



The Cybersecurity Value-at-Risk Framework: Informing Cybersecurity Decisions

Anuj Sanghvi, Cybersecurity Researcher
Jordan Smart, Software Developer
NREL

Contents

1 Project Overview

2 Research Approach

3 Technical Implementation

4 Outlook & Future Work

5 Q&A

Cybersecurity Value-at-Risk Framework Project Overview

- Leverages the architecture of the Distributed Energy Resources Cybersecurity Framework (DER-CF) – www.dercf.nrel.gov
- Targets the risk management process to prioritize action items and associated investments
- Considers various impacting factors such as environmental, economical, safety and operations risks
- Calculates risk, impact, and cyber-resilience scores for determining value at risk
- Prioritizes risk-based recommendations to enhance decision-making

Research Approach

Literature review, scoping, and asset identification

Resources

- Institute of Electrical and Electronics Engineers (IEEE) 1020, *Guide for Control of Small Hydroelectric Power Plants*
- IEEE 1010, *Guide for Control of Hydroelectric Power Plants*
- International Electrotechnical Commission (IEC) 31010, *Risk Assessment Techniques*
- IEC 62270, *Guide for Computer-Based Control for Hydroelectric Power Plant Automation*
- *Dams Sector Cybersecurity Capability and Maturity Model*

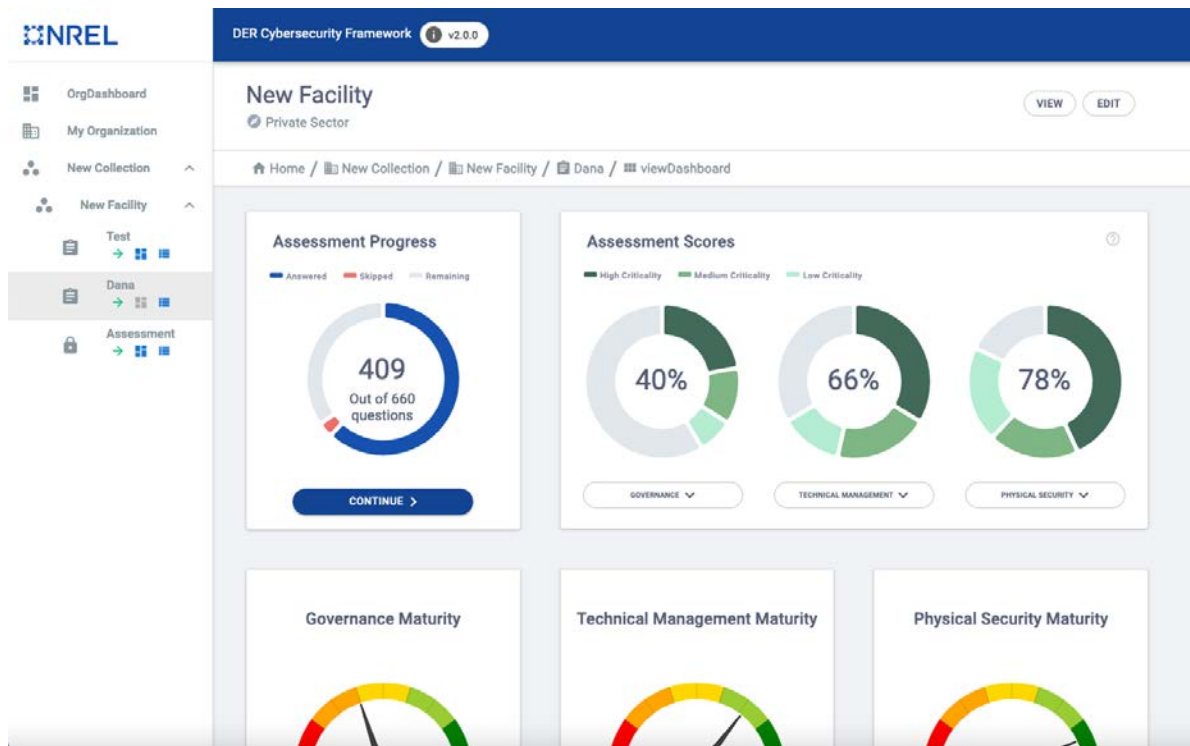
Advancing Cybersecurity Risk Assessment

Moving from
maturity-based
scoring to
semiquantitative
risk calculations

DER-CF

Pillar → Domain → Subdomain Model

Answer types/follow-ups and recommendations



Step 1: Hydropower Focused Operations and Assets

- Identify mission-critical hydropower systems
- Highlight areas of cyber concern for hydropower plant operations
- Scope assets that may be vulnerable to cyberattacks

Hydropower Operations	Discipline and Assets	Critical Cyber Assets
Water Conveyance Operation	Gates, penstock, inlet valve, hydraulic actuators, water flow meter	Inlet valve/gate operation system, spill gate control system, powerhouse drainage system, water injection and wicket gate system, remote gate and dam operation system
Generator	Generator rotor and stator, exciter, protective relay, cooling water, air injection, CO2 fire suppression, alarm system, governor	Condition monitoring system, vibration monitoring system, generation load control, generator circuit breaker, protective relay system, alarm system, governor control system
Turbine	Mechanical-Turbine, Electrical-Turbine sensor	Speed sensor, hydro turbine control system, turbine shaft vibration monitoring system
Automation, Control and Protection	Supervisory system, networking equipment, HMI, emergency shutdown system	Speed control and brake monitoring system, routers, switches, gateway devices (firewall, IDS/IPS), controller communication modules, fire and overspeed protection
Substation Operation	Circuit switches, surge arrestor, transformers, line switches	Remote terminal unit, programmable logic controller, protective device, HMI, gateway device
Plan Auxiliary System	Station lighting DC system-UPS and battery Diesel and battery generator	Lighting plant control system, plant security system Plant DC monitoring system Diesel generator monitoring system

Step 2: Impacts and Likelihood Categories

Impact

- Safety
- Environmental
- Economical
- Operational

Generic Control Catalog

Are commonly used **ports disabled** when not used or changed to site-specific port numbers? Examples include 80 (HTTP), 53 (DNS), 23 (TELNET), 161 (SNMP), 502 (MODBUS), 20000 (DNP3), and 44818 (Ethernet/IP).

Is the **operation technology (OT) specific data encrypted or at least password protected**? Examples include schematics, diagrams, control system layouts, etcetera stored either on workstations or databases

Are control system devices' **default credentials changed to more secure credentials** before being deployed in production environment?

Is there a **robust patch management policy** and control in place where patches to OT/control system devices are first tested in a sandboxed/virtual system environment to identify undiscovered vulnerabilities?

Are **secure coding practices** used to prevent malicious code consisting of configuration to inject project files? For ex: Code signing, encryption of sensitive information, restriction of files and directory permissions.

Are operational servers and other critical functional components **regularly backed up**? Are those backups offline or offsite, and do you regularly **prove the ability to restore** operations?

Likelihood Factor	Sub-category	Description
Location	Local	Asset is within boundary/sight of equipment
	Centralized	Asset is remote from controlled equipment, but within the plant
	Off-site	Asset is in a remote location from the plant
Operation Mode	Manual	Each operation needs a separate and deliberate initiation
	Automated	Two or more operations can be started by a single command or initiation
Staff Attendance	Attended	Operator must be physically available to initiate action
	Unattended	Operator can initiate control while off-site

Likelihood Descriptions

Factors affecting the calculation of cyberattack likeliness

Step 3: Define, Assign, and Validate Weighted Values

Security Control Attributes and Metadata

- Establish values and associated weights
- Threat activation mechanism
- Likelihood score depending on operation modes
- MITRE's ATT&CK¹ for industrial control systems (ICS)
 - Tactics, techniques, and procedures → assets
→ vulnerability → mitigation*
- Impact considerations to address priorities
- Value-at-risk calculation to inform the need to invest resources

Assessment Structure

Domain expansion for hydropower assessment

Domain	Subdomain
Critical Operations	Maintenance Plant Operations Generic Controls Safety
Management	Risk Management Asset Management Identity Management Policies/Procedure Training Communication Networks Personnel/Leadership
Site and Service Control	Physical Protection Access Control Monitoring Information Protection
Dependencies	Grid Operation Business Endpoint Data

CVF 2.0 Technical Implementation

DER-CF Extension and Additional
Functions in the Tool

Assessment Controls

Pillar -> Domain -> Subdomain -> Controls

- Impact level
- Action Items
- Metrics
 - NIST CSF Category
 - CIA Triad
 - Impact Category
 - Consequence Category
 - Feasibility

Assessment Scores

The screenshot displays the NREL Cybersecurity Value-at-Risk Framework v2.0.0 interface. The left sidebar contains navigation options: OrgDashboard, My Organization, Flatiron Campus, ESIF, test, IT Up, Base Line, and Table Mesa Campus. The main header shows the framework name and version, along with a user profile 'wtpqg'. The central progress bar indicates that the 'Management' category is 100% complete, with 'Leadership & Personnel' being the current focus. Below the progress bar, a breadcrumb trail reads: Home / Flatiron Campus / ESIF / test / Categories / Hydropower Valuation Assessment / Management. A red box highlights a specific assessment question: 'Is there a manager/department in charge of day-to-day cybersecurity management of the entire facility? test'. The response is 'Yes'. Other visible questions include 'Can resources be relocated physically? (i.e. a backup facility)' with 'False' selected, and 'Can critical assets be physically relocated to limit future or further damage?' with 'True' selected. Each question has associated icons for help, info, and completion, as well as buttons for 'ROLES' and 'COMMENT'.

Multiple Facilities and Multiple Assessments

The screenshot shows the NREL Cybersecurity Value-at-Risk Framework v1.0.0 interface. The left sidebar contains a navigation menu with items: OrgDashboard, My Organization, Flatiron Campus, ESIF, IT Upgrade, Base Line, test, Table Mesa Campus, and Hydro. The main content area displays 'NREL Collections' with a table listing collections for Flatiron Campus, ESIF, Table Mesa Campus, and Hydro. Each collection has a plus icon for adding, a pencil icon for editing, and a red minus icon for deleting. An 'ADD COLLECTION' button is located at the top right of the table.

Collection Name	Actions
Flatiron Campus	+ / ✎ / -
ESIF	+ / ✎ / -
Table Mesa Campus	+ / ✎ / -
Hydro	+ / ✎ / -

The screenshot shows the NREL Cybersecurity Value-at-Risk Framework v2.0.0 interface for the 'Hydro' facility. The top section, 'Comparative Analysis', displays a message: 'There are not enough assessments to compare. Complete 2 or more assessments to more than 50% for comparative analysis.' Below this, the 'Assessments' section shows a table with one entry: 'Base Line' (Tuesday, Apr 16, 2024). Underneath, the 'Assessment Scores' section features four donut charts representing different security domains: Manufacturing (71%), SITE AND SERVICE CONTROL SECURITY (66%), Critical Operations (0%), and Information (100%). A legend indicates the score ranges: High Impact (red), Medium Impact (orange), Low Impact (green), and Unrated/Assessed (dark green). At the bottom, there are buttons for 'ASSESSMENT', 'DASHBOARD', 'ACTION ITEMS', and 'DELETE'.

Assessment Name	Date
Base Line	Tuesday, Apr 16, 2024

Domain	Score
Manufacturing	71%
SITE AND SERVICE CONTROL SECURITY	66%
Critical Operations	0%
Information	100%

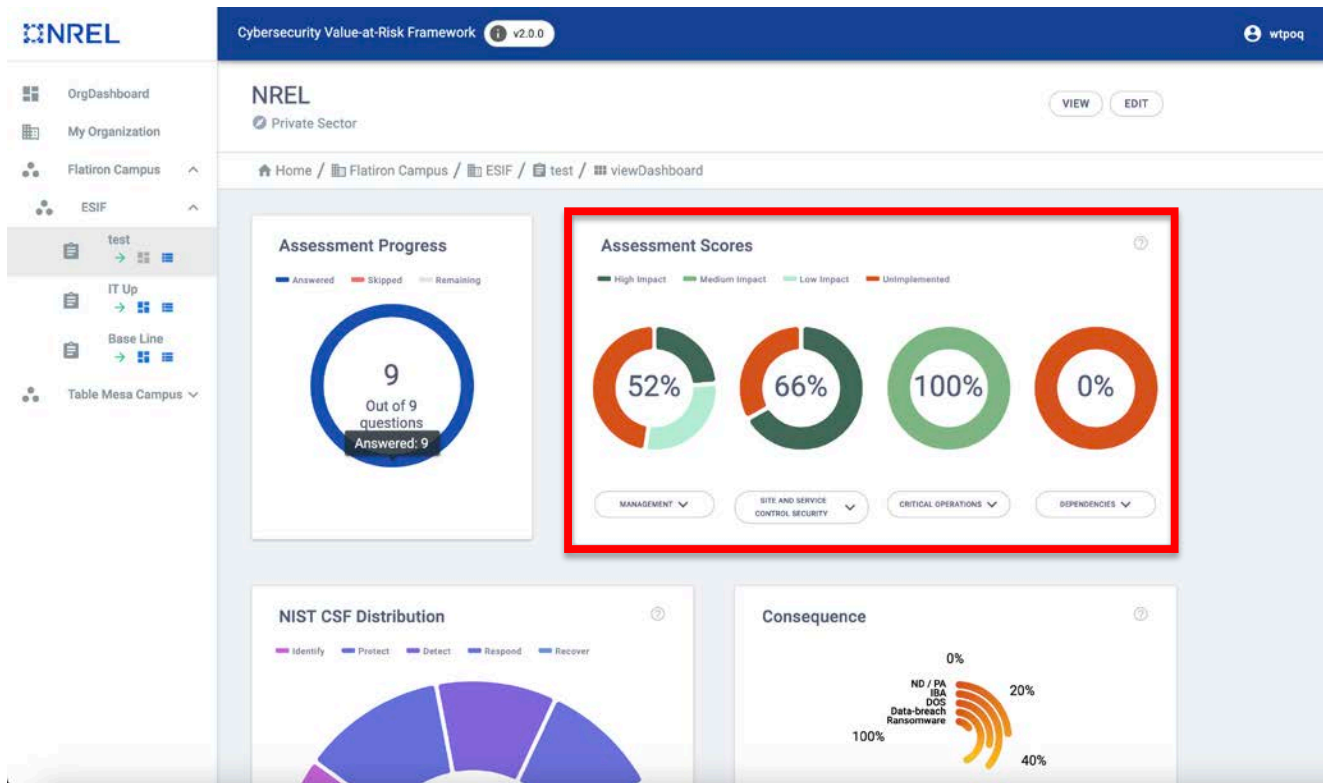
Assessment Scores

The screenshot displays the NREL Cybersecurity Value-at-Risk Framework interface. A modal window titled "Edit Facility Details" is open, highlighted with a red border. The modal contains the following fields and options:

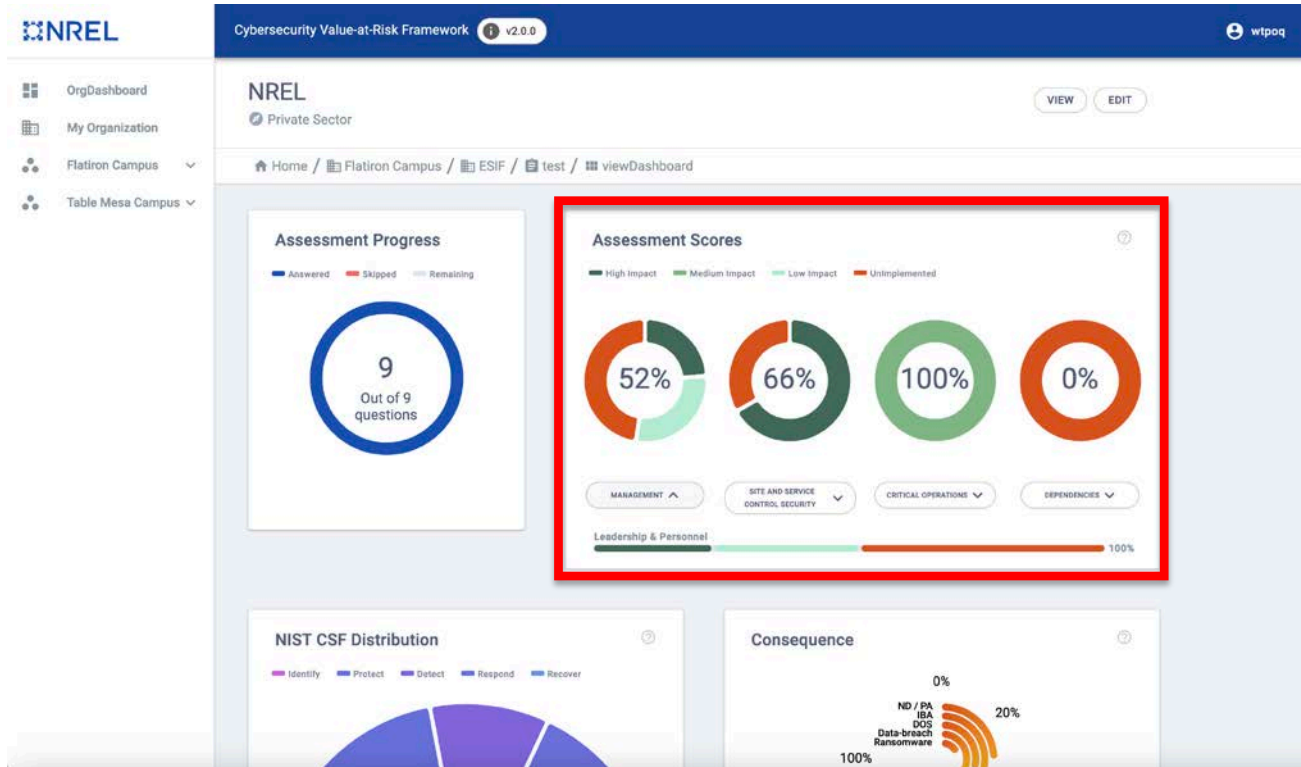
- Name:** ESIF
- Sector:** Private Sector
- Security Level:** High (III)
- Location (Country):** USA
- LEED Certification:** Silver
- Facility Type:** (empty field)
- DERS Power Generation (MW):** (empty field)
- Facility Size:** (empty field)
- Number of Cyber Employees:** (empty field)
- Authority to operate:** Authority to operate
- Federal:** Federal

Buttons for "CANCEL" and "SUBMIT" are located at the bottom of the modal. The background interface shows a sidebar with navigation options like "OrgDashboard", "My Organization", "Flatiron Campus", "ESIF", "test", "IT Up", "Base Line", and "Table Mesa Campus". The main content area displays "Facility Information" with fields for NAME, SECTOR, AUTHORITY TO OPERATE, FEDERAL, FSL LEVEL, LOCATION, LEED CERTIFICATION, FACILITY TYPE, POWER GENERATION, FACILITY SIZE, and # OF EMPLOYEES. An "EDIT INFORMATION" button is visible at the bottom of this section.

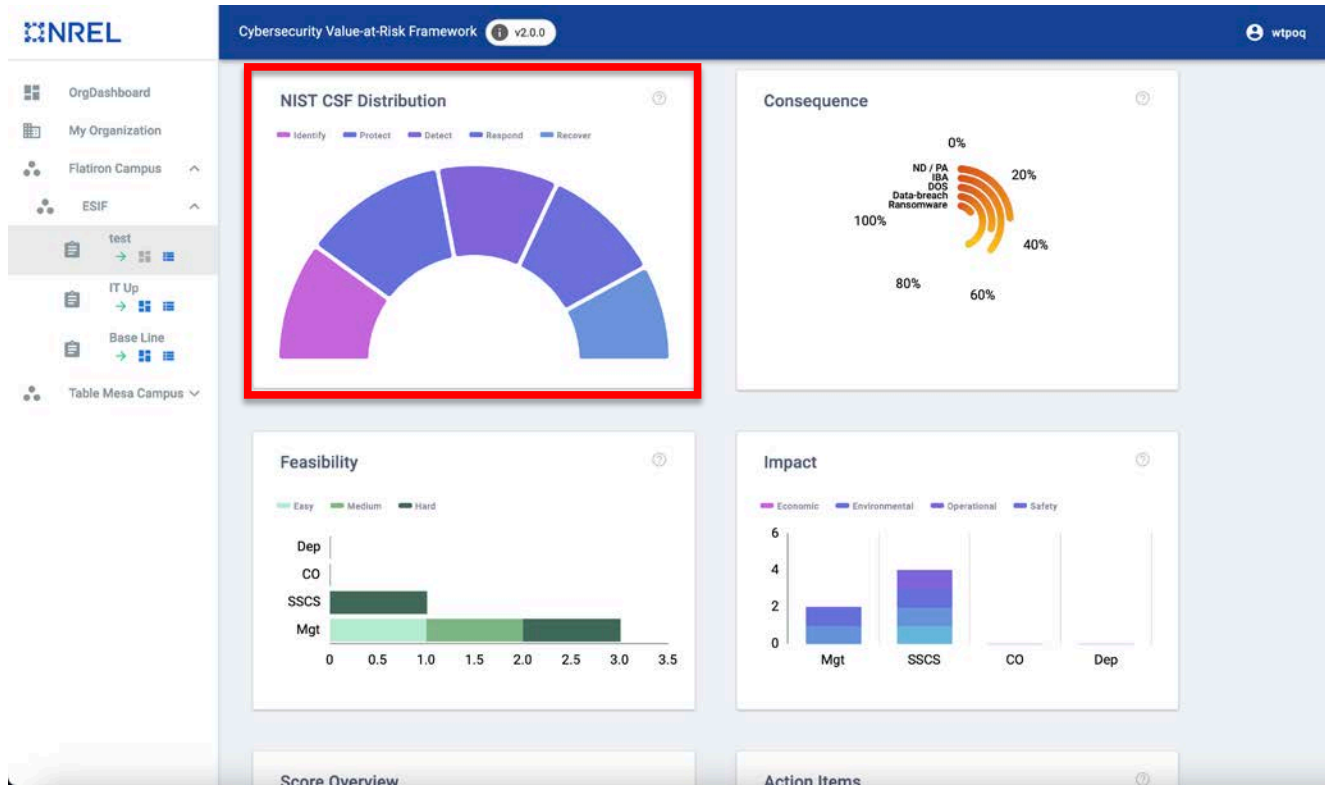
Assessment Scores



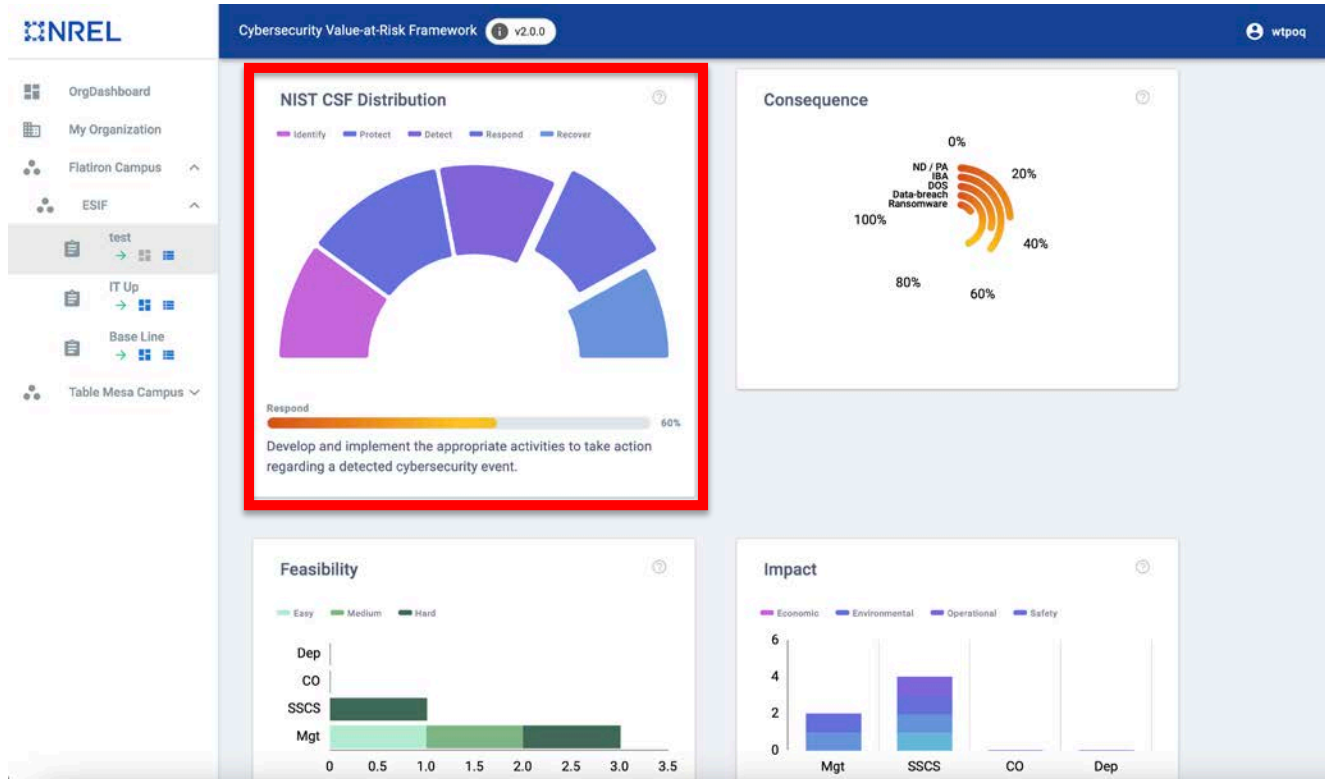
Assessment Scores



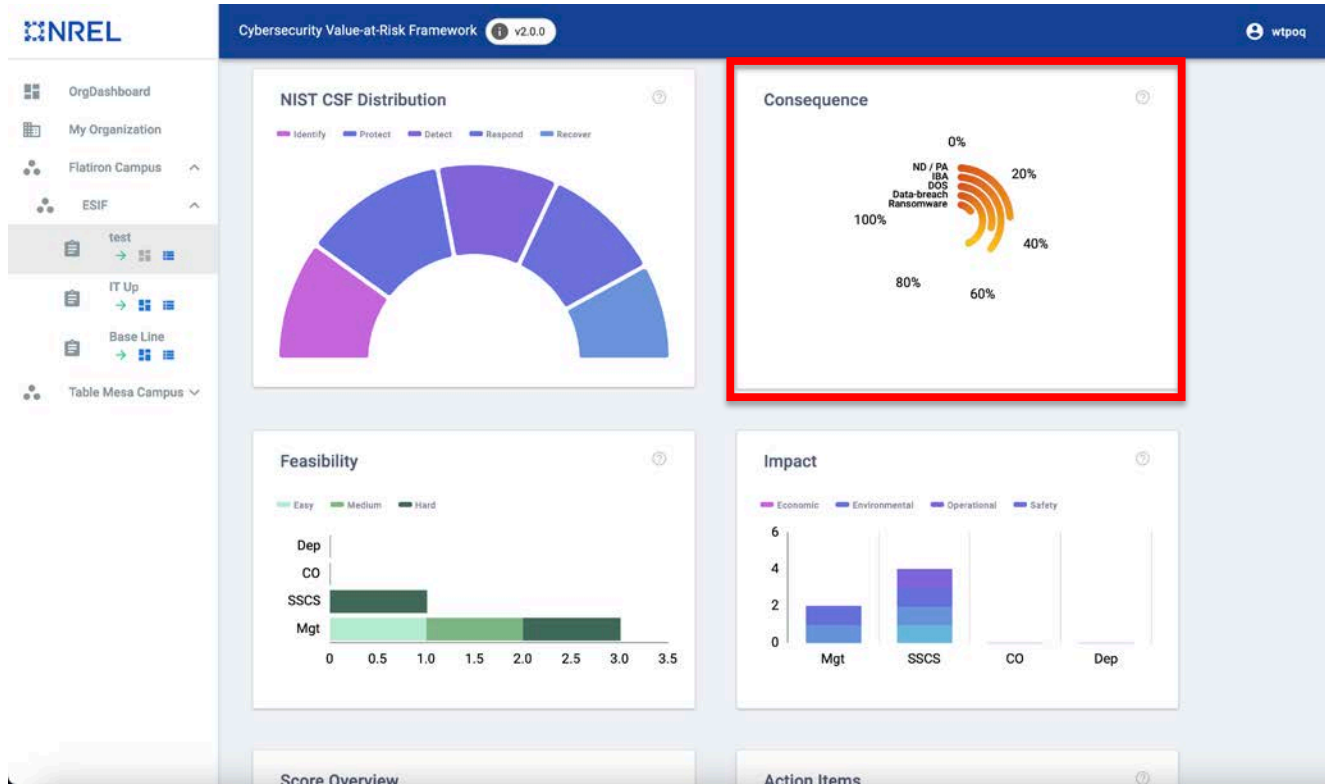
NIST CSF Distribution



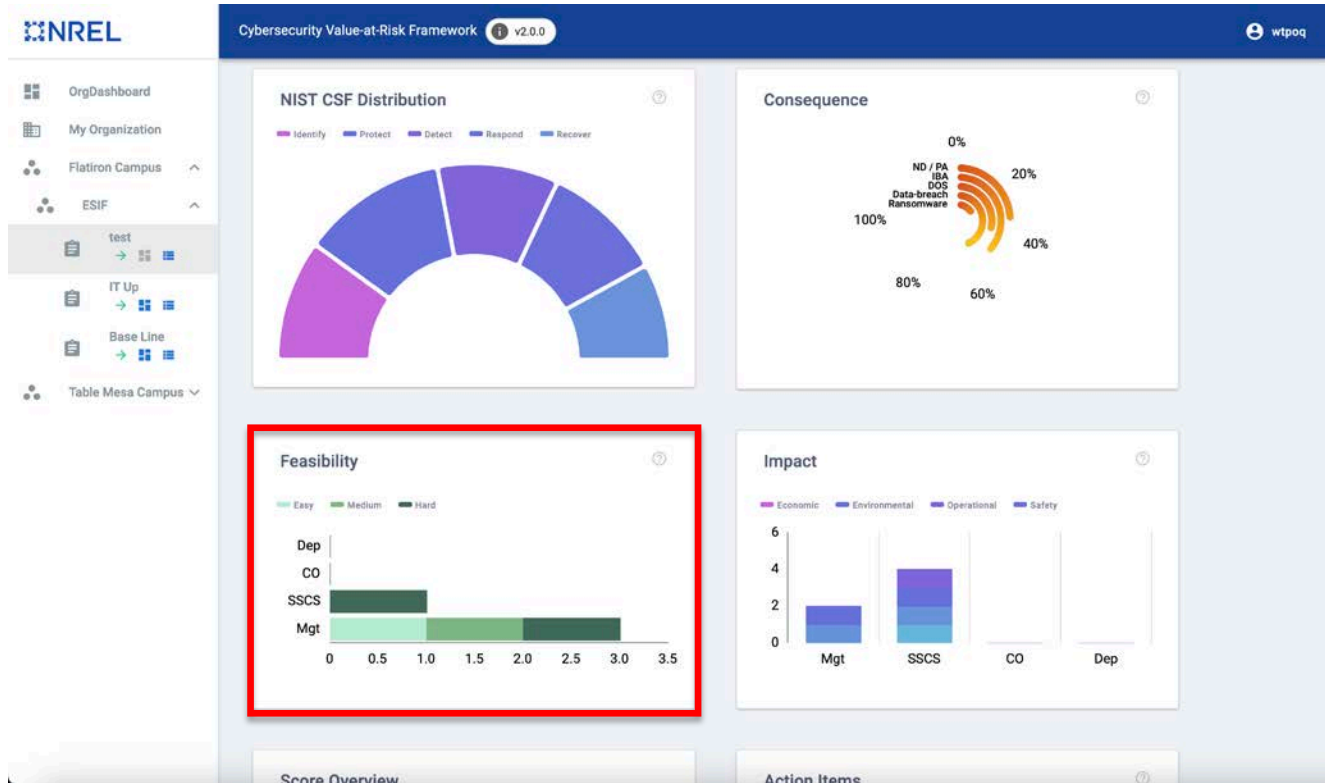
NIST CSF Distribution



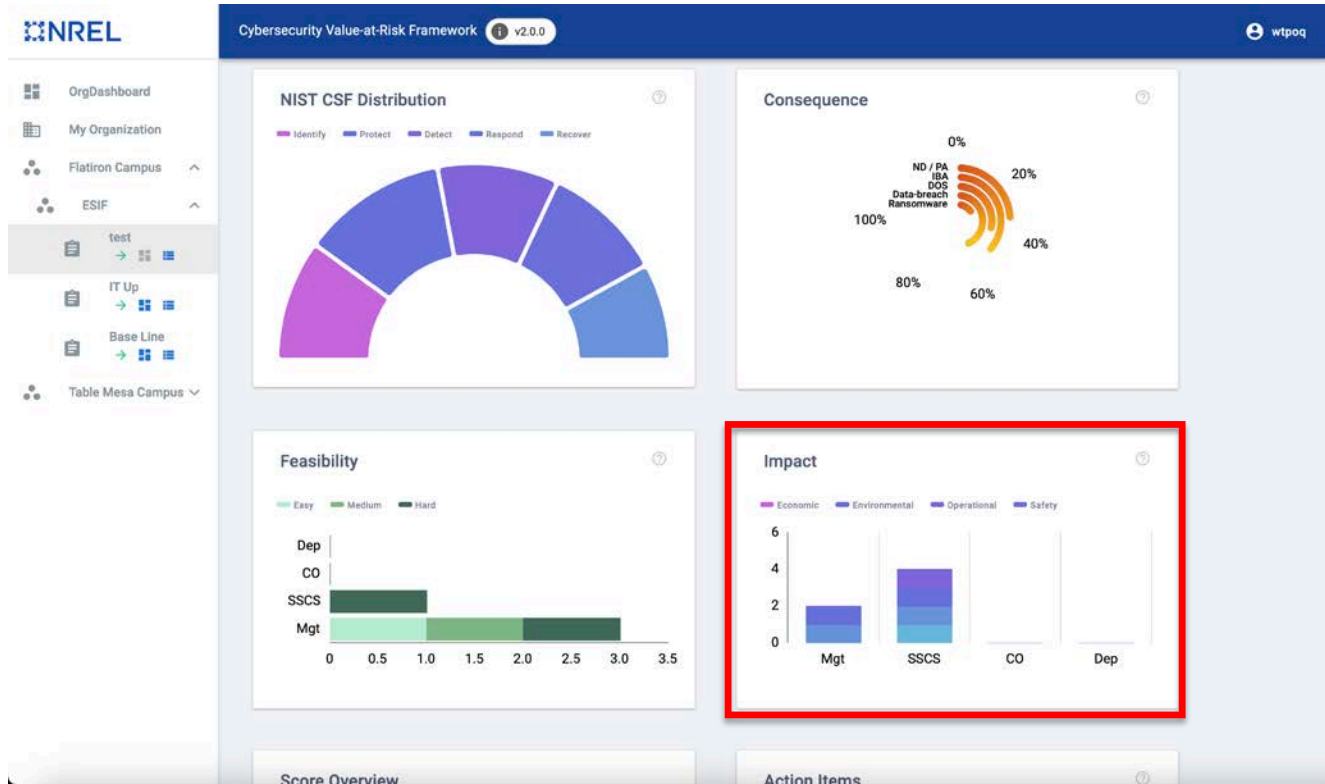
Consequence



Feasibility



Impact



Scores Overview

NREL Cybersecurity Value-at-Risk Framework v2.0.0 wtpq

OrgDashboard
My Organization
Flatiron Campus
ESIF
test
IT Up
Base Line
Table Mesa Campus

Score Overview

Impact is the overall score of what impacts could be present.

Control implementation: User's implementation of a control represents unmitigated risks

Likelihood: This is the probability of an attack/event occurring and resulting in above mentioned impact

Value-at-Risk score: VaR intends to signify a quantitative score directly proportional to the need for resources (workforce/funding /tools) which is based on facility's risk posture.

Control Implementation: Acceptable implementation with score: 0.636

Impact: Poor implementation with score: 0.275

Likelihood: High probability to cause Impact with score: 0.9

Value-at-Risk: Moderate necessity to invest resources (workforce/funding/tools) to mitigate associated risks with score: 0.09

Action Items

Percent	Count	Status
0%	0	Not Started
0%	0	In Progress
0%	0	In Review
100%	1	Complete

ALL ACTION ITEMS >

CVF Assessment Report

COMPILE REPORT

Action Items

NREL Cybersecurity Value-at-Risk Framework v2.0.0 wtpq

OrgDashboard
My Organization
Flatiron Campus
ESIF
test
IT Up
Base Line
Table Mesa Campus

Score Overview

Impact is the overall score of what impacts could be present.

Control implementation: User's implementation of a control represents unmitigated risks

Likelihood: This is the probability of an attack/event occurring and resulting in above mentioned impact

Value-at-Risk score: VaR intends to signify a quantitative score directly proportional to the need for resources (workforce/funding /tools) which is based on facility's risk posture.

Control Implementation: Acceptable implementation with score: 0.636

Impact: Poor implementation with score: 0.275

Likelihood: High probability to cause Impact with score: 0.9

Value-at-Risk: Moderate necessity to invest resources (workforce/funding/tools) to mitigate associated risks with score: 0.09

Action Items

Percent	Count	Status
0%	0	Not Started
0%	0	In Progress
0%	0	In Review
100%	1	Complete

ALL ACTION ITEMS >

CVF Assessment Report

COMPILE REPORT

Actions Items

NREL Cybersecurity Value-at-Risk Framework v2.0.0 wtpog

Action Items

HYDROPOWER VALUATION ASSESSMENT

Impact: High Medium Low

Home / Flatiron Campus / ESIF / test / viewActionItems

Domain	Status	Percentage
Management		
Site and Service Control Security	1 0 0 0	0%
Physical Protection	High impact	
Critical Operations		

Physical Protection High impact

Action: To be able to have critical assets and functionality continuously maintained without interruption in service should the main facility become compromised.

Write a new comment...

NOT STARTED

Actions Items

NREL Cybersecurity Value-at-Risk Framework v2.0.0 wtpoq

Action Items

DOWNLOAD ALL

HYDROPOWER VALUATION ASSESSMENT

Impact: High Medium Low

Home / Flatiron Campus / ESIF / test / viewActionItems

Domain	Status	Percentage
Management		
Site and Service Control Security	0 0 0 1	100%
Physical Protection		High impact

Physical Protection High impact

Action: To be able to have critical assets and functionality continuously maintained without interruption in service should the main facility become compromised.

New Comment

Write a new comment...

COMPLETE

Report Widget

NREL Cybersecurity Value-at-Risk Framework v2.0.0 wtpq

OrgDashboard
My Organization
Flatiron Campus
ESIF
test
IT Up
Base Line
Table Mesa Campus

Score Overview

Impact is the overall score of what impacts could be present.

Control implementation: User's implementation of a control represents unmitigated risks

Likelihood: This is the probability of an attack/event occurring and resulting in above mentioned impact

Value-at-Risk score: VaR intends to signify a quantitative score directly proportional to the need for resources (workforce/funding /tools) which is based on facility's risk posture.

Control Implementation: Acceptable implementation with score: 0.636

Impact: Poor implementation with score: 0.275

Likelihood: High probability to cause Impact with score: 0.9

Value-at-Risk: Moderate necessity to invest resources (workforce/funding/tools) to mitigate associated risks with score: 0.09

Action Items

Percent	Count	Status
0%	0	Not Started
0%	0	In Progress
0%	0	In Review
100%	1	Complete

ALL ACTION ITEMS >

CVF Assessment Report

COMPILE REPORT

Assessment Report

Executive Summary

The National Renewable Energy Laboratory (NREL) developed the Hydropower Cybersecurity Value-at-Risk Framework (CVF) and web application. The web-based tool assists reliability, energy management teams by walking the user through an assessment framework and bringing guidance and structure to the extensive array of cybersecurity controls applicable to hydropower plant resources. The assessment covers several domains containing multiple layers that address key cybersecurity topics and create a robust and flexible framework specifically designed for the hydropower fleet, domains containing multiple layers that address key cybersecurity topics and create a robust and flexible framework specifically designed for the hydropower fleet.

This report summarizes a completed assessment and contains sensitive, detailed information regarding ESIF's cybersecurity posture according to the CVF. Additionally, the appendices of this document contain customized and prioritized recommendations to begin creating a more secure environment. This document should serve as an ongoing reference during the development and improvement of cybersecurity and investment practices.

Importance of Cybersecurity Assessment

scoring methodology. The rapid migration of the public and private sector to a digital economy has made the risk of cyberattacks extremely high in recent years. The business continuity of an enterprise is now strongly dependent on the strength of its cybersecurity controls, cybersecurity awareness of its employees and contractors and standard business processes that minimize exposure to attacks. The cost to an organization for a cybersecurity incident on a critical hydro-power system can include direct financial loss, physical damage, severe reputation impact, and even loss of life. These consequences influence other impact categories such as environmental, economic, safety, and operational. Hydropower plants face numerous challenges in making informed decisions in managing systems and maintaining systems to ensure continuity of operations. Regular cybersecurity assessments that enable a risk-based approach to allocating resources and improving the overall cybersecurity posture of the organization is paramount in ensuring the security and resiliency of hydropower facilities. CVF was built to enable a comprehensive and periodic cybersecurity risk assessment that informs investment decisions. The National Institute of Standards and Technology (NIST) frameworks serve as reference guides in building the CVF assessment structure as well as the scoring methodology.

The remainder of this report is organized to provide a high-level summary followed by more detailed analysis of weak points categorized by CVF assessment, as well as their domains and subdomains.

Results Summary

ESIF completed the cybersecurity valuation assessment on 2024/10/24. The Value-at-Risk score from the assessment was Moderate necessitate invest resources (workforce/funding/tools) to mitigate associated risks with score: 0.09. This score is calculated by the CVF application based on the collective responses from the ESIF representatives that participated in the assessment. This suggests that the ESIF cybersecurity Value-at-Risk (VaR) score is at a Moderate necessitate invest resources (workforce/funding/tools) to mitigate associated risks with score: 0.09 and there is opportunity for considerable improvement over the next 6-12 months across multiple domains if the actions described in Appendix B are completed. Below is a summary of the four posture levels based on VaR score (where lower scores are better):

- **Low:** The facility has a stronger posture with some room for improvements. There is a lower need to invest resources (workforce/funding/tools).
- **Moderate:** The facility has a good foundation in terms of cybersecurity practices. There is a moderate need to invest resources (workforce/funding/tools) and management should prioritize resource allocation accordingly to mitigate associated risks.
- **High:** A weak foundation in cybersecurity practices. There is a higher need to invest resources (workforce/funding/tools) and management should prioritize resource allocation accordingly to mitigate associated risks.
- **Extreme:** There are no cybersecurity practices in place. There is an extreme need to invest resources (workforce/funding/tools) and management should prioritize resource allocation accordingly to mitigate associated risks.

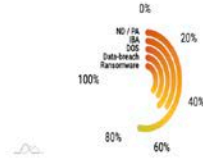
What is affecting my score?

It's critical to understand the immediate shortcomings of your cybersecurity score. This is caused by a combination of unanswered questions, which inhibit the potential to score points, and weak answers to questions with a high impact. Impact is defined as the importance a particular control has the rest of your security posture, and are categorized by low, medium, or high. Medium and high impact designated controls will have a greater impact on your score if not implemented.

Assessment Report

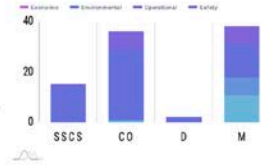
Consequences

Consequences are the effects of having a control not implemented or partially implemented. There are five consequences that are attributed to each of the controls: Denial of service, Natural disaster/Physical Attack, Integrity based attack, Data breach, and Ransomware. The graph to the right shows the breakdown of My Facility's consequence likelihood breakdown based on answers in the assessment.



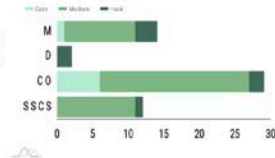
Impact Category

Impact category is the classification of where a particular impact may happen if a cyber attack were to occur. The breakdown of the chart is by domain, with different categories that we have defined as most applicable to this assessment: Economic, Environmental, Operational, and Safety. My Facility can see the breakdown of how the answers of the assessment relate to what potential impacts the facility may have in case of a cyberattack.



Feasibility

Feasibility is defined as how much resources will it take to implement a particular control. It is broken down into three different tiers: Easy, Medium, and Hard. Easy means that the control will require no existing process, and cost little to no money to implement. Medium means that a control will require multiple inputs from multiple personnel and may cost a significant amount. High means that a control will require a significant lift requiring multiple inputs from personnel and require a significant cost. My Facility can see how their facility breaks down in terms of how difficult controls will be to implement.



OrgDashboard



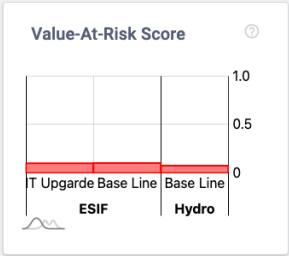
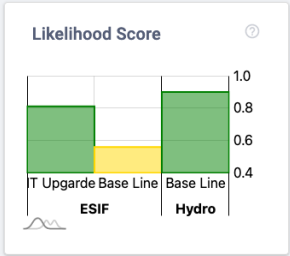
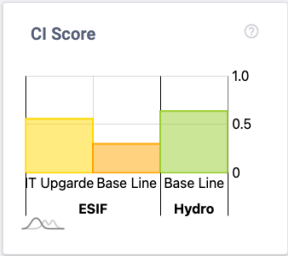
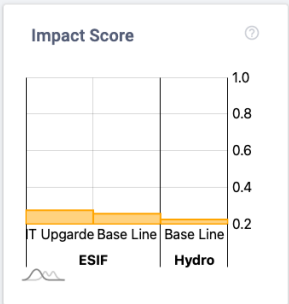
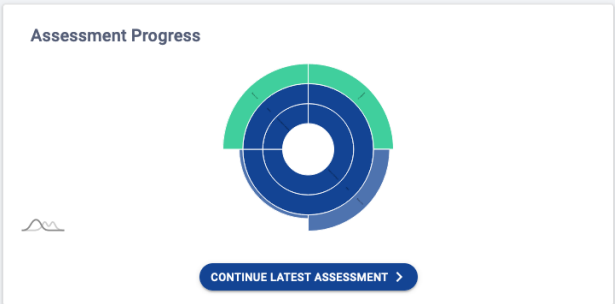
- OrgDashboard
- My Organization
- Flatiron Campus
- ESIF
 - IT Upgarde
 - Base Line
 - test
- Table Mesa Campus
- Hydro
 - Base Line

NREL

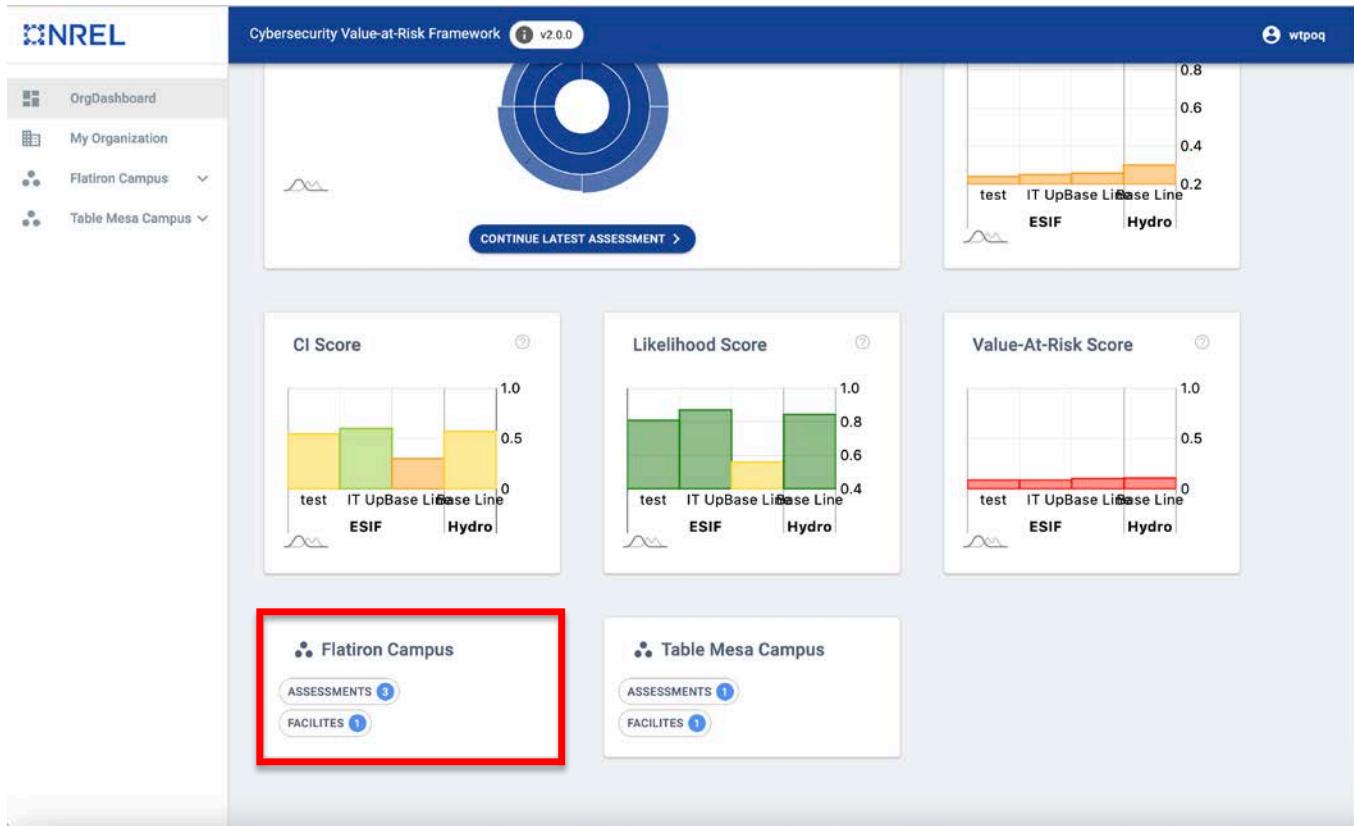
Private Sector

VIEW EDIT

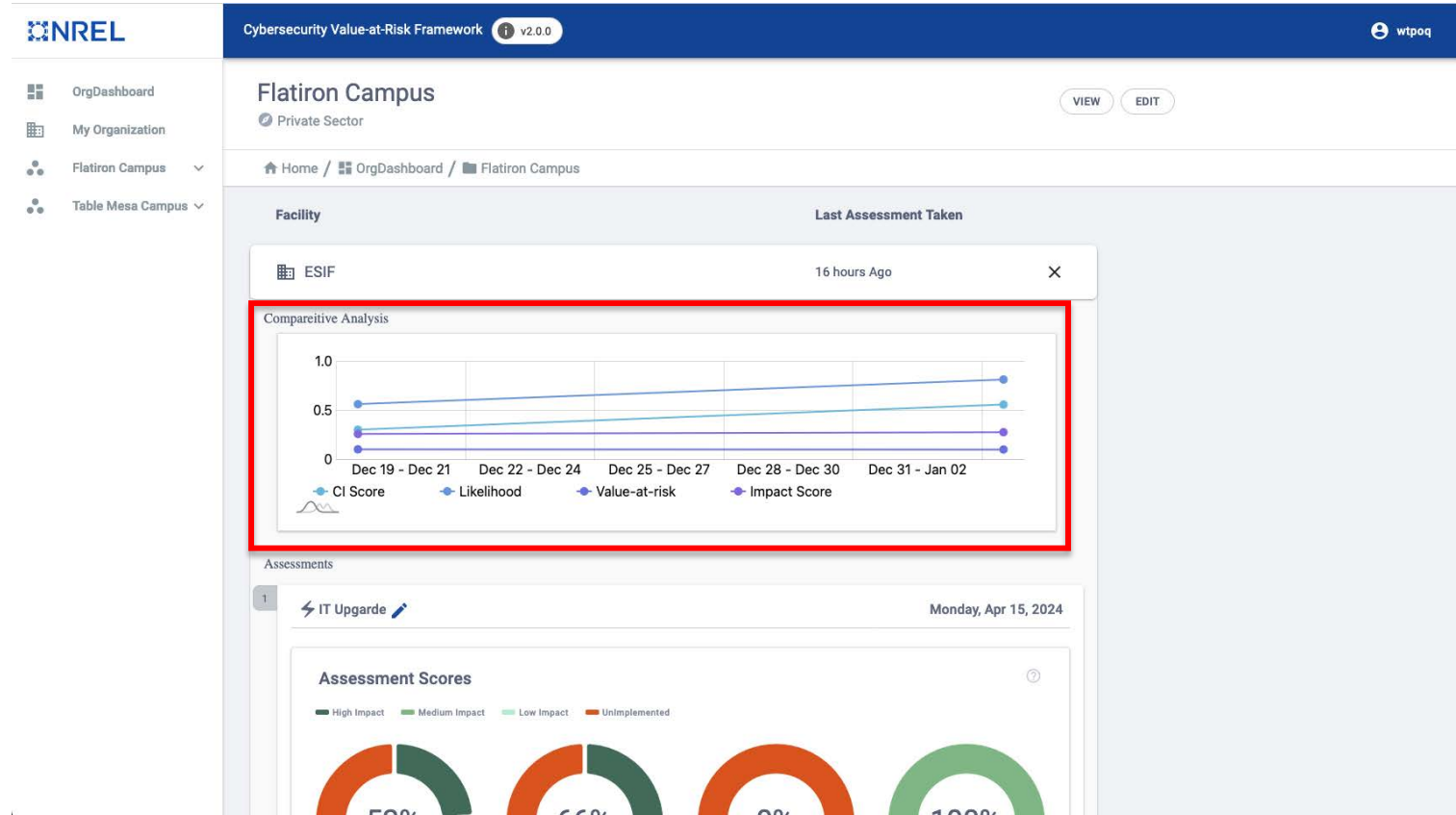
Home / OrgDashboard



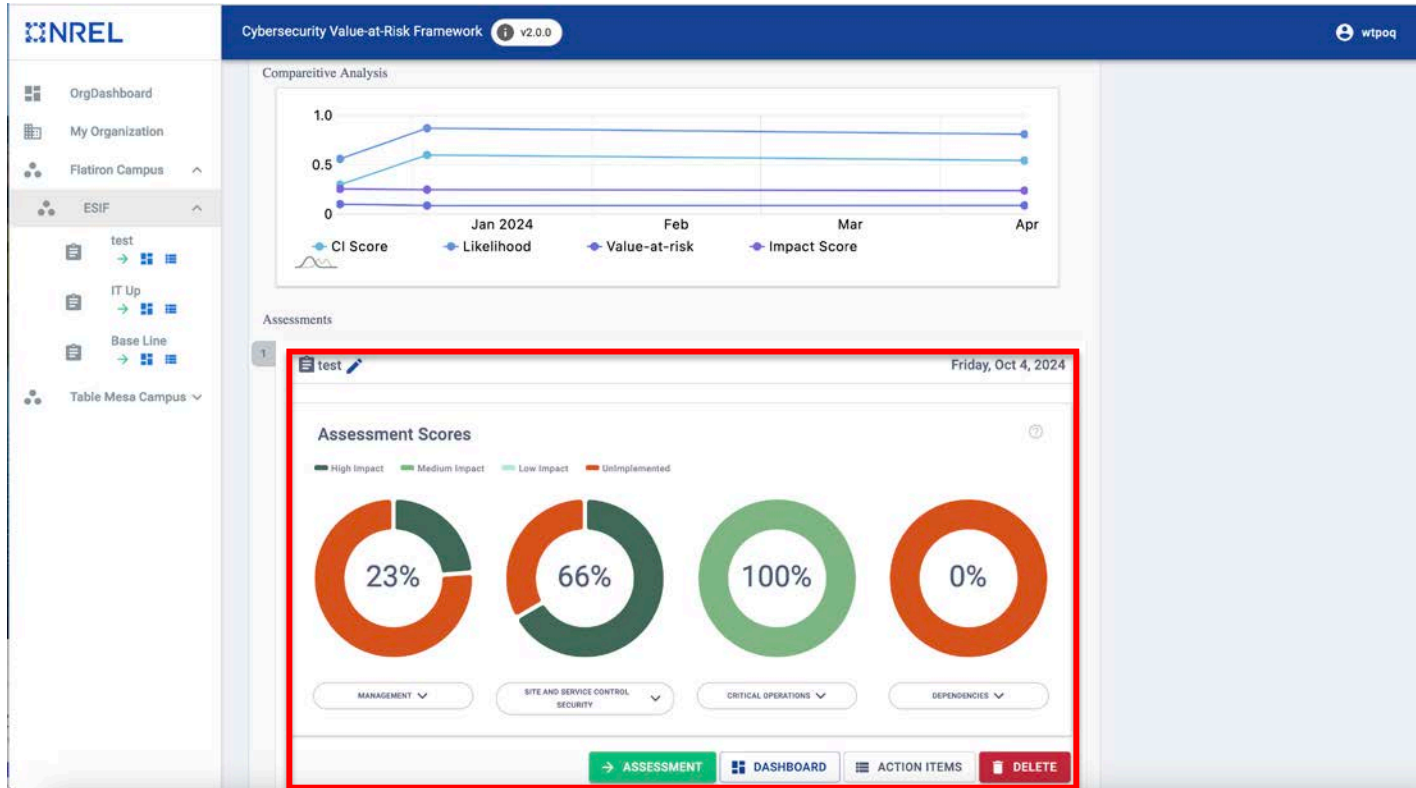
OrgDashboard



Comparative Analysis



Collection View



Future Work

- Advancements through Hydropower operational threat simulation and impact analysis
- Cost-benefit analysis for recommended mitigations with regards to potential cyber-attack consequences
- Monetary impact calculations for risks as well as mitigations

Q&A

www.nrel.gov

Anuj.Sanghvi@nrel.gov

Jordan.Smart@nrel.gov

NREL/PR-5T00-91581

This work was authored in part by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by the Department of Energy Water Power Technologies Office. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

