Applying the Risk Management Framework: The Distributed Energy Resource Risk Manager

Charisa Powell, Tami Reynolds, Anuj Sangvhi,
MD Touhiduzzaman, Joshua Van Natta, and Paul Wand

National Renewable Energy Laboratory

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5R00-78436
November 2022

Applying the Risk Management Framework: The Distributed Energy Resource Risk Manager

Charisa Powell, Tami Reynolds, Anuj Sangvhi,
MD Touhiduzzaman, Joshua Van Natta, and Paul Wand

National Renewable Energy Laboratory

Suggested Citation
Powell, Charisa, Tami Reynolds, Anuj Sangvhi, MD Touhiduzzaman, Joshua Van Natta, and Paul Wand. 2022. *Applying the Risk Management Framework: The Distributed Energy Resource Risk Manager*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-78436. https://www.nrel.gov/docs/fy23osti/78436.pdf.

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is availabl at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5R00-78436
November 2022

National Renewable Energy Laboratory
15013 Denver West Parkway
Golden, CO 80401
303-275-3000 • www.nrel.gov

NOTICE

This work was authored 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 U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Federal Energy Management Program Office. The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government.

Cover Photos by Dennis Schroeder: (clockwise, left to right) NREL 51934, NREL 45897, NREL 42160, NREL 45891, NREL 48097, NREL 46526.

List of Acronyms

ATO	authority to operate
CEEP	Cyber-Energy Emulation Platform
CNSSI	Committee on National Security Systems Instructions
DER	distributed energy resource
DERCF	Distributed Energy Resource Cybersecurity Framework
DoD	U.S. Department of Defense
ICS	Industrial Control System
NIST	National Institute of Standards and Technology
NREL	National Renewable Energy Laboratory
RMF	Risk Management Framework

Executive Summary

As part of a multiyear effort, the National Renewable Energy Laboratory (NREL) has dedicated resources to understand and identify cybersecurity weaknesses in distributed energy resources (DERs) by performing assessments. Due to a lack of standardization and rapidly increasing adoption of DERs, there is a critical need to address cybersecurity needs for DER systems in an interactive way. Furthermore, federal agencies, which are required to obtain an authority to operate, are challenged by the complexities of including their DERs. To help meet this need, in early 2020, NREL released the Distributed Energy Resource Cybersecurity Framework (DERCF) and accompanying Web application. This process is supported by the Risk Management Framework (RMF) developed by the National Institute of Standards and Technology.

This project, referred to as the DER Risk Manager, expands on the existing DERCF work to include methods that support walking a user through the seven RMF steps. The tool is available for download at no cost from https://nrel-cyber.github.io/DER-RM/. The purpose of this paper is to describe the steps the DERCF team at NREL took to understand Steps 1–5 of the RMF process. Additionally, this document will identify future work on the first five steps as well as a plan for Steps 6 and 7.

Table of Contents

1 Introduction 1
1.1 Background 1
2 Risk Management Framework Overview 2
3 Research and Implementation of the DER Risk Manager 3
3.1 Reference Documents 3
3.2 Technical Implementation 3
4 Challenges and Best Practices 5
5 Future Work 6
5.1 *Authorize* and *Monitor* Steps 6
5.2 Supply Chain Risk Management 6
5.3 Cybersecurity Cost Model 6
5.4 Cyber-Energy Emulation Platform Integration 6

List of Figures

Figure 1. RMF steps and relevant documents ("FISMA Implementation Project" 2020) 2

List of Tables

Table 1. Summary of Inputs and Outputs per RMF Step 4

1 Introduction

The National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) is a complex process that requires significant time and resources on the part of federal facilities. This includes, but is not limited to, identifying appropriate personnel, understanding document scope, and planning a course of action. The simplification of these tasks via an automated interface enveloped within a secure application will greatly benefit the efficiency of cybersecurity compliance for distributed energy resource (DER) systems.

1.1 Background

The Distributed Energy Resource Cybersecurity Framework (DERCF) and accompanying interactive Web application[1] is a dynamic capability serving as a starting point for cybersecurity posture assessment. Developed by the National Renewable Energy Laboratory (NREL) and released in January 2020, the DERCF is an accessible tool for energy system facility managers to gauge their initial cybersecurity posture via a guided assessment that provides recommendations and prioritized action items based on custom answers to the questionnaire. For more information, see the *Guide to the DERCF* (Powell et al. 2019).

In addition to streamlining the process of cybersecurity assessments, NREL researchers have also focused on identifying challenges faced by federal energy managers during the process of complying with the RMF for DER systems. Developed by NIST, the RMF is a cyclical process designed to incorporate principles of security and risk management into an organization's system policies and procedures. The RMF is supported by a collection of documents (SP 800 Series 2020) that provide guidance on legislation considerations, security controls (including assessment and monitoring), and the authorization for a system to operate.

The DER Risk Manager takes the fundamentals of the DERCF Web assessment tool and applies it to the stepwise process of the RMF. An overview of the RMF steps can be found in Section 2. The remainder of this document outlines the approach taken to integrate the RMF into the existing DERCF application. The application also adheres to some Department of Defense (DoD) specific guidelines for national security systems that overlay NIST recommendations. Note that this document only contains content up to and including *Assess.* The remaining steps, *Authorize* and *Monitor*, are out of scope for this segment of work and will be subsequently addressed.

[1] DERCF Web assessment tool: www.dercf.nrel.gov

2 Risk Management Framework Overview

Targeted at understanding and reducing organizational risk, the RMF is supported by relevant legislation, ranging from executive orders to industry standards. Of importance are Executive Orders 13800 (2017) and 13636 (2013), both of which emphasize the need to prioritize cybersecurity of critical infrastructure and utilize NIST resources. The RMF is designed for application to systems across an organization by becoming an integral part of the system development lifecycle. In particular, the RMF is focused on the handling of an information system and its associated risk to develop a plan and achieve authority to operate (ATO), a required process for many federal sites.

Figure 1 depicts each of the main six steps of the RMF. It is important to know that a seventh step, known as *Prepare*, is uniquely placed in the center because it is relevant to all steps as an initial process. For the remainder of this document, this step will be referred to as Step 0.

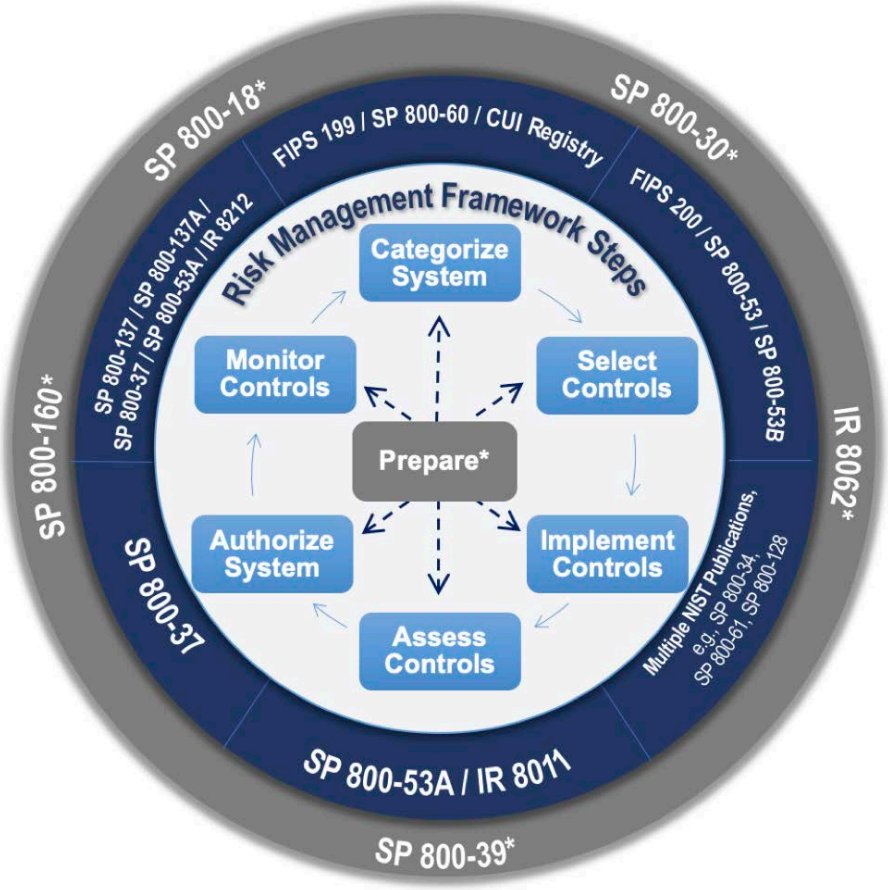

Figure 1. RMF steps and relevant documents ("FISMA Implementation Project" 2020)

3 Research and Implementation of the DER Risk Manager

The work associated with the DER Risk Manager is supported by NIST as well as other frameworks to provide a holistic foundation.

3.1 Reference Documents

The RMF is also leveraged by various DoD facilities with some additional requirements to the process. Because these systems are considered national security systems, certain modifications such as compliance with the Committee on National Security Systems Instructions (CNSSI) 1253 for categorizing DER systems are also required (CNSS 2009). These specifications shape the DER Risk Manager to target a wider audience to support their compliance needs. In addition, the Risk Manager references the MITRE ATT&CK Industrial Controls Systems framework—a tool that describes attacker tactics and techniques as they relate to industrial control systems (MPN 2020). This framework is a pivotal piece of support to identify common threats to operational technology, which includes DERs.

3.2 Technical Implementation

Each step of the RMF has several subtasks to provide additional clarity. These substeps are handled by the tool in two ways:

1. Following the sequential order of the RMF tasks
2. Collecting information as an ongoing process and populating one or more resources at once.

Some pieces of the RMF process, such as planning, review, and approval from the authorizing official to obtain ATO, are fully dependent on the user performing a task outside of the Web application. In these cases, the application will give guidance and supplemental resources to the user.

As the user moves through the Risk Manager application, the resources required for the RMF package to be considered as complete are generated automatically. These include:

- System Security Plan
- Risk Assessment Report
- Security Assessment Report (SAR)
- Plan of Action and Milestones (POA&Ms).

These documents will be securely created and stored by the application and will contain the details originally created by the user. Upon completion of the DERCF RMF process, the application will allow for the documents listed above to be downloaded and packaged for reference. If applicable, this package can also be used as a starting point for requirements related to ATO.

Table 1 provides a high-level overview of inputs and outputs associated with the DERCF, per RMF step. Many of the subtasks within each step use outputs from previous steps as input.

Table 1. Summary of Inputs and Outputs per RMF Step

RMF Step	NIST Description	DERCF Input	DERCF Output	Reference Document
Step 0: Prepare	Prepare to carry out essential activities at the organization, mission and business process, and information-system levels of the enterprise to help prepare the organization to manage its security and privacy risks using the RMF.	Role identification, upload of existing risk assessments or other supporting initial documents	Documentation, DER applicable guidance for asset identification, system boundary definitions and security requirements, calculation of risk score for the system, and role identification.	NIST 800-53 Rev 4, NIST SP 800-39, NIST SP 800-60v1, NIST SP 800-64
Step 1: Categorize	Categorize the system and the information processed, stored, and transmitted by that system based on an impact analysis.	Characteristics of a system to create "system description"	System description documented from security categorization results	NIST SP 800-18, NIST SP 800-30, FIPS 199, CNSSI 1253
Step 2: Select	Select an initial set of baseline security controls for the system based on the security categorization; tailor and supplement the security control baseline as needed, based on organization assessment of risk and local conditions.	Relevant controls based on system environment and protection requirements	Low/moderate/high control baseline selection; tailored controls, continuous monitoring strategy for DERs	NIST 800-53 Rev 4, NIST SP 800-160v1
Step 3: Implement	Implement the security controls and document how the controls are deployed within the system and environment of operation.	Security controls established in *Select*	Documentation of implemented controls and any associated changes with implementation status	NIST SP 800-53A Rev 4, NIST SP 800-160v1
Step 4: Assess	Assess the security controls using appropriate procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	Assessment report from internal or external assessor	Documentation of completed assessments to create guidance and templates for SAR and PO&AMs	NIST 800-160v1

4 Challenges and Best Practices

There are several challenges aligned with the RMF process, ranging from the complexities of the framework to the lack of a uniform process followed by federal sites. One of the main challenges is related to the inconsistency of knowledge, experience, and responsibilities from site to site. While it is expected for organizations to have different processes, it is important to utilize consistent resources and ensure that appropriate education is available.

Additional challenges arise in the vastness of operational technology in general and understanding how existing frameworks and processes might overlook critical security concerns, due to being generally information technology focused. The field of DERs is important in ongoing energy system evolutions and can have serious consequences via physical damage and/or loss of availability if not properly secured.

To overcome these challenges, organizations should prioritize the following:

- Use the DERCF as an entry point resource for implementing and updating cybersecurity procedures for DERs.
- Utilize NIST as a baseline resource to ensure reliable information and consistency across organizations.
- Continuously update documentation as changes occur and share knowledge with relevant parties.

These elements, in addition to maintaining strong security posture overall, begin to target important challenges in overall cybersecurity but do not create a comprehensive list. Organizations can also participate in validation assessments, in which the NREL research team meets with an organization (physically or virtually) to walk them through their first assessment.

5 Future Work

As a dynamic and evolving tool, the DERCF is expanding the avenues that will increase flexibility, usability, and efficiency. To ensure the maximum effectiveness of the RMF process, it is imperative to engage with the RMF as a cyclical process, which ensures continuous attention to all its aspects. NREL's forward-looking work will focus on the remaining steps of the RMF, supply chain risk management, cost analysis, and visualization of assessment results.

5.1 *Authorize* and *Monitor* Steps

The remaining steps of the RMF will be included in future work associated with the DER Risk Manager. The *Authorize* step contains tasks related to packaging, delivering, and receiving approval of the documents required to complete an ATO package.

Although *Authorize* contains tasks primarily outside of the application itself, the *Monitor* step presents many opportunities for the DERCF to serve as a useful resource. One main component will be reminders for engineers and managers to check on the controls that have been implemented and make updates if there have been changes. These reminders will be fully customizable, allowing for organizations to adhere to their unique requirements.

5.2 Supply Chain Risk Management

In addition to the Risk Manager, NREL's DERCF team envisions several opportunities to build additional capability to the DERCF tool. One of these includes helping identify vulnerabilities within the supply chain by researching and providing solutions to help mitigate problems. NREL will leverage the lessons learned while developing and coordinating these security controls to conduct supply chain risk assessments of different grid-tied operational technology products, including DERs, and will develop a methodology that would include device and system metrics to quantify risks in a way that can be easily understandable to the operators at federal sites.

5.3 Cybersecurity Cost Model

Researching the cost of cybersecurity controls would provide significant value to federal sites. This would afford organizations an opportunity to conduct a cost-benefit analysis to make decisions about what actions to take to improve their cyber posture and how to budget accordingly. This research is also extremely relevant as cybersecurity becomes an element that is factored into the design and development process.

5.4 Cyber-Energy Emulation Platform Integration

NREL's Cyber-Energy Emulation Platform (CEEP) is a new, innovative way to research and analyze energy systems. CEEP can replicate a federal site through data visualization. Using this advanced technology with the integration of data from the DERCF tool could help identify gaps in an organization's cybersecurity posture in a more comprehensive way then what is currently possible. This two-pronged approach could help merge the two complex cybersecurity topics of policy and technology by providing an integrated way to interact with cybersecurity logs and alerts.

References

Committee on National Security Systems (CNSS). 2009. "CNSS Instruction No. 1253: Security Categorization and Control Selection for National Security Systems: Version 1." National Security Agency. https://www.steptoe.com/images/content/5/7/v1/5778/CNSSI-1253.pdf.

"Executive Order 13636 of February 13, 2013, Improving Infrastructure Cybersecurity." Code of Federal Regulations, Title 3. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

"Executive Order 13800 of May 11, 2017, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." Code of Federal Regulations, Title 3 (2017 comp.). https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

"FISMA Implementation Project." 2020. NIST Information Technology Laboratory Computer Security Resource Center. https://csrc.nist.gov/projects/risk-management/rmf-overview.

MITRE Partnership Network (MPN). 2020. "ATT&CK for Industrial Control Systems." Last modified June 3, 2020. https://collaborate.mitre.org/attackics/index.php/Main_Page.

National Institute of Standards and Technology (NIST). Federal Information Processing Standards Publication 199: Standards for Security Categorization of Federal Information and Information Systems. FIPS PUB 199. Gaithersburg, MD, 2004. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

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.

"SP 800 Series." 2020. NIST Information Technology Laboratory Computer Security Resource Center. https://csrc.nist.gov/publications/sp800.