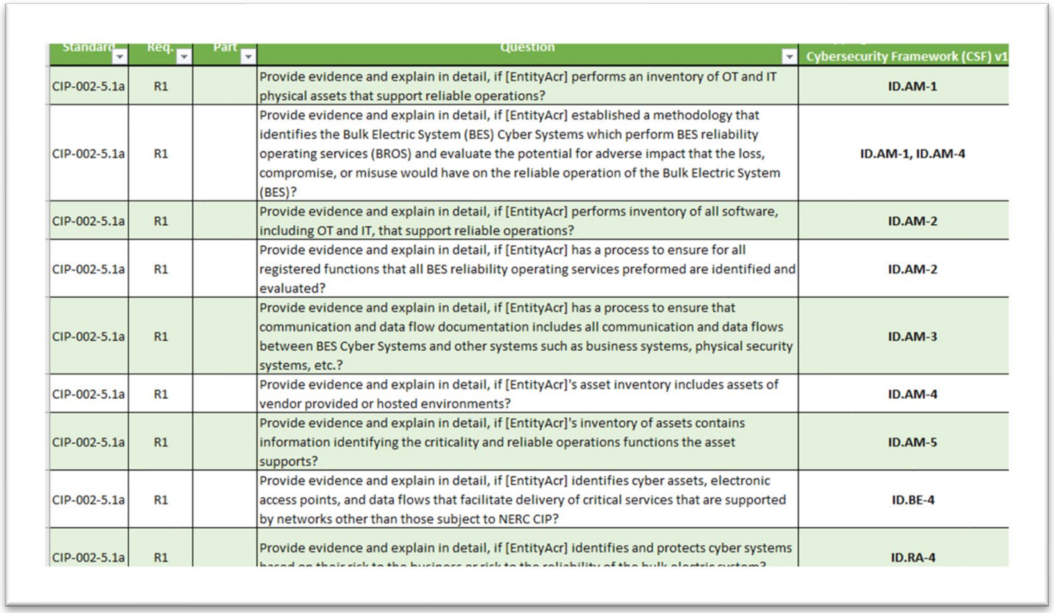
NERC One Stop Shop

CIP & O&P Common Questions





Standard	Req.	Part	Question	Notes
CIP-002-5.1a	R1		Explain in detail, did [EntityAcr] consider all non-BES transmission and/or non-BES generation Facilities owned?	Used for all functions
CIP-002-5.1a	R1		Explain in detail, if and how [EntityAcr] considered its VoIP, UPS, and HVAC Cyber Assets for BES Cyber Systems?	Used for all functions
CIP-002-5.1a	R1		Explain in detail, did [EntityAcr] consider Cyber Assets that provide Interpersonal Communication and/or Alternative Interpersonal Communication (COM-001-3) for BES Cyber Systems?	Used for TOP, BA, RC, DP, GOP
CIP-002-5.1a	R1		Explain in detail, how Cyber Assets used for external data exchange and communication are considered for [EntityAcr]'s CIP-002 evaluation?	Used if TOP, GOP
CIP-002-5.1a	R1		Explain in detail, did [EntityAcr] consider all ICCP Cyber Assets (servers, routers, etc.) for BES Cyber Systems? If the ICCP Cyber Assets are not considered BES Cyber Assets, explain	Used if TOP, GOP



Standard	Req.	Part	Question	Cybersecurity Framework (CSF) v1
CIP-002-5.1a	R1		Provide evidence and explain in detail, if [EntityAcr] performs an inventory of OT and IT physical assets that support reliable operations?	ID.AM-1
CIP-002-5.1a	R1		Provide evidence and explain in detail, if [EntityAcr] established a methodology that identifies the Bulk Electric System (BES) Cyber Systems which perform BES reliability operating services (BROS) and evaluate the potential for adverse impact that the loss, compromise, or misuse would have on the reliable operation of the Bulk Electric System (BES)?	ID.AM-1, ID.AM-4
CIP-002-5.1a	R1		Provide evidence and explain in detail, if [EntityAcr] performs inventory of all software, including OT and IT, that support reliable operations?	ID.AM-2
CIP-002-5.1a	R1		Provide evidence and explain in detail, if [EntityAcr] has a process to ensure for all registered functions that all BES reliability operating services preformed are identified and evaluated?	ID.AM-2
CIP-002-5.1a	R1		Provide evidence and explain in detail, if [EntityAcr] has a process to ensure that communication and data flow documentation includes all communication and data flows between BES Cyber Systems and other systems such as business systems, physical security systems, etc.?	ID.AM-3
CIP-002-5.1a	R1		Provide evidence and explain in detail, if [EntityAcr]'s asset inventory includes assets of vendor provided or hosted environments?	ID.AM-4
CIP-002-5.1a	R1		Provide evidence and explain in detail, if [EntityAcr]'s inventory of assets contains information identifying the criticality and reliable operations functions the asset supports?	ID.AM-5
CIP-002-5.1a	R1		Provide evidence and explain in detail, if [EntityAcr] identifies cyber assets, electronic access points, and data flows that facilitate delivery of critical services that are supported by networks other than those subject to NERC CIP?	ID.BE-4
CIP-002-5.1a	R1		Provide evidence and explain in detail, if [EntityAcr] identifies and protects cyber systems based on their risk to the business or risk to the reliability of the bulk electric system?	ID.RA-4

Questions?

TEXAS RE

Ensuring electric reliability for Texans