Cyber Resilience Assessment Tool FAQ

What is the Cyber Resilience Assessment Tool?

This proprietary new tool is part of the ReliabilityFirst (RF) Resilience and Risk Program. It is a voluntary self-assessment that allows entities to evaluate and benchmark their cyber resilience (CR) posture, as well as measure effectiveness.

The tool will characterize the operational resilience of an entity's Bulk Power System (BPS) infrastructure in the presence of cyber attacks. The assessment output is an extensive report that will give BPS operators the ability to identify areas of improvement through deeper insights into components and processes that impact CR.

Why is measuring Cyber Resilience important?

The potential for disruptions in the BPS can be attributed to the dependence upon, and the vulnerability of, the networks' interconnecting substations and control centers. The RF Resilience and Risk Program works to promote and enhance grid reliability, security and resilience. As an integral part of the Program, CR focuses on developing, implementing and maintaining comprehensive resilience capabilities that work to minimize negative impacts to the BPS.

There is a need to develop CR metrics for the BPS to provide quantitative insights into security controls to:

- Support risk management and mitigation decisions.
- Provide quantitative and qualitative insights to ensure operational resilience and assist in development of cost-effective mitigation plans.
- Motivate BPS operators to continually assess their resilience capabilities and benchmark their performance.
- Identify factors contributing to resilience, investments with better ROI or actions that enhance the resilience of the electric grid.
- Educate entities on factors contributing to grid resiliency.

Who is eligible to use this tool?

Any registered entity within the RF Region that is involved in ensuring the security, reliability and resilience of BPS will be able to take advantage of the CR Assessment Tool.

Is there a cost to use the tool?

No, the tool is available free of charge to registered entities within the RF region.

Is the information submitted in the CR Assessment Tool protected?

The information stored in the CR Assessment Tool is in a database. The data in this database is always encrypted at rest. The data in transit is secured by secure sockets layer encryption. Access to the tool is controlled by multi-factor authentication and stringent password policies. Further, the data is segmented in the tool (and database) in such a way that confidentiality and integrity is maintained between individual users and entities.

How will ReliabilityFirst use the information submitted in the CR Assessment Tool?

The tool is designed to be a voluntary self-assessment for entities to measure and benchmark their cyber resilience posture. The tool is not used to assess compliance to NERC Standards or in any compliance-related activities. The reports and subsequent results from the tool are provided as generic recommendations on areas of improvement rather than non-conformance to any Standard.

RF will periodically analyze the information in aggregate to generate anonymized regional observations.

How will I receive my report?

The report is accessed from each user's Assessment Summary page within the tool. It can be viewed directly within the tool and downloaded as a PDF.

Who can the report be shared with?

The report is a valuable internal resource to be used within an entity by anyone who may benefit from the information, but the document must be handled according to the entity's data distribution and security policy.

How many people at my organization can use the tool?

An unlimited number of users at each entity can utilize the CR Assessment Tool, but the number of users depends on the type of role/level of access each person has within their organization. Currently, access to the tool will be granted by RF. Users will be pre-screened by RF based on vetting information provided by entities' Resilience Subject Matter Expert (SME) or Primary Compliance Contact.

RF encourages the involvement of as many applicable SMEs as possible in this assessment in order to derive individual and collective resilience of an entity through increased awareness of contributing factors. Participation is especially important for SMEs in the areas of cyber, IT/OT and physical security, as well as any personnel involved in operations or securing the BPS.

Does the assessment need to be completed by a certain date?

Yes, every user from an entity will be assigned a due date within which that user is expected to complete the assessment. The due date is assigned by RF, and it can be extended upon request.

How often should the assessment be completed?

Entities have the freedom to complete the assessment as many times as desired, on a voluntary basis. By completing the assessment multiple times, entities will be able to benchmark historical CR performance to drive continuous improvement efforts.

Who should I contact if I have questions?

Please visit the RF Contact Us page and choose Resilience from the list of Areas.