TEXAS RE

Internal Controls Assessments

Devin Kitchens
Compliance Team Lead

CIP & O&P Common Questions

https://www.texasre.org/compliance

Entity Resources

Texas RE has developed guidance and reference documents to help entities prepare for compliance engagements and complete data request forms. Below are links to the guidance and reference documents. Additional documents associated with specific compliance activities are included in the corresponding sections below.

Texas RE encourages registered entities to review the Engagement (CIP and O&P) Common Questions. These questions provide insight on how Texas RE may approach a registered entity and are based on past experience monitoring the NERC Reliability Standards. The questions include internal control questions, which are critically important in understanding how a registered entity manages risk.

The Protection System Operations and Misoperations Procedure and Form reflects best practices that Texas RE has experienced reviewing PRC-004. The document provides a clear path for roles and responsibilities when determining what has occurred during an event and what should be done to support reliable operations. Some of the actions described reflect mitigation efforts noted as a result of compliance monitoring. With any best practice the outcome depends upon the personnel executing the actions and utilizing this form; the process ***does not*** guarantee compliance. This is simply being provided for registered entities who may not have a clearly documented process or want to compare their inhouse solution.

The Generator Welcome Package was designed to provide Generator Owner(s) (GO) and Generator Operator(s) (GOP) a framework to aid in preparing for compliance obligations and expectations. The Generator Welcome Package was developed based on Texas RE experiences with new GOs and GOPs and does not guarantee that compliance will be achieved. However, with proper planning and a framework for assessing the state of compliance, an entity is better prepared to be compliant on its registration date and beyond.

Documents

CIP & O&P Common Questions

Original Version

CIS Controls	Industry Best Practices

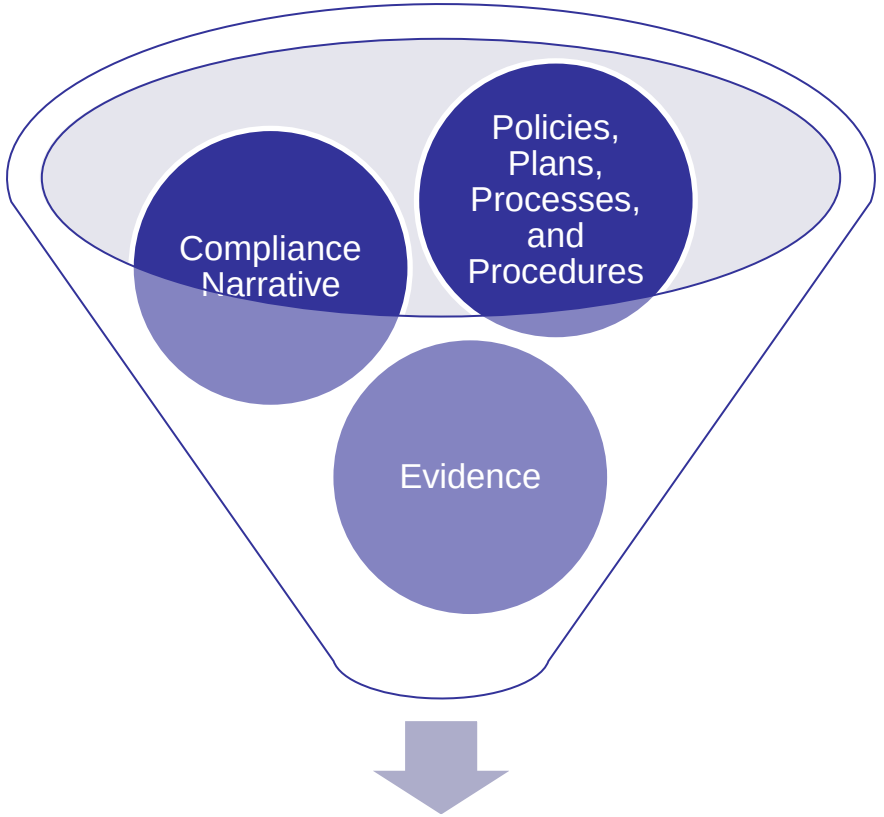
Updated Version

CIS Controls	Industry Best Practices	NIST CSF

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	

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	ID.RA-4

Assessment Approach



Internal Controls Questions

CIP-002-5.1a Example

A	B	C	D	E	F	G
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						
Function	Category	CSF SubCat ID	Subcategory	CIP ID	CIP Mapping Logic *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

NIST CSF Framework V1.1 Core

Function	Category	Subcategory	Informative References
		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

NIST CSF Framework V1.1

CM-8 - Information System Component Inventory

Special Publication 800-53 Revision 4 — Security and Privacy Controls for Federal Information Systems and Organizations

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
CM-6	Configuration Settings	P1	CM-6	CM-6	CM-6 (1) (2)
CM-7	Least Functionality	P1	CM-7	CM-7 (1) (2) (4)	CM-7 (1) (2) (5)
CM-8	Information System Component Inventory	P1	CM-8	CM-8 (1) (3) (5)	CM-8 (1) (2) (3) (4) (5)
CM-9	Configuration Management Plan	P1	Not Selected	CM-9	CM-9
CM-10	Software Usage Restrictions	P2	CM-10	CM-10	CM-10
CM-11	User-Installed Software	P1	CM-11	CM-11	CM-11

Control Enhancements

CM-8 INFORMATION SYSTEM COMPONENT INVENTORY

Control: The organization:

a. Develops and documents an inventory of information system components that:

1. Accurately reflects the current information system;
2. Includes all components within the authorization boundary of the information system;
3. Is at the level of granularity deemed necessary for tracking and reporting; and
4. Includes [*Assignment: organization-defined information deemed necessary to achieve effective information system component accountability*]; and

b. Reviews and updates the information system component inventory [*Assignment: organization-defined frequency*].

Supplemental Guidance: Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner). Information deemed necessary for effective accountability of information system components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location. Related controls: CM-2, CM-6, PM-5.

Control Enhancements:

(1) *INFORMATION SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATIONS / REMOVALS*

The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

TEXAS RE
Ensuring electric reliability for Texans