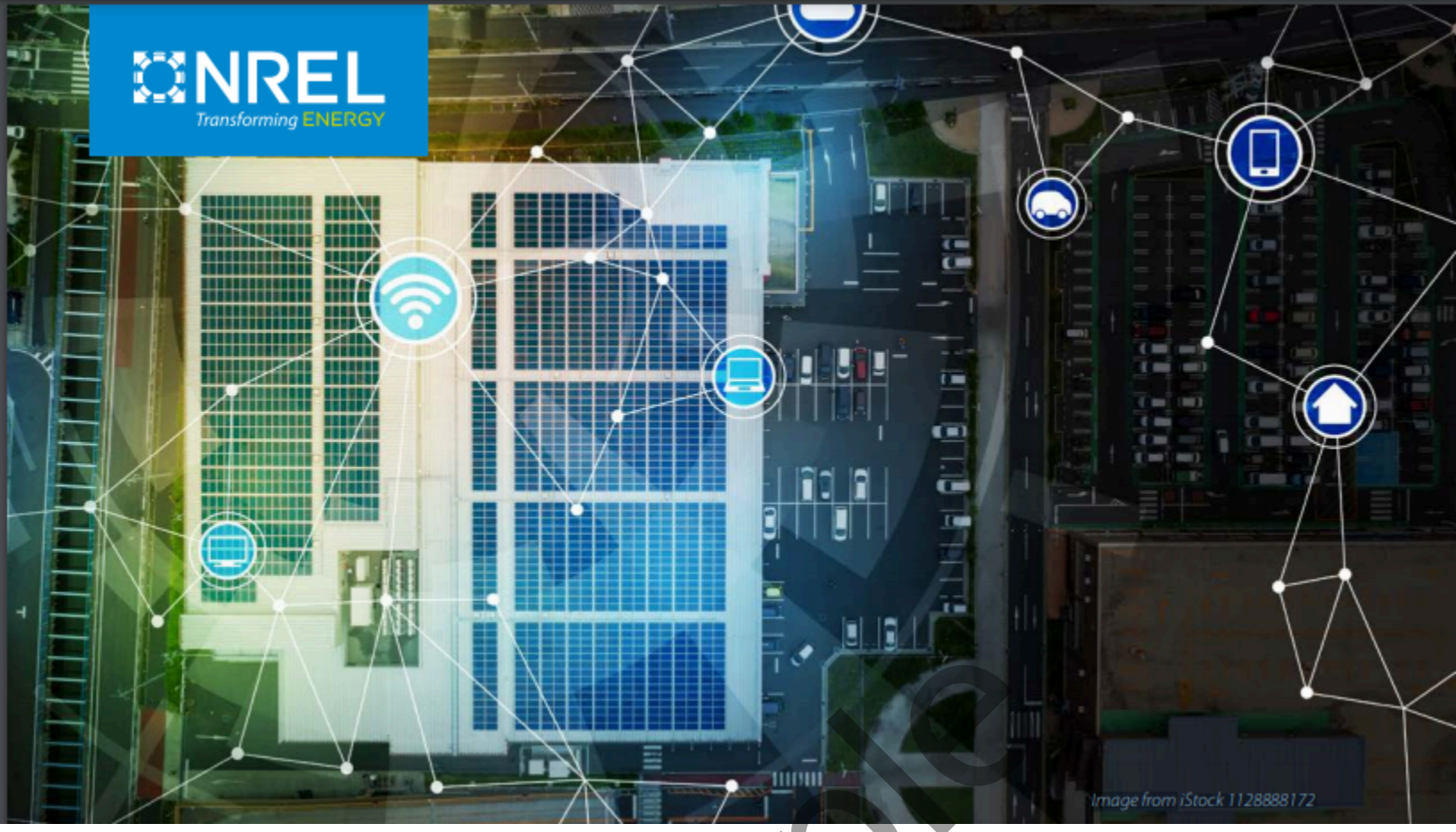


Distributed Energy Resources Cybersecurity Framework: Your Assessment

New Facility

SAMPLE REPORT

2025-05-07T21:22:48.134Z

DER-CF

The Distributed Energy Resource Cybersecurity Framework (DER-CF) helps organizations mitigate gaps in their cybersecurity posture for distributed energy resources.

Distributed Energy Resources Cyber Security Framework

New Facility Assessment Results:

Maturity Levels: Number of Implemented Controls

Governance

190.5
out of **368**

The Cybersecurity Capability Maturity Model (C2M2) arises from a combination of existing cybersecurity standards, frameworks, programs, and initiatives. It provides flexible guidance to help organizations develop and improve their cybersecurity capabilities.

Technical Management

51.15
out of **97**

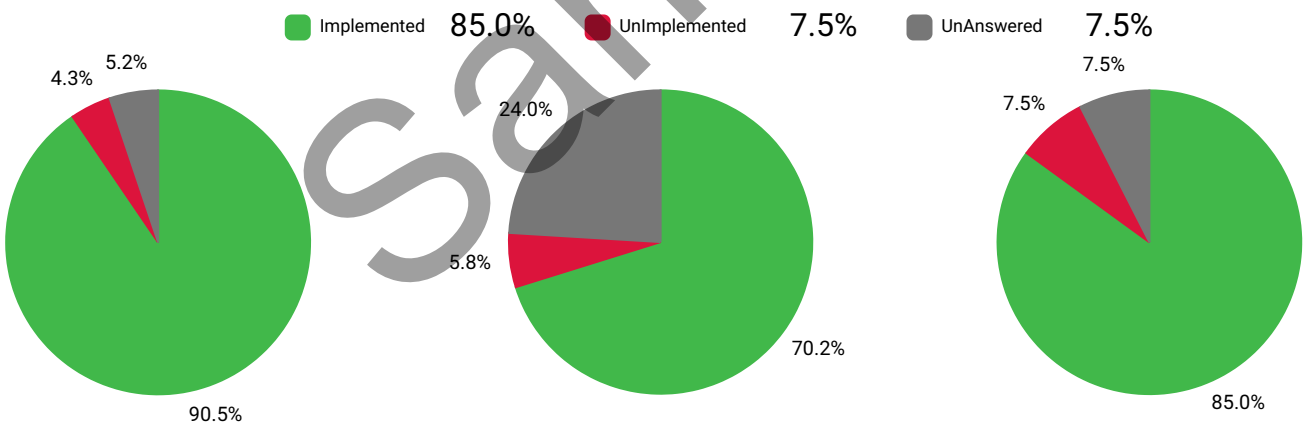
This domain contains practices and polices that extend the Governance domain and are directly related to the operation of the systems. More specifically, this domain is focused on preserving the confidentiality, integrity, and availability of data traveling within a DER system and abroad.

Physical Security

34
out of **40**

DER-CF assessment questions under the physical security pillar are based mostly on guidance from the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, and in smaller part from: 1) NIST 800 series guidance; 2) observations from federal site visits; 3) best practices for physical security controls; and 4) the SANS Institute's physical security specialist training. Questions in the physical security assessment are designed to be applied sitewide, because elevated access to a site or facility in which DERs reside can have equally significant (if not more severe) implications than threats that originate from remote and/or unauthorized access to DER controls alone.

The pie charts below represent the number of implemented, unimplemented, and unanswered controls.



Top Governance Actions

1. Protect sensitive data rest by employing mechanisms such as write-once-read-many (WORM) cryptography to achieve confidentiality and integrity.
2. Assign responsibility, accountability, and authority for the performance of activities in the ARCHITECTURE domain to relevant personnel.
3. Require secure software configurations as part of the organization's software deployment process. Ensure secure default settings on all software. Approve, inventory, and securely configure systems by disabling any unnecessary functionality. Address roles, responsibilities, and configuration management processes and procedures. Establish a process for identifying configuration items throughout the system development life cycle (SLDC) and for managing these items. Develop and maintain secure configuration standards for all systems that

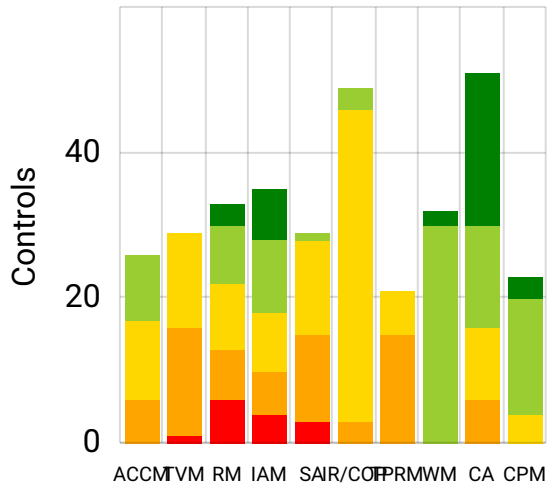
Top Technical Management Actions

1. Create a section within the DER system account management policy for DER-function-specific roles and authorizations. Each function such as deployment, operation, maintenance, etc. should have specific privileges and authorization levels. Ensure the location's DER system administrator accounts for these and follows the principle of least privilege across all domains.
2. Create a policy that ensures management of DER system accounts under supervision of the location's Energy Systems Manager. The policy must include rules of engagement, separate authentication mechanisms and credentials for the DER network, and a single secure authentication system responsible for managing all system accounts. Implement a separate vetting process for third party contractors to obtain DER system accounts.

Top Physical Security Actions

1. Ensure the organization installs buried RF wires or pressure sensors below ground level and with protections from vehicles and animals.
2. CCTV camera should have proper lens dependent upon the applicable coverage and/or lighting needs
3. Ensure the organization uses an alarm-activated VSS that can alert force personnel in the event of an unauthorized access attempt.

Governance



	ACCM	TVM	RM	IAM	SA	IR/COP	TPRM	WM	CA	CPM
Adaptive	0	0	3	7	0	0	0	2	21	3
Repeatable	9	0	8	10	1	3	0	30	14	16
Risk Informed	11	13	9	8	13	43	6	0	10	4
Partial	6	15	7	6	12	3	15	0	6	0
Unimplemented	0	1	6	4	3	0	0	0	0	0
Skipped	0	0	0	0	0	0	0	0	0	0

This graph shows the statistical breakout of the users responses by the level of implementation based on NIST Cybersecurity Framework (CSF) maturity levels (e.g. adaptive, repeatable, etc.), across the 10 domains of the DoE Cybersecurity Capability Maturity Model (C2M2). Achieving higher levels of maturity ensures a better security posture

Domains

IAM = Identity and Access Management
ISC = Information Sharing and Communications (DOMAIN WITHDRAWN)
IR/COP = Event and Incident Response, Continuity of Operations
CPM = Cybersecurity Program Management
SA = Situational Awareness
RM = Risk Management
TVM = Threat and Vulnerability Management
CA = Cybersecurity Architecture
ACCM = Asset, Change, and Configuration Management
TPRM = Third-Party Risk Management
WM = Workforce Management

Unimplemented - Not implemented

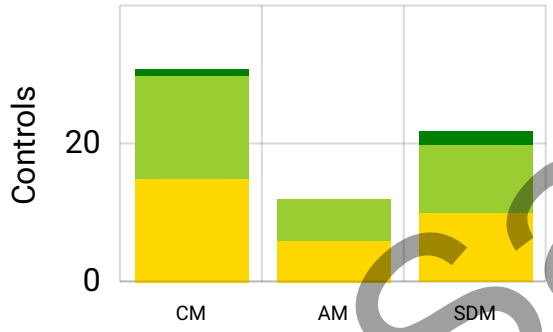
Partial - Limited (i.e., concepts have been casually discussed)

Risk Informed - Documented

Repeatable - Documented and shared

Adaptive - Documented and shared, with training available.

Technical Management



	CM	AM	SDM
Expert	1	0	2
Advanced	15	6	10
Practical	6	3	1
Novice	0	0	0
Basic	0	0	0
Skipped	0	0	0

This bar chart depicts technical competence levels based on the answers submitted by the user in the Technical Management Security Assessment. This suggests the controls answered poorly will fall under basic and novice competence levels and will need immediate attention, time, and resources.

Domains

CM = Configuration Management
SDM = System and Device Management
AM = Account Management

Basic - Lack of knowledge and negligible implementation of tools, technologies, and/or configurations

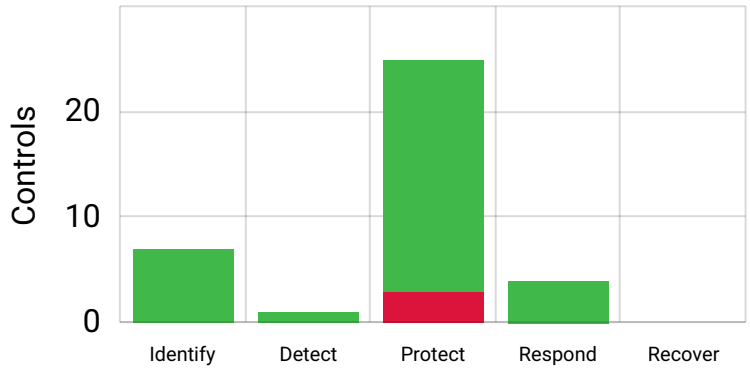
Novice - Weak knowledge and moderate implementation of tools, technologies, and/or configurations

Practical - Satisfactory knowledge and implementation of tools, technologies, and/or configurations

Advanced - Good knowledge and proper implementation of tools, technologies, and/or configurations

Expert - Excellent knowledge and cutting edge implementation of tools, technologies, and/or configurations

Physical Security



	Identify	Detect	Protect	Respond	Recover
Implemented	7	1	22	4	0
UnImplemented	0	0	3	0	0
UnAnswered	0	0	2	1	0

This bar chart shows which NIST CSF domain need to be taken care off in a facility based on the stakeholder need through the mapping between DER-CF physical security control and NIST CSF domain.

AC = Administrative Controls
PAC = Physical Access Control
TAC = Technical Access Control

Notice

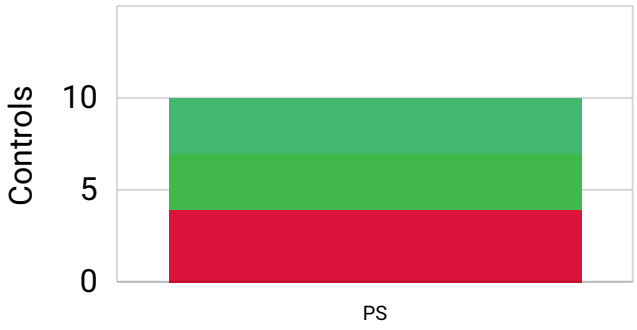
Importance of Cybersecurity Assessments

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 distributed energy resource (DER) system can include direct financial loss, physical damage, severe reputation impact, and even loss of life. The U.S. Department of Energy (DOE) created the Cybersecurity Capability Maturity Model (C2M2) [4] to simplify the complex subject of cybersecurity assessment and mitigation for public and private enterprises. The National Institute of Standards and Technology (NIST) created the Cybersecurity Framework (CSF) to also help public and private enterprises categorize and quantify the level of maturity of their critical cyber governance security controls across five major categories and identify the partially implemented or unimplemented controls that could pose a cyber risk. Details on the five CSF categories can be found at the end of this report. As part of research funded by the Federal Energy Management Program (FEMP), the National Renewable Energy Laboratory (NREL) created the Distributed Energy Resources Cybersecurity Framework (DERCF) [1] with an accompanying web application designed to aid energy system managers at federal sites improve their cybersecurity posture via a guided assessment. Cyber assessments that integrate the DOE and NIST frameworks allow enterprises to identify and mitigate cyber risks from inadequate business process security controls quickly and cost-effectively. The DERCF utilizes the content from the C2M2 and NIST frameworks and expands upon two additional domains: Technical Management and Physical Security. The remainder of this report is organized to provide a high-level summary followed by more detailed analysis of weak points categorized by DERCF pillars as well as their domains and subdomains.

Results Summary

completed the DER cybersecurity assessment on 5/7/2025. The overall score from the assessment was 275.65 out of a maximum score of 505. this score is calculated by the DERCF application based on the collective responses from the representatives who participated in the assessment. This suggests that the cybersecurity maturity level is at a , and there is opportunity for considerable improvement over the next 6-12 months across multiple NIST and DOE C2M2 domains, given the actionable intelligence described in Appendix B. Below is a summary of your posture level:

- Moderate: your site has a moderate foundation in cybersecurity practices. To improve this, it is important to keep documents updated and continue sharing and updating your processes and provedures as necessary.



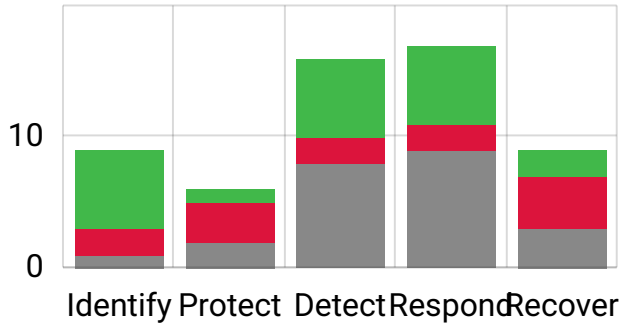
The figure above shows the overall distribution of strengths and weaknesses across the three DERCF pillars. Scores are defined by the maturity of each of the domains. More details about each domain's score can be found in the Analysis section.

What is Affecting My Score?

It is 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 criticality. Criticality is defined as the importance that a particular control has to the rest of your security posture, and criticalities are categorized by low, medium, or high. Medium- and high-criticality-designated controls will have a greater impact on your score if not implemented.

Unanswered Questions

The figure below provides the distribution of unanswered questions in your assessment. Recall that unanswered questions do not count negatively against your score; however, they prevent you from scoring points.



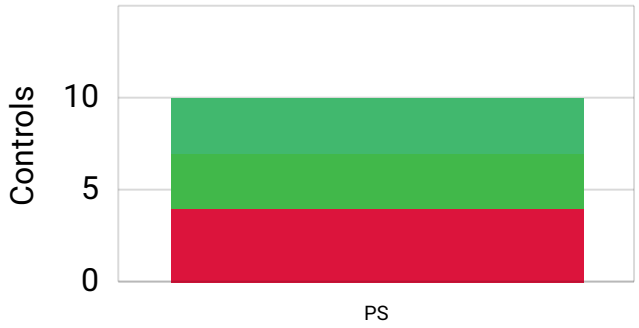
Unimplemented High Criticality Questions

Having limited implementations for controls with high criticality also greatly impacts score, as they carry a high weight. These items become a high priority for recommendations to bolster cybersecurity posture. A complete list of unimplemented high-criticality questions is available in Appendix A. The chart below depicts the distribution of unimplemented high-criticality controls per pillar. It represents all the unimplemented controls out of 386 controls and across the 10 domains of DOE C2M2 at a high level to focus an organization's attention on the key domains. Understanding key areas that need attention is a primary step in prioritizing cybersecurity efforts.

Analysis

NIST Integrated Cybersecurity Governance Summary

The figure below shows the statistical breakout of the responses by the level of implementation (based on NIST CSF maturity levels) across the 10 domains of the C2M2. The bar chart indicates the domains containing controls that need the most attention because they have not been fully implemented. The NREL Cybersecurity team recommends that addresses the unimplemented and partially implemented controls listed in Appendix A before completing the full set of controls listed in the separate CSV spreadsheet provided with this report. See Abbreviations for C2M2 domains.

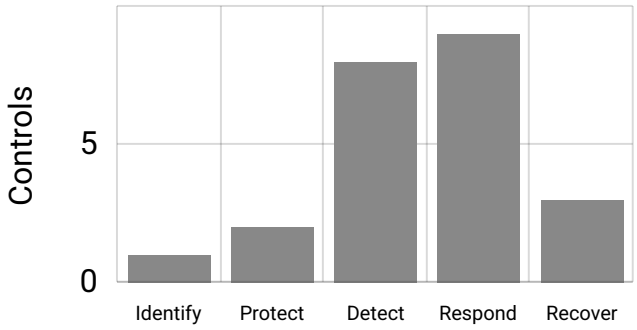


Technical Management Summary

The Technical Management domain focuses on assessing cybersecurity posture on a more granular level, including identifying weaknesses in device settings and configurations, remote access, and more. The figure below provides a graphical view of this information. Typically, the answers to questions in the Technical Management domain are best provided by system engineers or others who have direct contact with DER systems.

Physical Security Summary

Similar to Technical Management, the Physical Security domain takes a deeper dive into how DER systems are secured from potential hazards and malicious activity. Physical security is equally as crucial to maintaining the availability of DER systems. Due to the nature of these systems potentially being off-site or in remote locations, they can become susceptible to physical damage or tampering unless the proper controls are put in place. The figure below shows the distribution of your score by criticality



Methodology for Prioritization

The method for prioritization of unimplemented controls in the DERCF assessment is based on the product of two weighting factors:

- The criticality of the control (how large of an impact it can have on the DER system and beyond if not properly implemented).
- The maturity level of the control (four levels of implementation according to NIST CSF - unimplemented, risk-informed, repeatable, and adaptive).

The higher the control's criticality level, the greater the weighting applied. The lower level of maturity, the greater the weighting applied.

It is recommended that the controls selected at the "unimplemented" or "partial" level of implementation (in the tables presented in Appendix A) be realized first, with secondary priority to "risk-informed" and "repeatable" in level of implementation. The number of controls in the prioritized action item list to be implemented in the first phase should be determined based on access to funding, material resources, and labor required. This ensures that critical controls are implemented on an established timeline with budget estimates, labor, and material resource allocation metrics to align with the strategic goals of the organization.

Conclusion

Based on the figures above and with the deep analysis of assessment results, your organization has an overall Moderate cybersecurity posture but still has areas that require improvement. The weaknesses described in the tables below, organized by pillars in Appendix A are critical and need to be addressed immediately. These weaknesses provide an opportunity for an attacker to cause catastrophic results during serious cyberattack, which could compromise key components of your DER systems.

A separate comma-separated-value spreadsheet provides all action items relevant to your organization sorted by level of priority (highest to lowest). We strongly recommend that your group first has a thorough look at key areas of cyber vulnerabilities identified in Appendix A, along with the full set of prioritized action items listed in Appendix B to develop a strategic plan to mitigate your organization's cyber risk methodically, affordably, and with transparency. Additionally, this report should continue to serve as a reference for future work in improving cybersecurity posture

Bibliography

[1] Powell, Charisa, Konrad Hauck, Anuj Sanghvi, Adarsh Hasandka, Joshua Van Natta, and Tami Reynolds. 2019. Guide to the Distributed Energy Resources Cybersecurity Framework. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-75044. https://www.nrel.gov/docs/fy20osti/75044.pdf.

[2] National Institute of Standards and Technology (NIST). 2020. Cybersecurity Framework (CSF). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[3] National Renewable Energy Laboratory (NREL). "Distributed Energy Resources Cybersecurity Framework." Last modified October 1, 2020.

https://d

[4] U.S. D
Capabilit
https://w
Feb2014