The Distributed Energy Resource Risk Manager

DER-RM

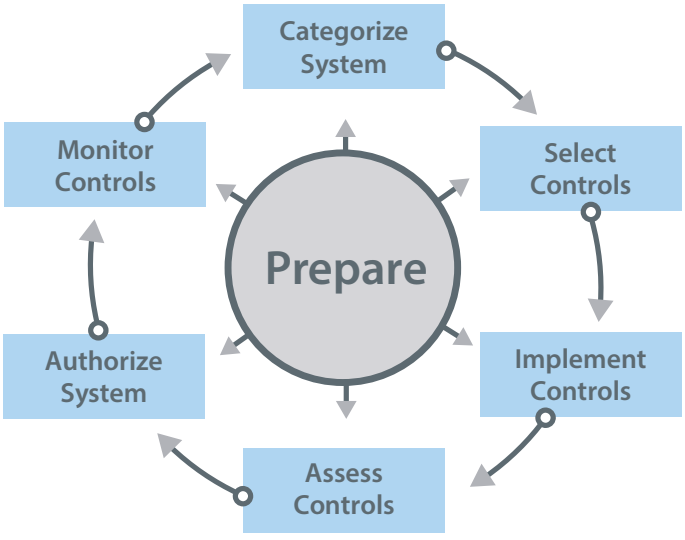
Organizations need a comprehensive approach to managing security and privacy risks, especially for energy resources that are becoming increasingly distributed. A tool by the National Renewable Energy Laboratory (NREL) makes it possible to manage these risks and maintain the highest standards of cybersecurity.

To simplify risk management for facilities and distributed energy resources (DERs), NREL has created the **Distributed Energy Resource Risk Manager (DER-RM)**, an automated, user-friendly tool that helps navigate and implement one of the most widely trusted frameworks for information security, the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF).

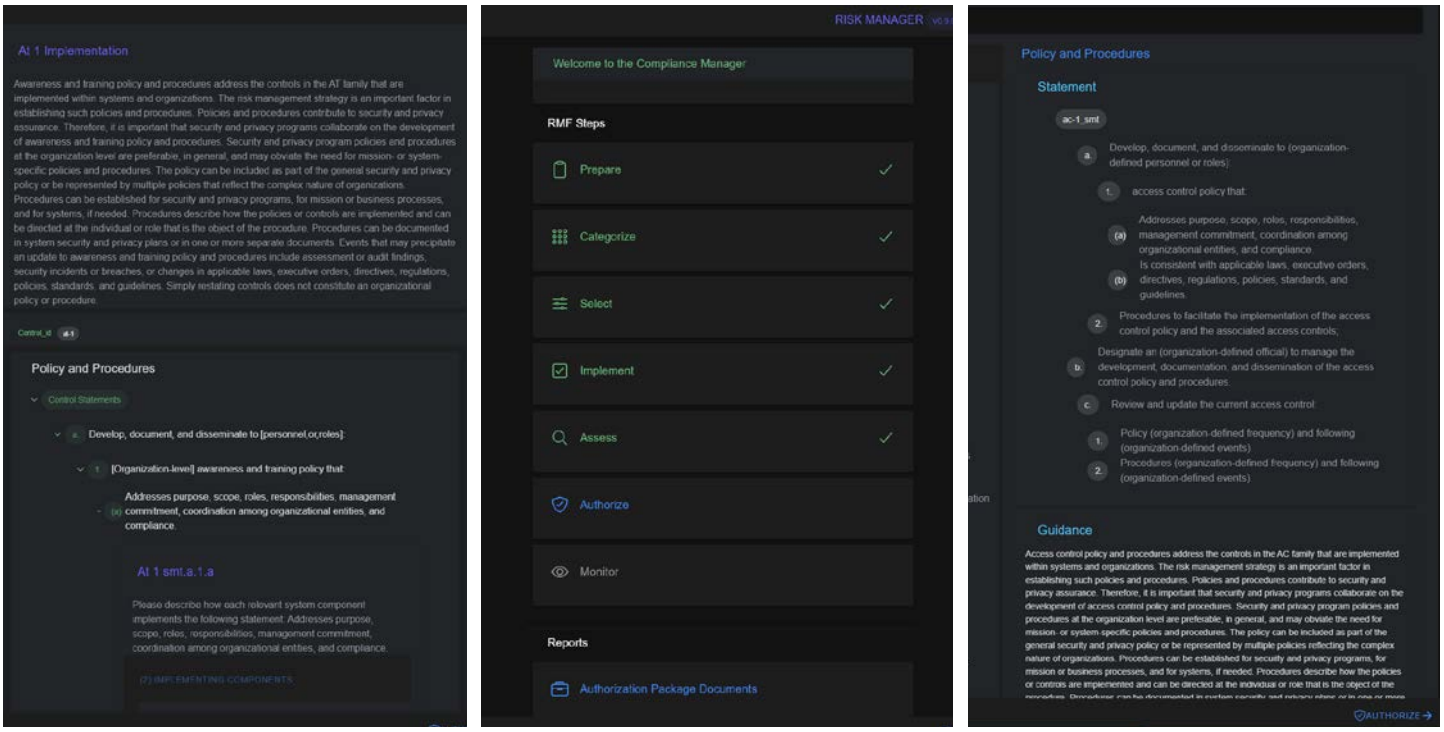
Easy Application of the NIST-RMF

Compliance with the NIST-RMF is required by most federal facilities and practiced by many other organizations. The NIST-RMF directs users to current NIST standards that apply to all dimensions of risk management, including information privacy, supply chain risks, and critical infrastructure resilience. The NIST-RMF requires cyclical self-evaluation, which maintains a high level of system security but also demands ongoing time and attention. The DER-RM lightens the workload for organizations by streamlining and managing the NIST-RMF process in an easy-to-use, downloadable application.

Risk Management Framework Steps



The NIST-RMF compliance requires continual self-evaluation across many dimensions of security and risk management. NREL's DER-RM alleviates that effort by organizing, automating, and managing a user's risk management process.



System-level preparatory tasks assist with identifying the business functions, assets, information types, and other system-dependent information.

How the DER-RM Works

The DER-RM runs locally as a desktop application and uses an intuitive interface to walk users through NIST-RMF compliance step by step, automating the process where possible and providing risk management recommendations where applicable.

From information about the user's system, the DER-RM populates common attacks on DER controls that test the user's security. The DER-RM then offers tailored strategies and DER control recommendations derived from NIST standards. Users can import their control data in Open Security Controls Assessment Language (OSCAL) format for an automated assessment and export their results in a variety of report templates to achieve compliance in a way that best suits organizational needs. For DERs, the DER-RM includes specialized guidance for systems powered by solar panels, wind generation, electric vehicles, and other energy resources, and it helps organizations achieve an Authorization to Operate for new device interconnections.

Not only does the tool navigate the NIST-RMF, but it also provides all-around knowledge and guidance for site security, backed by real-world examples and NREL expertise.

Guiding Frameworks

The DER-RM is an extension of NREL's DER Cybersecurity Framework (DER-CF) (dercf.nrel.gov), a much broader tool for mitigating gaps in cybersecurity at facilities and organizations. The DER-CF involves increased emphasis on physical security and technical management as well as a sharper focus on distributed energy technologies, whereas the DER-RM specifically focuses on NIST-RMF compliance—a major undertaking for federal sites and a critical framework for secure operations.

Learn More

Check out the tool and see how it could benefit your energy system: nrel-cyber.github.io/DER-RM/.

Learn more about NREL's research in cybersecurity: www.nrel.gov/security-resilience/cybersecurity.html

Contact:

Tami.Reynolds@nrel.gov
Project Manager and Lead

NREL Transforming ENERGY

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

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

NREL/FS-5R00-83237 • July 2022