

RELIABILITY & SECURITY

Workshop - Tempe, Arizona



March 25–26, 2025

Managing Risk to the Bulk Electric System

NextEra Energy - NERC Information Command Center (NICC)

Presenters:

Robert Wargo, Senior Director – NERC Center of Excellence

Carlos N. Morales, Senior Manager – NERC Center of Excellence

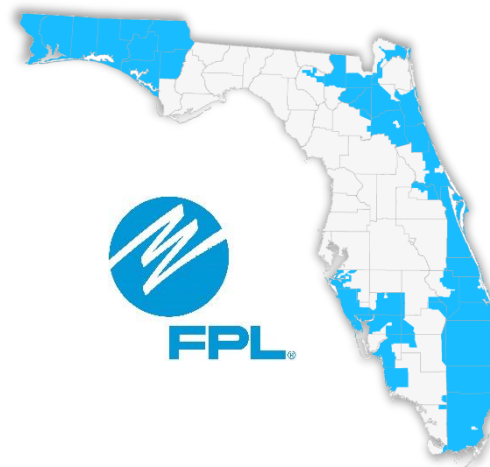
Date:

March 2025

NextEra Energy is powered by industry-leading companies focused on customer value and operational excellence.



- World's largest generator of renewable energy from the wind and sun, and a world leader in battery storage, committed to producing clean, emissions-free electricity across North America.

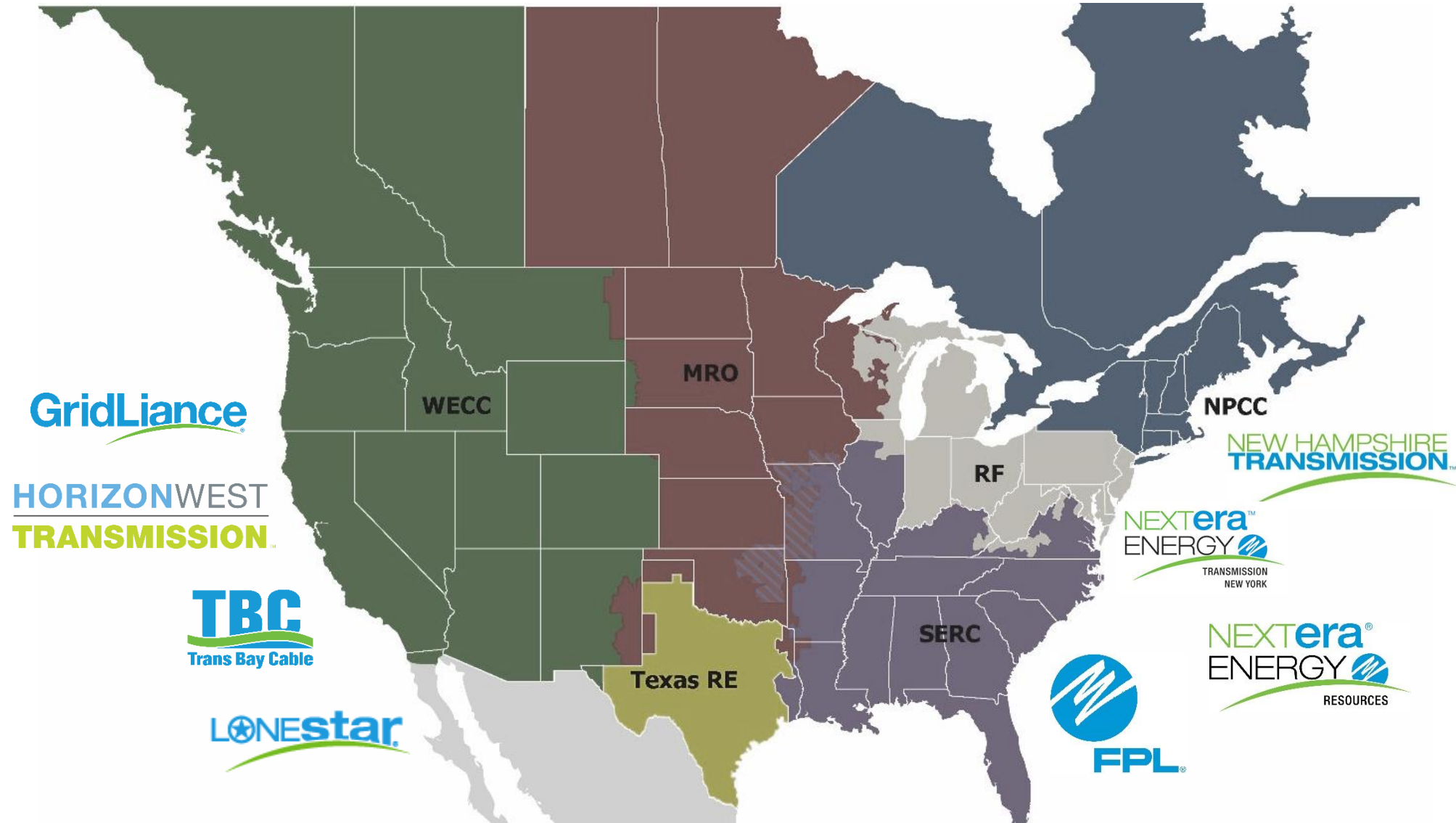


- America's largest electric utility (vertically integrated) serving approximately 12 million people across Florida with reliable electricity from a diverse energy mix, while keeping bills as low as possible.



- Leading competitive transmission company that owns, develops, finances, constructs, operates and maintains transmission assets across North America.
- Operates through its regional subsidiaries to integrate renewable energy and strengthen the electric grid.

NextEra Energy's NERC compliance obligations span across several subsidiaries and operate in every region.



Organization Registration and Certification Program and Compliance Monitoring and Enforcement Program Annual Report

February 14, 2024

RELIABILITY | RESILIENCE | SECURITY



3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Top 10 O&P Noncompliance Reported in 2023

In 2023, the most frequently reported noncompliance involving the O&P Standards included FAC-008, which has been an ERO Enterprise focus area for several years, PRC-005 and VAR-002, which involve high frequency conduct, and several Standards involving coordination or verification of generator data (e.g., PRC-024, MOD-025, PRC-019, MOD-026, and MOD-027).

EOP-011-2, which became effective on April 1, 2023, and incorporated new Requirements for cold weather preparedness plans for generating units and training on the same, also made the most frequently reported list, with the bulk of the noncompliance involving the new Requirements R7 and R8. Most of these R7 and R8 noncompliances were self-identified or reported as part of self-certifications.

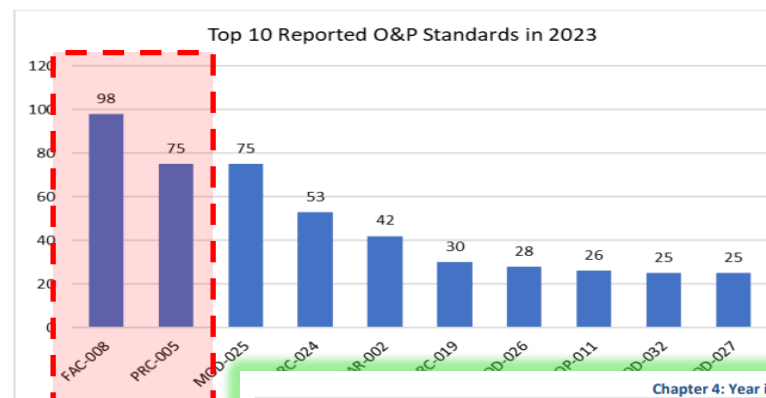


Figure 7:

Top 10 CIP Noncompliance Reported in 2023

In 2023, the most frequently reported noncompliance involving the CIP Standards included CIP-007, CIP-010, and CIP-004, which all involve high volume and high frequency conduct.

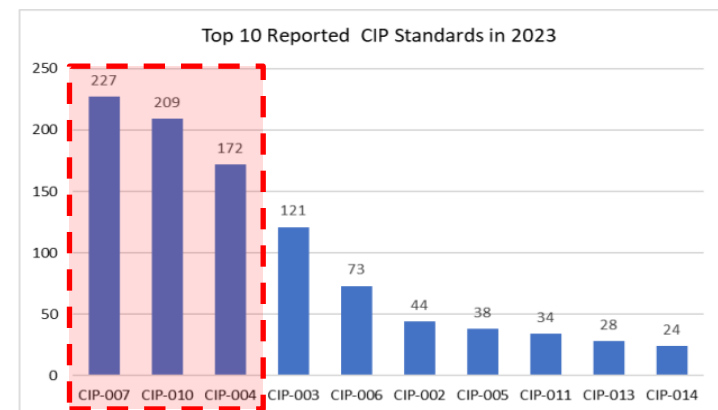
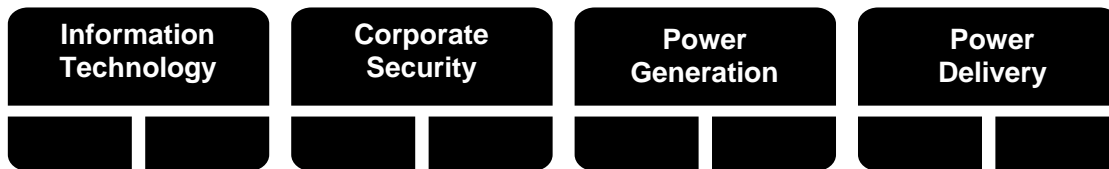


Figure 6: CIP Noncompliance Reported in 2023

In 2020, we saw an opportunity and a need to reimagine our approach specific to our NERC compliance program.

Before

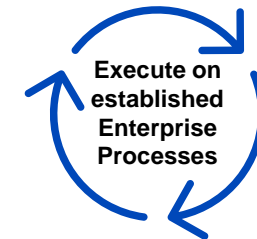
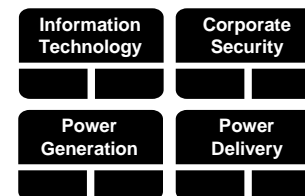
Spin up the audit machine / Reactive



- Manual evidence production / minimal information validation
- Different processes and interpretations of what was needed to substantiate compliance
- Presentation by business unit resulted in fragmented view/representation of the registered entity
- O&M costs associated with audit support and execution continued to increase
- Focus was on compliance not on managing security risk

After

Always Audit Ready / Proactive



Produce standard evidence sets to substantiate compliance

In 2020, we saw an opportunity and a need to reimagine our approach specific to our NERC compliance program.

Before

"Spin up the audit machine" / Reactive



- Manual evidence production / minimal information validation
- Different processes and interpretations of what was needed to substantiate compliance
- Presentation by business unit (vs. registered entity) resulted in fragmented view/representation of the registered entity
- O&M costs associated with audit support and execution continued to increase
- Focus was on compliance not on managing security risk

Preparation

- Months of manual planning & preparation
- 100+ people
- Unsure of scope
- Boil the ocean

Audit Notification

- Company
- Date Range
- Standards & Requirements

Hours devoted to manual prep work not relevant to audit scope could have been used elsewhere

Evidence Generation

- Process Narratives (RSAW)
- Audit Workbook (ERT)
- Initial Evidence Requests (L1/L2 & Follow-On Data Requests)

"Open Book Test"

Submission to Auditors

- Audit scope drives level of effort & cycle time

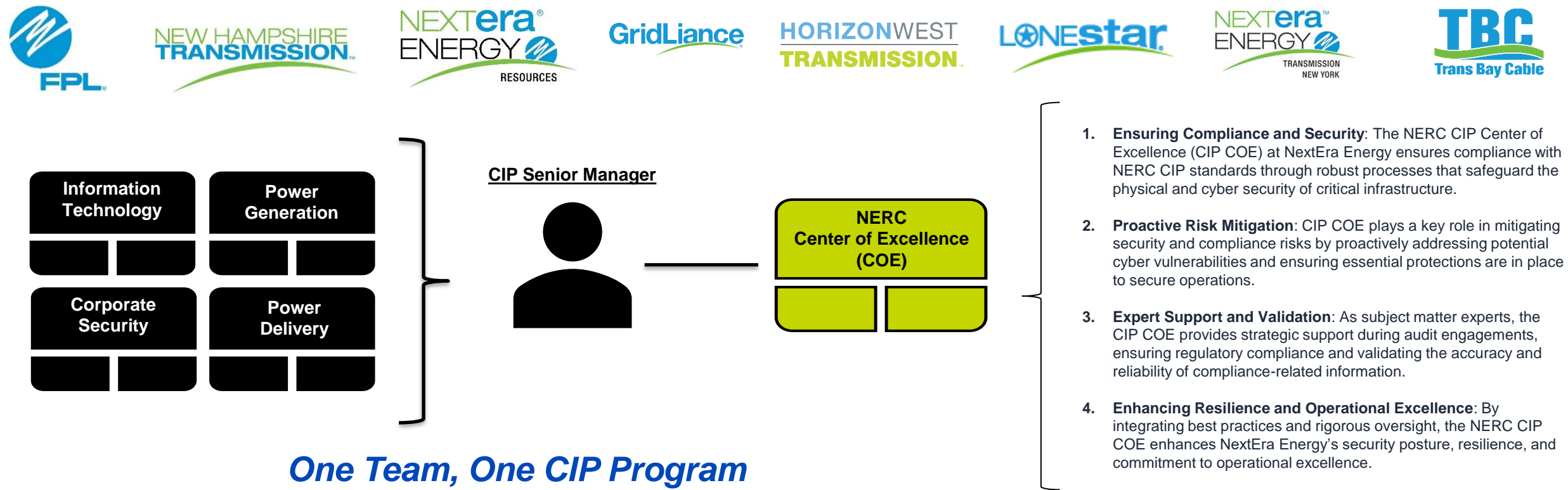
Subsequent "ad-hoc" requests for evidence

On site interviews

Only Time Compliance Evidence is 100% Assembled, Tested & Assured

Automation of evidence generation, quality assurance, and delivery is how we go from Good to Great

To induce change, we needed an organization that could serve as an aggregator with purview across all lines of business and all registered entities.

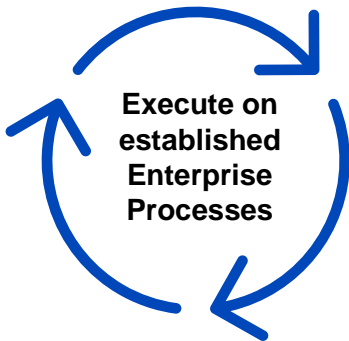
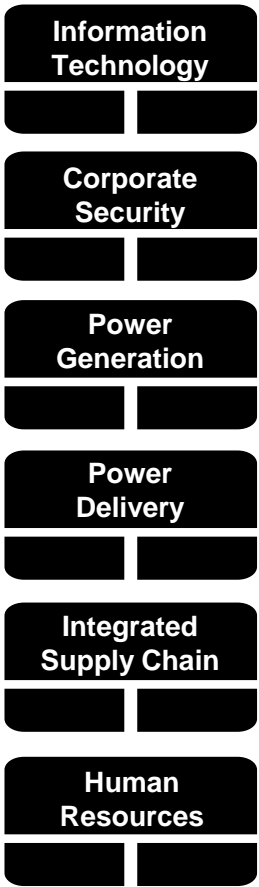


With our reimagination efforts underway, the NERC COE established a vision for the future that would capitalize on an environment that was data-rich.

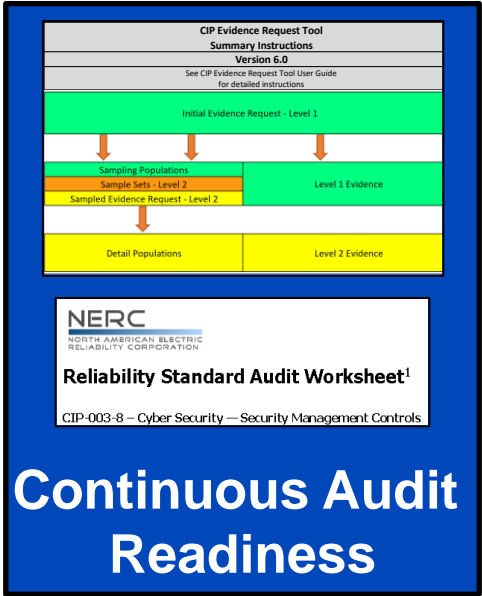
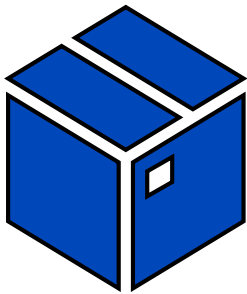
**NEE Registered Entities
performing NERC
Registered Functions**



**NEE Service
Organizations supporting
grid reliability / security**



Leverage common toolset



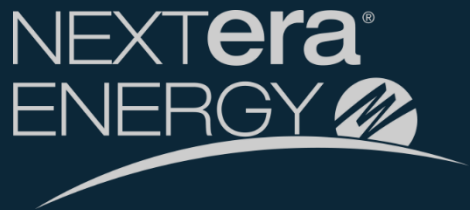
Establish common meta
data and aggregate into
a unified CIP Data
Warehouse



Produce standard
evidence sets to
substantiate compliance

Program Approach we moved toward

What is Continuous Monitoring?



Foundational Elements of a Continuous Monitoring System

1

Automated and Verified Systems

Monitor threats, vulnerabilities, and compliance status continuously, ensuring data accuracy and completeness.

(NIST SP 800-137, Section 3.1.2)

2

Timely Awareness and Real-Time Information Validation

Provide timely notifications about potential issues and validate compliance in real time, maintaining continuous audit readiness.

(NIST SP 800-137, Sections 2.3.2 and 3.1.3)

3

Complete and Frequent Data Acquisition

Comprehensive data sets are gathered and validated frequently to inform monitoring efforts and detect emerging issues early.

(NIST SP 800-137, Sections 3.1.4 and 3.1.5)

4

Proactive Auditing

Real-time data is used to perform continuous and proactive auditing, enhancing control testing and validation frequency.

(NIST SP 800-137, Section 3.2.4)

5

Informed Decision Making and Risk Management

Automated and human decision-making is supported through an established operational model, maintaining acceptable risk levels through adherence to SLAs and critical process validation checks.

(NIST SP 800-137, Sections 2.2 and 3.3)

Operationalize internal controls and real-time continuous monitoring to assist with mitigating risk

F

Failure

M

Mode

E

Effect

A

Analysis

Identify what can go wrong with the process, consider the potential for occurrence, the negative effects that can be realized, and determine ways to mitigate the likelihood.

Control Type

Prevent

Detect

Control Frequency

Automated

Manual

Operational Model

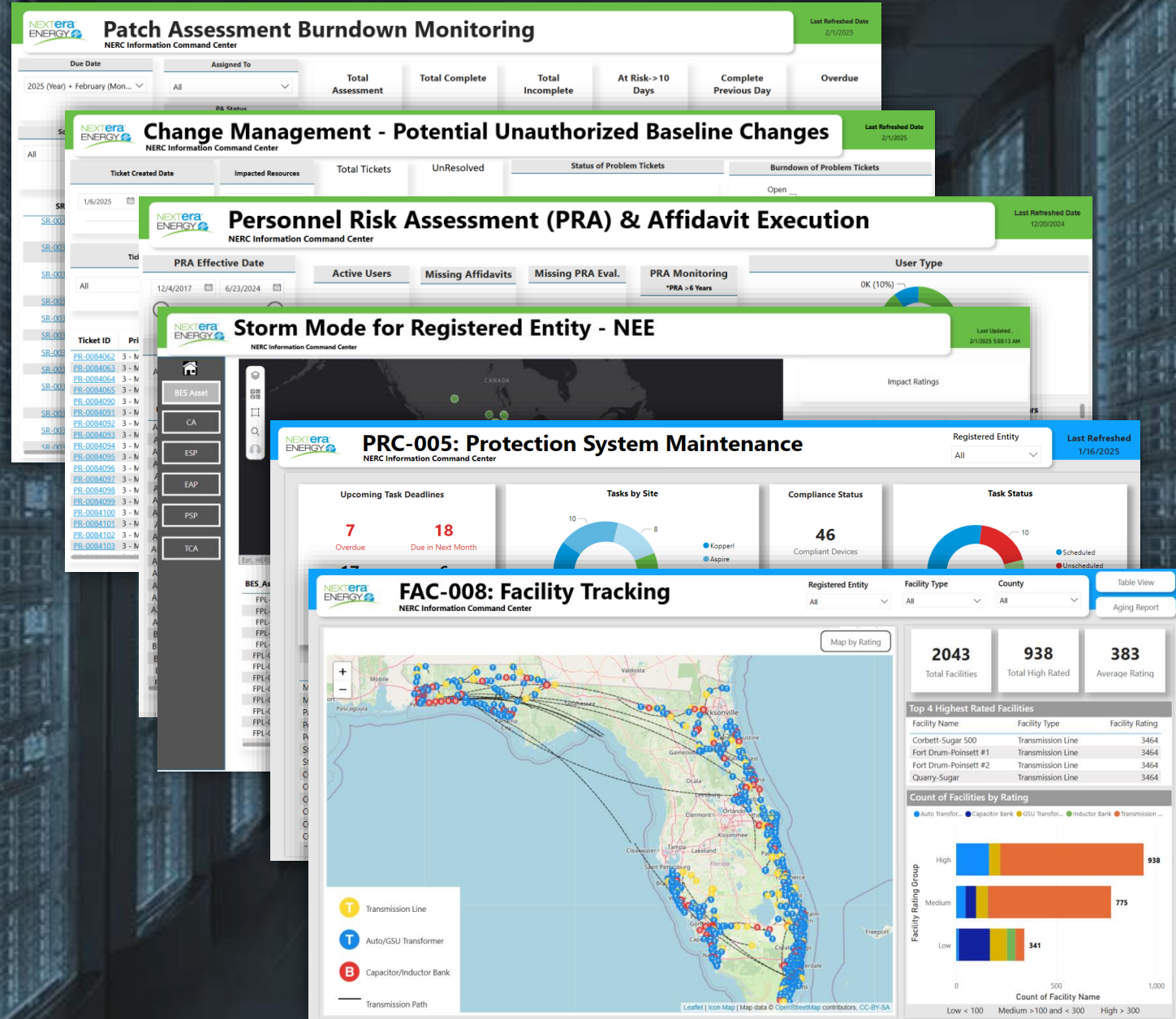
Establish playbooks to respond to off-normal conditions identified and determine appropriate SLAs to ensure the process remains in control (as designed).

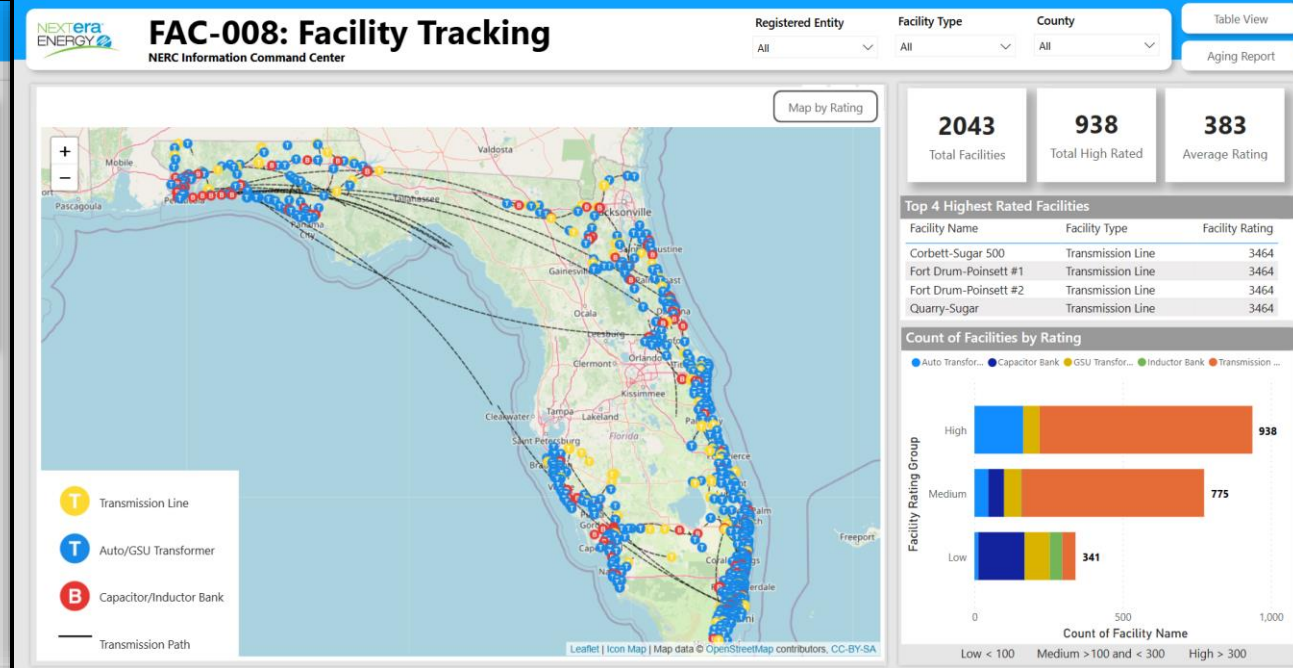
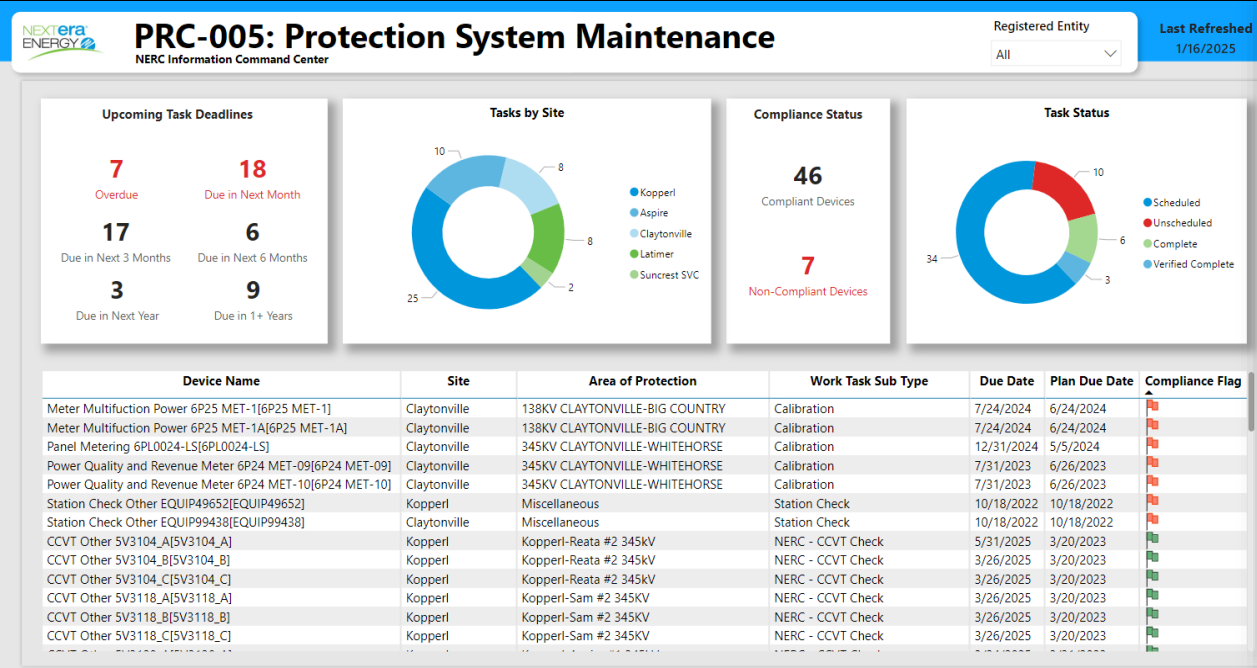
NERC Information Command Center (NICC) is now live as we look to refine continuous monitoring in the Critical Infrastructure Protection (CIP) space

- ➔ Real-time continuous monitoring and automated information validation
- ➔ Enhanced situation awareness and audit support capabilities
- ➔ Unified visibility between the activities associated with NERC CIP and NERC O&P compliance obligations
- ➔ Reduced risk to the business



We implemented proactive measures to **reduce risk** tied to our NERC compliance obligations all centered around a **safe, secure, reliable grid.**





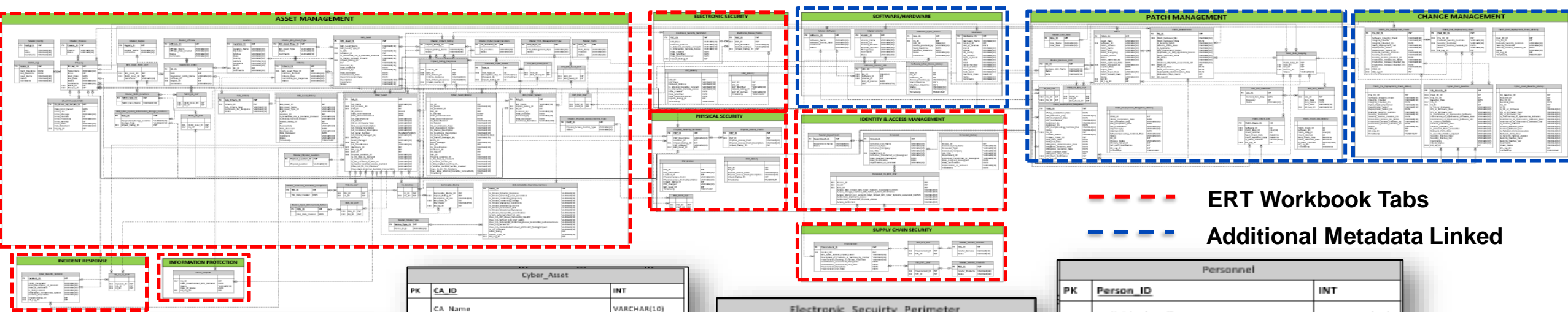
➔ Each visualization will have an associated Operational Model

- Response plan tied to process control limits
- Early indicators of off-normal conditions
- Processes to perform information validation

➔ Instructions on pull the data from source systems

- Identification of source systems
- Establish standard on metadata needed
- Steps to extract and load the data

In data rich environment and with standard definition for continuous monitoring, we set out on a journey to build an Information Management system.



BES_Asset		
PK	BES_Asset_ID	INT
FK3	BES_Asset_Name	VARCHAR(10)
	BES_Asset_Type_ID	INT
FK2	Is_BES	VARCHAR(10)
	Location_ID	INT
FK1	Is_Accessible_Via_a_Routable_Protocol	VARCHAR(10)
	Is_Dialup_Connect_Present	VARCHAR(10)
	Impact_Rating_ID	INT
	KV	VARCHAR(10)
	Assessed_By	VARCHAR(10)
	Date_Assessed	DATE
	Reviewed_By	VARCHAR(10)
	Date_Reviewed	DATE
	Commissioned_Date	DATE

Cyber_Asset		
PK	CA_ID	INT
	CA_Name	VARCHAR(10)
FK4	CA_Function_ID	INT
FK5	PSP_ID	INT
	IP_Address	FLOAT
	Date_Commissioned	DATE
	Date_Decommissioned	DATE
	CA_Manufacturer	VARCHAR(10)
	CA_Model	VARCHAR(10)
	OS_or_Firmware_Type	VARCHAR(10)
	Risk_Assessment_Status	VARCHAR(10)
	CA_Device_Description	VARCHAR(10)
	CA_Functional_Description	VARCHAR(10)
	CA_Serial_Number	NUMBER(38,0)
	CA_Device_Managed_By	VARCHAR(10)
FK2	BROS_ID	INT
	Asset_Manager	VARCHAR(10)
FK3	BCS_ID	INT
	CA_Classification	VARCHAR(10)
FK7	Hardware_ID	INT
FK6	Ext_Log_ID	INT
FK8	EAP_ID	INT
	Physical_Location_ID	VARCHAR(10)
	is_CA_Dial_up_Connect	VARCHAR(10)
	is_Control_Center_CA	VARCHAR(10)
	is_IRA_Enabled_to_This_CA	VARCHAR(10)
	is_Vendor_Remote_Access_Enabled	VARCHAR(10)

Electronic_Securty_Perimeter			
PK	ESP_ID	INT	
FK1	ESP_Desc	VARCHAR(10)	
	Network_Address	VARCHAR(10)	
	Is_External_Routable_Connect	VARCHAR(10)	
	Is_interactive_Remote_Access	VARCHAR(10)	
	Date_Created	DATE	
	Date_Modified	DATE	
	Date_Decomm	Physical_Ac	
	Impact_Rating	PK	PAP_ID

Personnel		
PK	Person_ID	INT
FK1	Individual_Full_Name	VARCHAR(10)
	Personnel_Type	VARCHAR(10)
	Individual_Company	VARCHAR(10)
	Job_Title	VARCHAR(10)
	Department_ID	VARCHAR(10)
	Individual_Transferred_or_Reassigned	VARCHAR(10)
	Date_Assigned_Reassigned	
	Date_Termination	
Implementer_or_Implementer_ID	PK	Procurement ID

Procurement		
PK	Procurement_ID	INT
FK1	Vendor_ID	INT
	BES_Cyber_System_Impact_Level	VARCHAR(10)
	Description_of_Products_or_Services_by_Vendor	VARCHAR(10)
	Procurement_resulting_in_Vendor_Transition	VARCHAR(10)
	Identification_Assessment_Start_Date	DATE
	Identification_Assessment_End_Date	DATE
	Procurement_Start_Date	DATE
	Procurement_End_Date	DATE

Physical_Access_Points		
PK	PAP_ID	INT
FK1	PSP_ID	INT
	Physical_Access_Point	VARCHAR(10)
	Physical_Access_Point_Description	VARCHAR(20)
	Impact_Rating_ID	INT

[illegible]

NERC Information Command Center (NICC) – Data Warehouse

Source Systems

AVAMAR  BIGFIX

 Change Gear

 JIRA 

 Documentum

 SharePoint

 TREND MICRO  Radar

 OnGuard
 LENEL S2



ETLs

Extract, Transform, Load



Data Warehouse

*Centralized aggregated data hub
used for analytics to perform
continuous monitoring and audit
support services*





Extract Transform and Load (ETL) Health

NERC Information Command Center (NICC)

Successful Jobs
68

Failed Jobs
0

March 11, 2025
9:00 AM

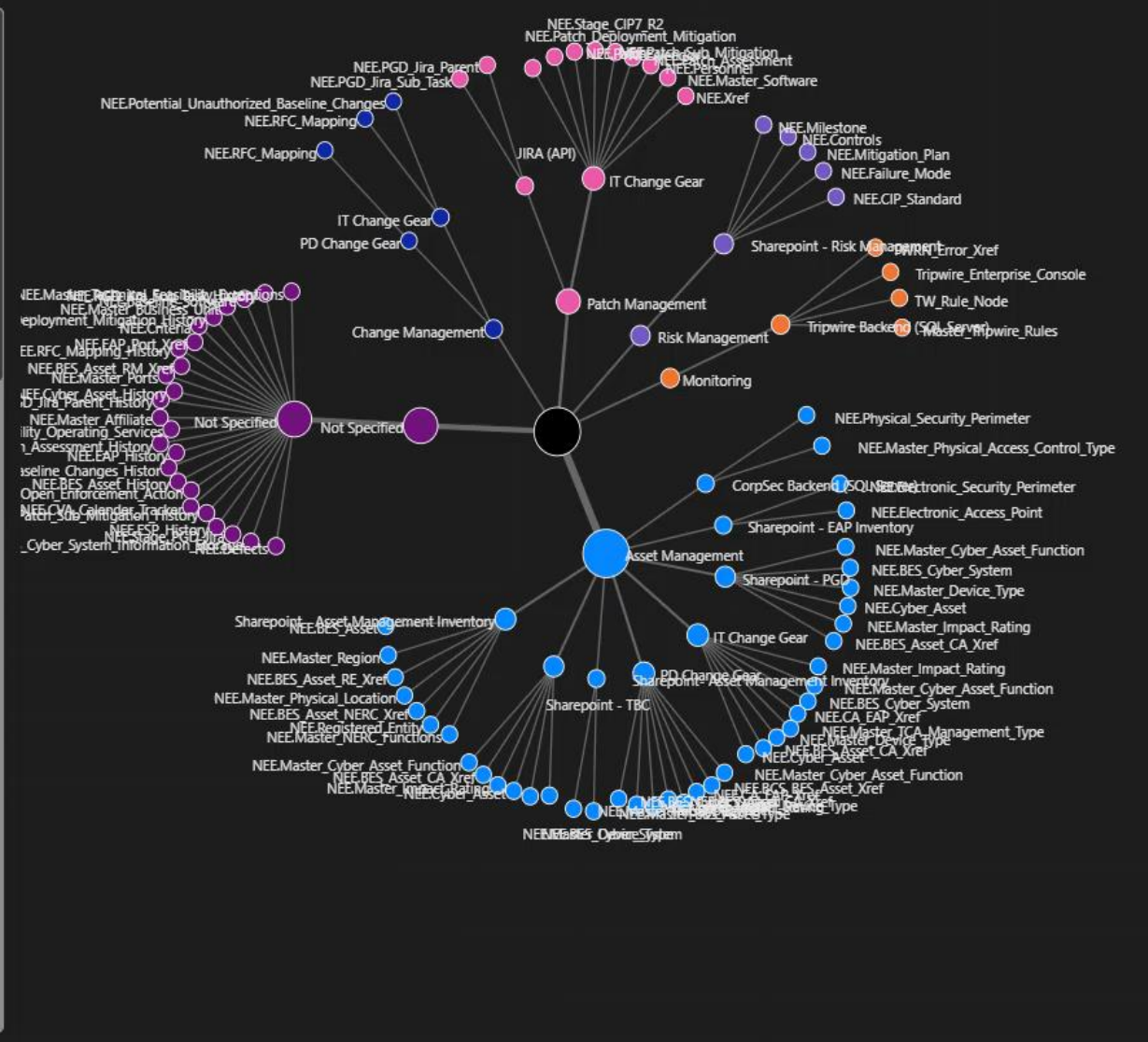
Job Status
All

Domain
All

Tool
All

Table
All

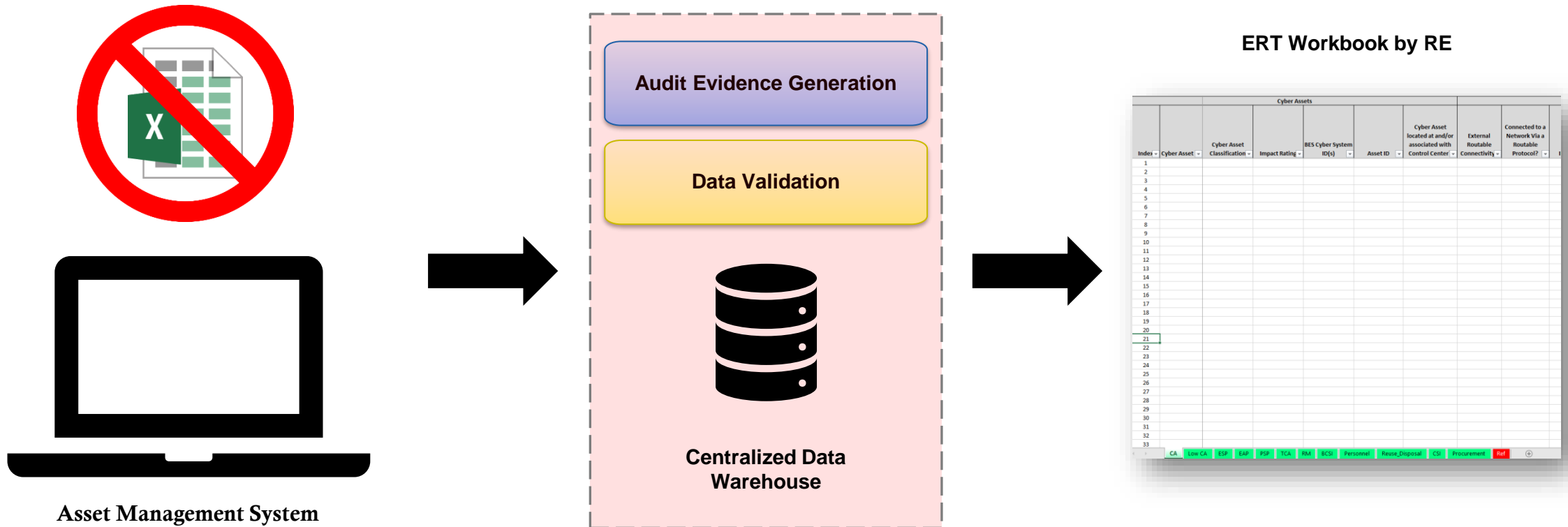
Domain	Tool	Table	Job Status
Asset Management	CorpSec Backend (SQL Server)	NEE.Master_Physical_Access_Control_Type	Success
		NEE.Physical_Security_Perimeter	Success
	IT Change Gear		Success
	PD Change Gear	NEE.BCS_BES_Asset_Xref	Success
		NEE.BES_Asset_CA_Xref	Success
		NEE.BES_Cyber_System	Success
		NEE.CA_EAP_Xref	Success
		NEE.Cyber_Asset	Success
		NEE.Master_Cyber_Asset_Function	Success
		NEE.Master_Device_Type	Success
		NEE.Master_Impact_Rating	Success
Sharepoint - Asset Management Inventory	Sharepoint - Asset Management Inventory	NEE.BES_Asset	Success
		NEE.BES_Asset_NERC_Xref	Success
		NEE.BES_Asset_RE_Xref	Success
		NEE.Master_NERC_Functions	Success
		NEE.Master_Physical_Location	Success
		NEE.Master_Region	Success
		NEE.Registered_Entity	Success
		NEE.Electronic_Access_Point	Success
		NEE.Electronic_Security_Perimeter	Success
		NEE.BES_Asset_CA_Xref	Success
Sharepoint - EAP Inventory	Sharepoint - EAP Inventory	NEE.BES_Cyber_System	Success
		NEE.BES_Cyber_System	Success
		NEE.Cyber_Asset	Success
		NEE.Master_Cyber_Asset_Function	Success
		NEE.Master_Device_Type	Success
		NEE.Master_Impact_Rating	Success
		NEE.BES_Asset_CA_Xref	Success
		NEE.BES_Cyber_System	Success
		NEE.Cyber_Asset	Success
		NEE.Master_Cyber_Asset_Function	Success
Sharepoint - PGD	Sharepoint - PGD	NEE.BES_Asset_CA_Xref	Success
		NEE.BES_Cyber_System	Success
		NEE.Cyber_Asset	Success
		NEE.Master_Cyber_Asset_Function	Success
		NEE.Master_Device_Type	Success
		NEE.Master_Impact_Rating	Success
		NEE.BES_Asset_CA_Xref	Success
		NEE.BES_Cyber_System	Success
		NEE.Cyber_Asset	Success
		NEE.Master_Cyber_Asset_Function	Success
Sharepoint - TBC	Sharepoint - TBC	NEE.BES_Asset_CA_Xref	Success
		NEE.BES_Cyber_System	Success
		NEE.Cyber_Asset	Success
		NEE.Master_Cyber_Asset_Function	Success
		NEE.Master_Device_Type	Success
		NEE.Master_Impact_Rating	Success
		NEE.BES_Asset_CA_Xref	Success
		NEE.BES_Cyber_System	Success
		NEE.Cyber_Asset	Success
		NEE.Master_Cyber_Asset_Function	Success



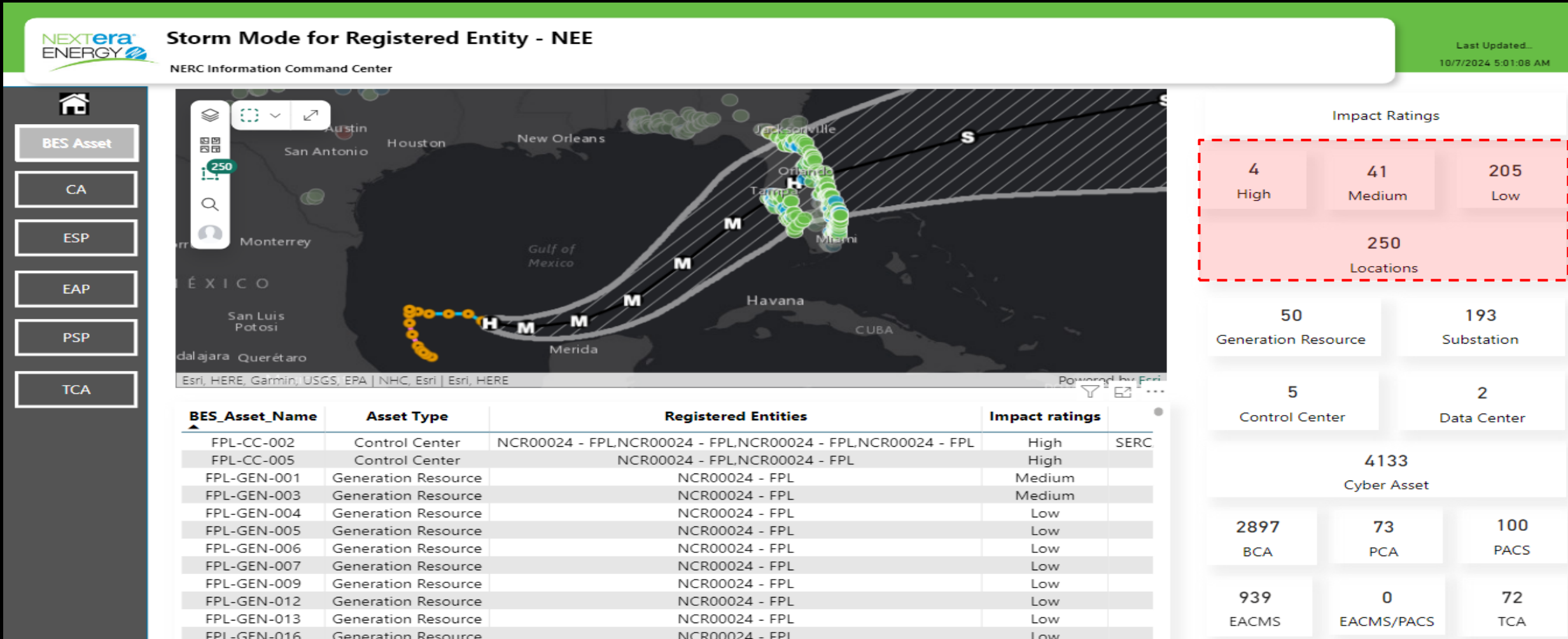
Asset Management

NERC Information Command Center (NICC)

Asset Management – Continuous Monitoring & Audit Support

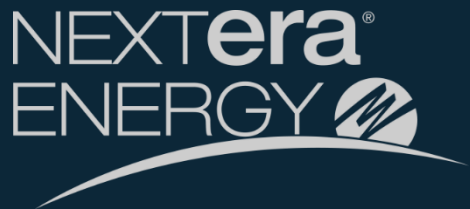


Asset Management – Storm Response

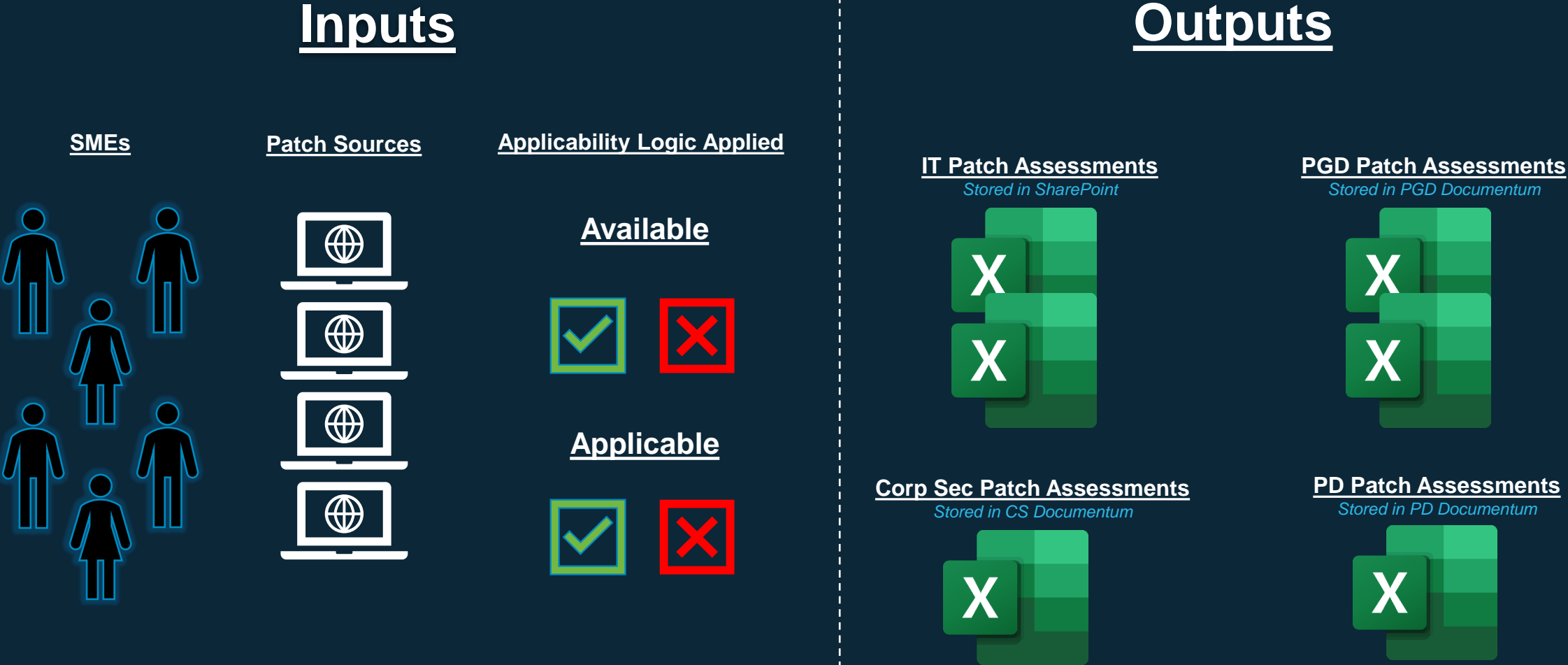


- **Direct feed from NOAA**
- **Overlay with CIP002 – Asset Management Data**
- **Assists with storm response**

Security Patch Management

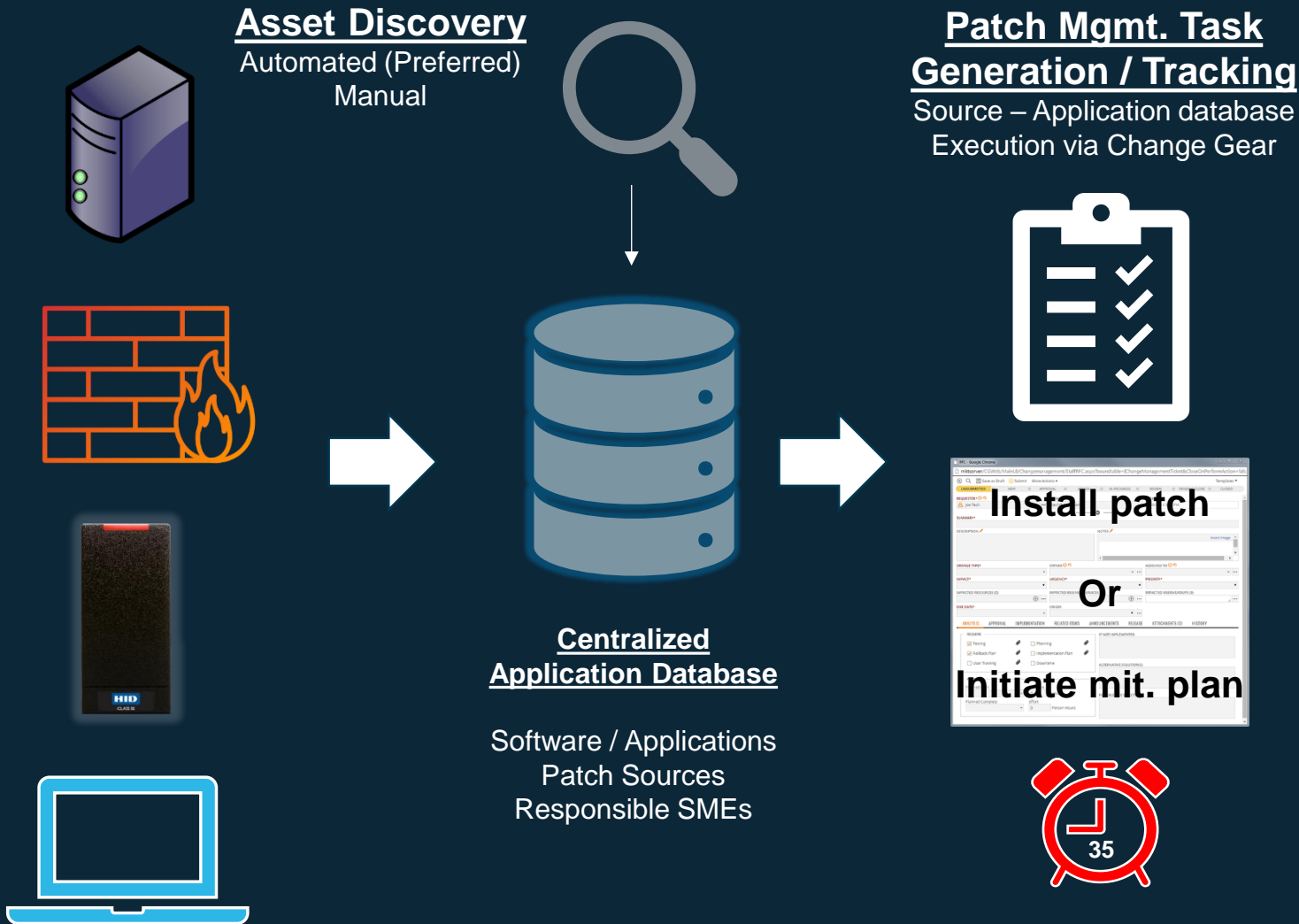


From January 2021 to August 2022, a total of 21 out of 65 samples selected specific to CIP007 R2 – Security Patch Assessments exceeded the 35-day max allowed cycle time by an average of 1-7 days – a 32% Defect Rate!



In 2023, we started an 18-month journey that called for the reimagination of our work tied to Security Patch Assessments and Orchestration.

DMAIC – Analyze / Improve



NERC Information Command Center (NICC)

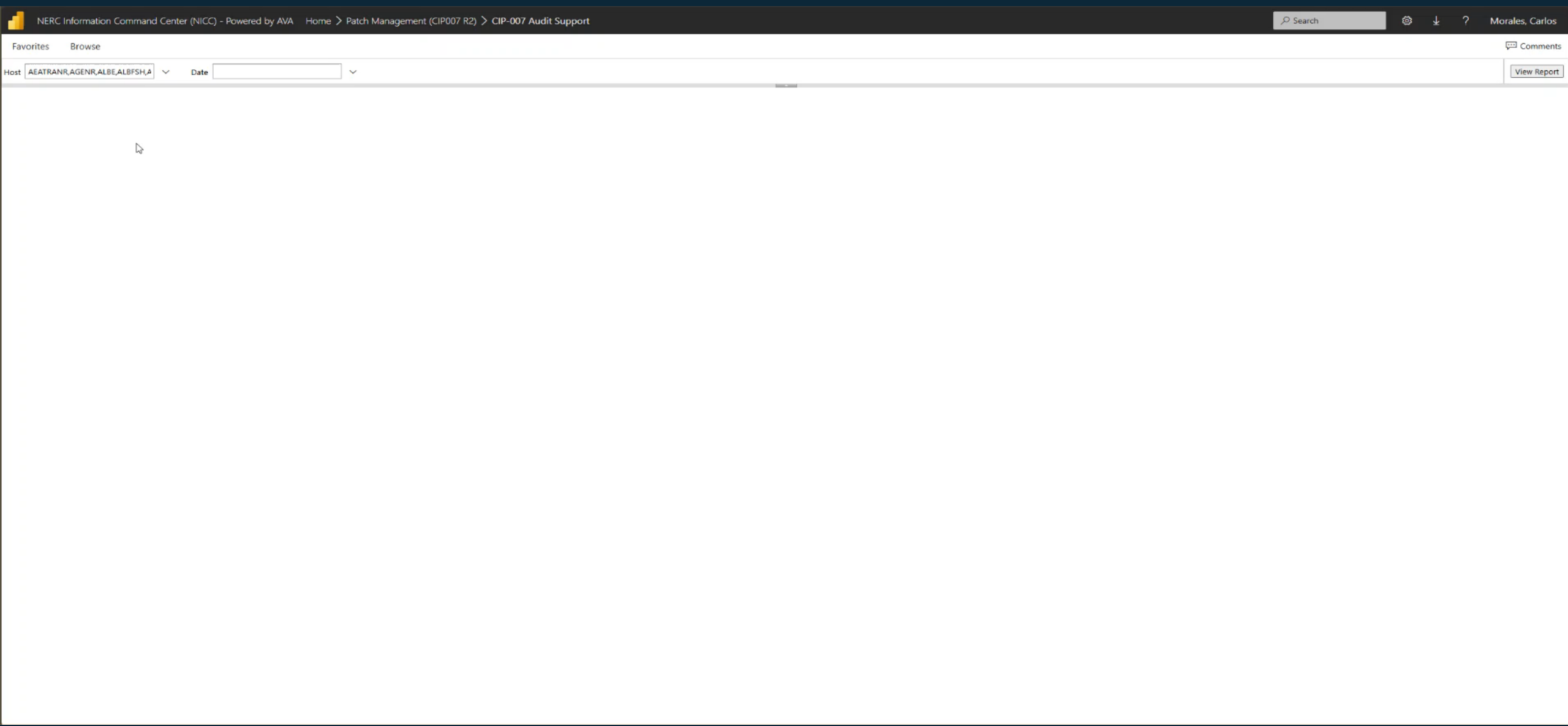
- ✓ Real Time Monitoring
- ✓ Condition Response
- ✓ Trend Analysis
- ✓ Process Execution Evaluation

Our CIP Program is now realizing a **41% decrease in average time to complete patch assessments.**

	<u>June 2024</u>	<u>June 2024</u>	<u>June 2024</u>	<u>July 2024</u>	<u>July 2024</u>	<u>July 2024</u>
	Total Patch Assessments Required to Perform (Opportunities)	Total Patch Assessments Completed (Actuals)	Average Completion Window	Total Patch Assessments Required to Perform (Opportunities)	Total Patch Assessments to Complete (Opportunities)	Average Completion Window
Information Technology	271	271	23 Days	255	255	24 Days
Corporate Security	8	8	25 Days	11	11	17 Days
Power Delivery (TSO)	70	70	23 Days	66	66	24 Days
Power Delivery (GCS)	134	134	22 Days	231	231	21 Days
Power Delivery (PDC)	13	13	24 Days	13	13	25 Days
Power Generation	16	16	25 Days	15	15	23 Days
Totals	512	512	24 Days	591	591	22 Days

NERC requires Patch Assessments to be performed no later than 35 days from the last assessment performed. Historical audit performance also noted that when we realized defects in patch assessment execution, we missed the 35 requirement by an average of 1 and 7 days.

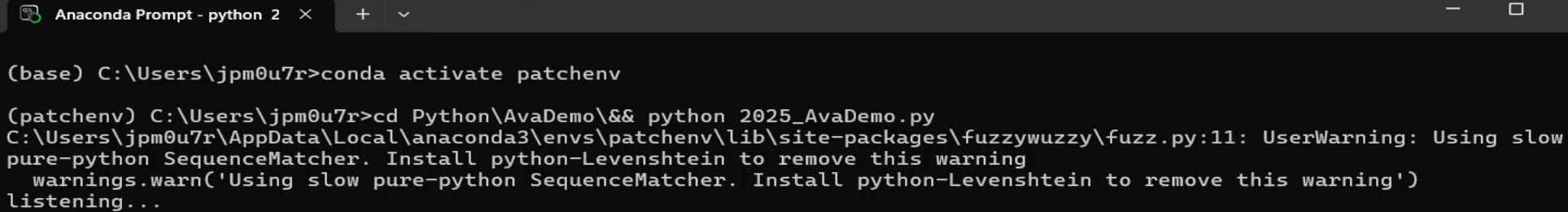
Time to complete NERC's data request tied to patch management went from 6 weeks to 5 days - Over an 80% improvement!



The future of the NERC Information Command Center (NICC) will be powered our AI enabled Advanced Virtual Auditor (AVA).



AVA generates & validates the ERT Workbook required for all NERC CIP Audits along with detecting off-normal conditions tied to task execution!

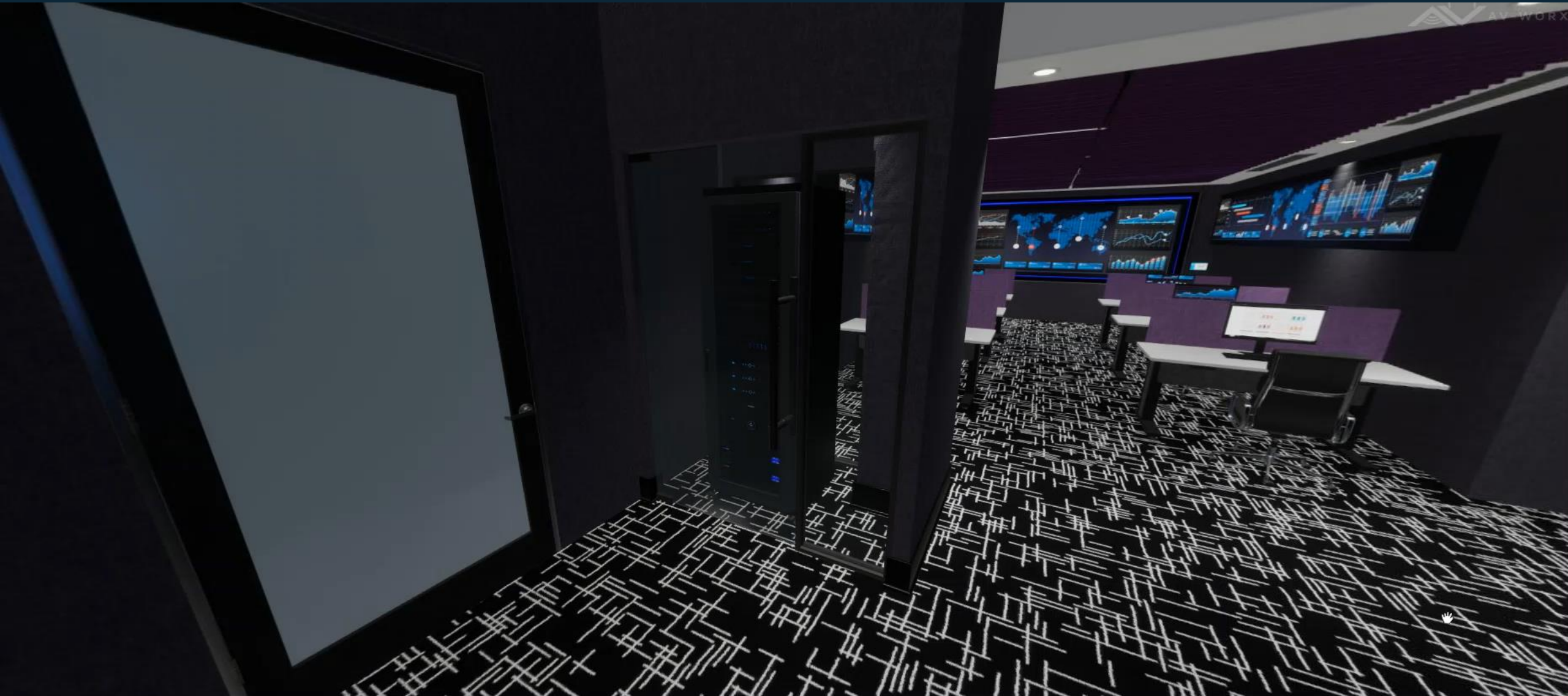


```
Anaconda Prompt - python 2  x  +  v

(base) C:\Users\jpm0u7r>conda activate patchenv

(patchenv) C:\Users\jpm0u7r>cd Python\AvaDemo\&& python 2025_AvaDemo.py
C:\Users\jpm0u7r\AppData\Local\anaconda3\envs\patchenv\lib\site-packages\fuzzywuzzy\fuzz.py:11: UserWarning: Using slow
pure-python SequenceMatcher. Install python-Levenshtein to remove this warning
  warnings.warn('Using slow pure-python SequenceMatcher. Install python-Levenshtein to remove this warning')
listening...
```


NICC 2.0 is coming! We are expanding the existing space to realize our vision of a unified NERC Information Command Center to include both CIP and O&P compliance obligations.



NERC Information Command Center (NICC) Continuous Monitoring Key

1	Automated and Verified Systems: CM involves automated systems that continuously monitor threats, vulnerabilities, and compliance status, ensuring that the collection of data is accurate, complete and up-to-date (NIST SP 800-137, Section 3.1.2).
2	Timely Awareness: The system provides timely notifications about potential issues, allowing prompt responses to threats and vulnerabilities and potential compliance issues (NIST SP 800-137, Section 2.3.2).
3	Real-time Compliance Validation: The CM system validates compliance in real-time, ensuring that the organization meets regulatory and internal standards consistently and is in continuous audit readiness with fully documented evidence sets generated at task completion (NIST SP 800-137, Section 3.1.3).
4	Complete Data Acquisition: A comprehensive data set is gathered, assembled, and contextualized to inform monitoring efforts. This ensures that all relevant information is available for analysis (NIST SP 800-137, Section 3.1.4).
5	Frequent Data Validation: Data is validated frequently to maintain continuous compliance and to provide early detection of emerging issues, thereby allowing for corrective action before any non-compliance or risk becomes significant (NIST SP 800-137, Section 3.1.5).
6	Proactive Auditing: CM enables both internal and external auditors to perform continuous and proactive auditing, using real-time data to test and validate controls more frequently, including the use of an AI Virtual Auditor (AVA) (NIST SP 800-137, Section 3.2.4).
7	Informed Decision Making: The system supports both automated decision-making (through business rules) and complex decision-making requiring human intervention. This leads to timely and informed responses to potential issues (NIST SP 800-137, Section 2.2).
8	Risk Management: CM helps maintain an acceptable risk appetite for the organization by ensuring that processes adhere to established Service Level Agreements (SLAs), and that validation checks are in place at critical process steps (NIST SP 800-137, Section 3.3).
9	Regulatory Cost: Compliance Program Cost Tracking/Long Term Cost Savings / Continuous Improvement

The NICC *Powered by AVA*

Product Module Offerings





HORIZONWEST
TRANSMISSION

NEXtera
ENERGY
TRANSMISSION

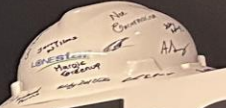
GridLiance

NEXtera
ENERGY
RESOURCES

LONestar
TRANSMISSION

TBC
Trans Bay Cable

NEW HAMPSHIRE
TRANSMISSION



One Team

NERC
Information
Command
Center

Question & Answers

NEXTERA[®]

ENERGY

