

New cybersecurity tool simplifies site evaluations

August 3 2022



Credit: Pixabay/CC0 Public Domain

As federal sites invest in distributed energy resources (DERs) like solar panels and battery backups, investments in cybersecurity must also be considered. More energy resources create more complexity to manage—introducing the potential of new cyber vulnerabilities and added costs down the road.

Luckily, there is a new tool available to help manage this risk: the National Renewable Energy Laboratory's (NREL's) [DER Risk Manager \(DER-RM\)](#), a downloadable application that implements and automates a widely trusted framework for information security from the National Institute of Standards and Technology (NIST). The DER-RM, developed with support from the U.S. Department of Energy Federal Energy Management Program (FEMP), offers a user-friendly solution for sites that must comply with NIST's Risk Management Framework.

"After two years of the team's hard work and extensive research on the NIST 800-37 Risk Management Framework, we're very excited to launch the beta version of this tool," said Tami Reynolds, NREL [cybersecurity](#) project lead. "The seven-step NIST framework is a comprehensive process that helps organizations manage [information security](#) and privacy risk, but it wasn't designed specifically for operational technologies like distributed energy. The DER-RM offers this service for organizations seeking to adopt more renewable and distributed [energy systems](#)."

Compliance often requires time-consuming, cyclical evaluations, which the DER-RM streamlines. In addition to NIST compliance, the design of the DER-RM was informed by NREL's previously developed [DER Cybersecurity Framework \(DER-CF\)](#), a cyber evaluation tool that casts a wider net, evaluating multiple domains of a site's security such as its cyber governance, cyber-physical technical management, and physical security. Both applications guide users through tailored questions to build a profile of their energy system, which is then assessed, scored, and improved with unique recommendations.

"The DER-RM provides a streamlined process for completing and generating associated reports to achieve compliance, whereas the DER-CF is a flexible, hybrid application that enables implementation of fundamental cybersecurity practices," said Anuj Sanghvi, cybersecurity

researcher and technical lead for the project. "For organizations beginning to assess the cybersecurity posture for their distributed generation assets, the DER-CF application plays a vital role for onboarding DER systems to federal enterprises."

In addition to the launch of the DER-RM, the NREL team recently released a series of training modules on the more fundamental evaluation tool, DER-CF, through FEMP's accredited training portal.

Easy compliance for controls and communication

For risk management, the DER-RM is built around the controls-oriented NIST framework, which is mandatory for federal agencies and many other organizations. The tool specifically provides guidance to help organizations attain an Authorization to Operate (ATO), which allows facilities to document and weigh the risks that the system introduces to an organization's personnel, operations, and other organizations. With an ATO approval, authorizing officials accept the risks involved—and the plan to mitigate them—from integrating the system onto federal networks.

Users can input their system information, which the DER-RM assesses by applying common cybersecurity attacks and testing the system's defense. Users can also upload their control data files directly, which the DER-RM checks for NIST compliance and reports where [risk management](#) steps are needed. Because the NIST framework requires ongoing evaluations, the DER-RM is a significant time-saver for maintaining compliance.

"The DER-RM utilizes as much dynamic components as possible to provide a truly tailored experience to the user," said Ryan Cryar, lead developer of the DER-RM and DER-CF. "Utilizing the NIST Open Security Controls Assessment Language, or OSCAL, we have a single

schema that allows us to develop around a centralized data model for easier importing and exporting from different tools for a more custom user experience. No two assessments are the same."

Both the DER-RM and DER-CF are available at no cost, with an accessible user interface and the option to anonymize users. For organizations that require cybersecurity compliance, these tools offer a quick, user-friendly approach to align with several cybersecurity frameworks and best practices. For organizations that are simply interested in improving the security of their facilities and DERs, the DER-RM and DER-CF offer accessible solutions with a unique focus on DERs, allowing organizations to continue to evolve their [energy](#) systems and keep ahead of the cyber threat.

Provided by National Renewable Energy Laboratory

Citation: New cybersecurity tool simplifies site evaluations (2022, August 3) retrieved 5 May 2024 from <https://techxplore.com/news/2022-08-cybersecurity-tool-site.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.
