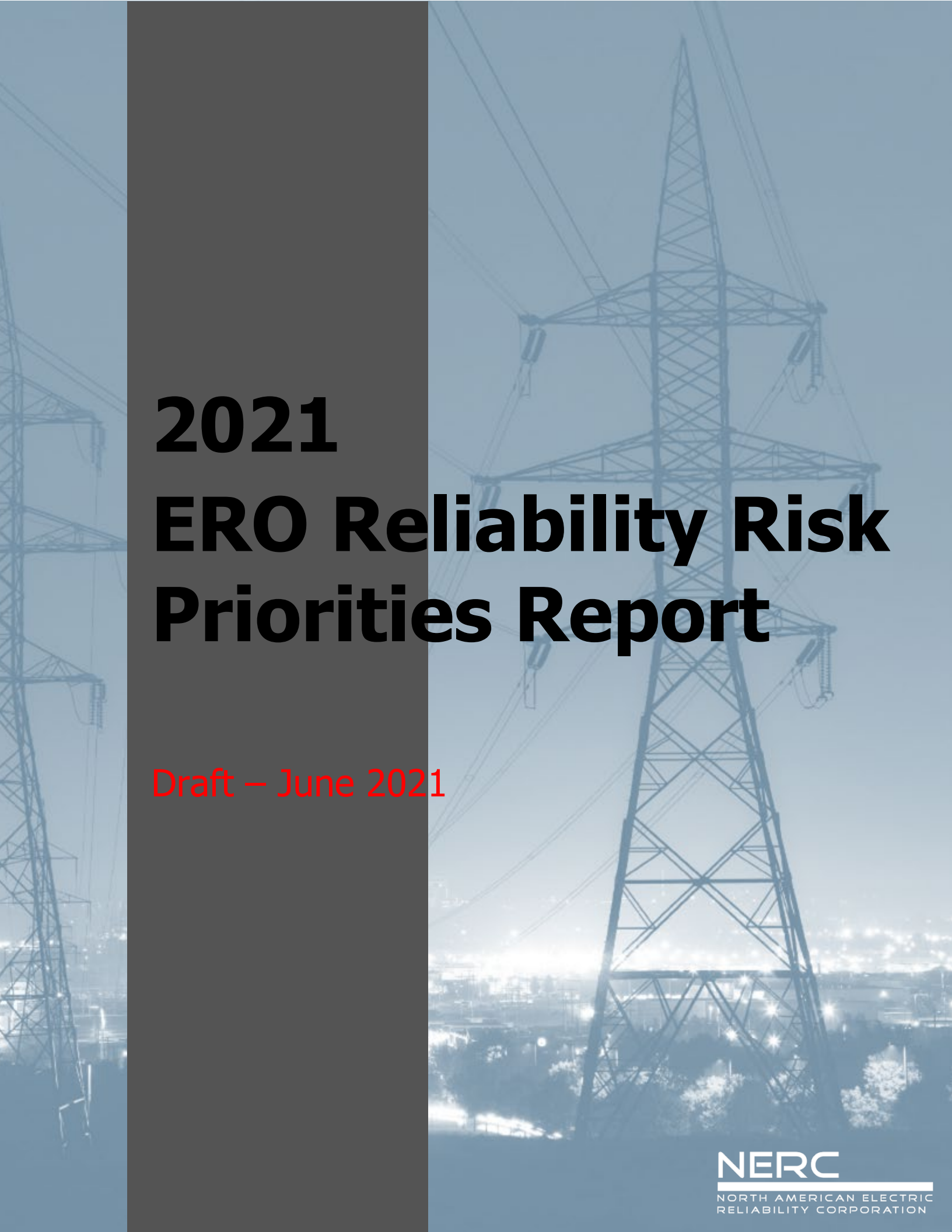


2021 ERO Reliability Risk Priorities Report

Draft – June 2021

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Table of Contents

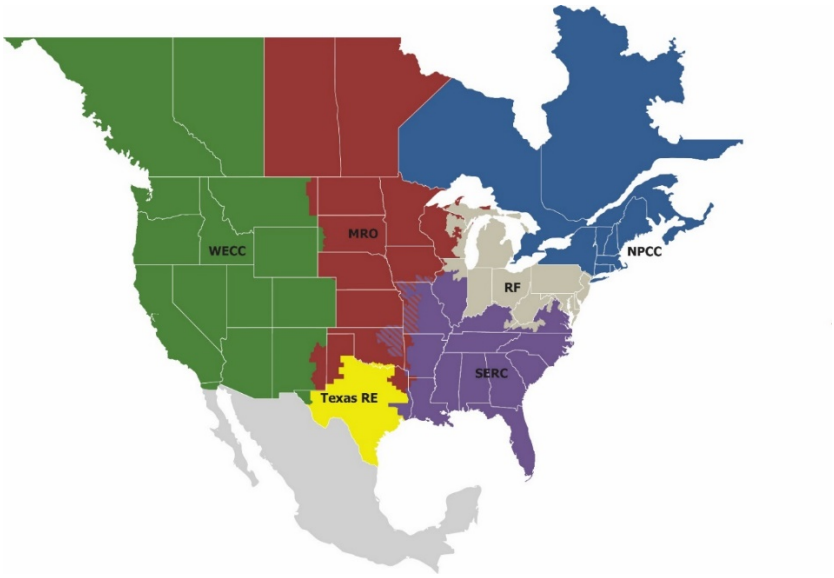
Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (RE), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security

Because nearly 400 million citizens in North America are counting on us.

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Reliability Issues Steering Committee

The Reliability Issues Steering Committee (RISC) is an advisory committee to the NERC Board of Trustees (Board). The RISC provides key insights, priorities, and high-level leadership for issues of strategic importance to BPS reliability. The RISC advises the Board, NERC committees, NERC staff, regulators, REs, and industry stakeholders to establish a common understanding of the scope, priority, and goals for the development of solutions to address emerging reliability issues. The RISC provides guidance to the ERO Enterprise[1] and the industry to effectively focus resources on the critical issues to improve the reliability of the BPS.

This ERO *Reliability Risk Priorities Report* (RISC Report) presents the results of the RISC's continued work to strategically define and prioritize risks to the reliable operation of the BPS and thereby provide recommendations to the Board regarding the approach that NERC, the ERO, and industry should take to enhance reliability and manage those risks.

[1] ERO Enterprise is interpreted to mean NERC, the Regional Entities, and the technical committees of NERC.

Executive Summary

The primary objective of the *2021 ERO Risk Priorities Report* is to report on key risks to the BPS that merit attention and recommend mitigating actions that align with those risks. This report differs from other ERO reports in that it is a forward-looking view of the BPS with the intent to provide industry with potential strategic direction to understand imminent risks and plan for the mitigation of those risks. For example, this is in contrast to the *State of Reliability*[2] report or Event Analysis Reports which reviews data from previous years or events to draw objective conclusions about events, emerging risks and appropriate monitoring for their mitigation. This year's report has been published earlier in the year versus previous reports to provide industry with additional time to plan and budget for potential action plans to mitigate risks.

This report reflects the collective opinion and conclusions drawn from the RISC membership regarding present and emerging risks and their respective priorities. The RISC reviewed and assembled information from ERO Enterprise stakeholders and policymakers[3] and focused subgroup work to evaluate the current set of risk profiles to include the descriptors of the risks and recommended mitigating activities. Additional risks and potential mitigating activities were identified during the 2021 Reliability Leadership Summit that was held in January 2021. The Leadership Summit participants were comprised of industry leaders, executives, and subject matter experts with keen perspective on the inherent and trending risks that affect BPS reliability.

For the 2021 report, the RISC also reduced the number of recommendations. This was completed by consolidating overlapping recommendations and removing recommendations that reflected ongoing activities; though these activities are important, they are already well underway and monitored as part of NERC's Long-Term Strategy Plan and applicable NERC committee plans. This 2021 report builds on the 2019 report, recognizing progress, but also underscoring new risks continue to emerge and often times the potential severity of risks can increase as well. Industry must continue to be vigilant and collaborative to stay in front of those emerging risks and develop mitigating strategies before risks become more impactful.

The **Risk Profiles** section of this report provides a statement, descriptors, and recommendations for mitigating the risk. The RISC recommends actionable mitigating activities that enable the ERO Enterprise and industry to use the composite risk profiles and the mitigating activities map for baseline and recurring evaluations. Grid transformation has broad implications across the other risk profiles, as it catalyzes other changes and often amplifies their effects. As such, while the grid transformation risks and recommendations are broad in nature and overlap to some degree with other Risk Profile sections, grid transformation provides an important framework for this report and its recommendations.

[2] 2019 State or Reliability Report: https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2019.pdf

[3] Policymakers is used generally to mean any organization that can impact the legal or regulatory framework in place at various levels, including local, state, federal, and provincial governmental authorities in addition to various trades and lobbying organizations.

When possible, the RISC also identified the group or organization that it believes should lead the mitigating action. However, some recommendations do not present a clear owner or responsible party. In these cases, the recommendation is presented as a more generalized action item that can apply to numerous entities, including policymakers, industry, and the various organizations within the ERO Enterprise. The RISC did not assess resource needs for the mitigating actions that will be addressed with industry during the annual ERO Enterprise Business Plan and Budget activities.

Additionally, the committee evaluated risks based on impact to the BPS regardless of the source or location of the risk. To evaluate key risks to the system, the RISC recognized emerging issues emanating from different areas of the grid (e.g., resources like distributed energy resources (DERs) which are not located or directly connected to the BPS). Operators and planners of the BPS are aware of the need to have a wide-area view of changes to the system to provide an understanding of external conditions that can affect them. Therefore, the profiles identify several risks where the BPS can be impacted at interfaces (e.g., customers distributed resources, resources located on the electric distribution system, natural gas delivery system, grid infrastructure for energy deliverability telecom system, water system). The RISC is illuminating external factors that increase BPS risk and offer recommendations to address those risks.

Common Themes and Emerging Trends

For risks that the committee recommends active monitoring, a convergence of centralized themes and emerging trends is present. These themes and trends underscore not only the increasing interdependency between identified BPS risks, but also an increase in potential magnitude of emerging risks. Common themes and emerging trends are indicated as follows:

- Interdependencies between industries and fuel types;
- Increased security risks (both cyber and physical);
- The increase in natural gas and renewable variable energy generation coupled with the decline in nuclear and coal-fired generation, and implications resulting on dynamic performance of the BPS;
- The importance of emerging technologies and how to best plan and incorporate those into a reliable and secure BPS ;
- Significant changes to the grid require new models, more advanced tools, and grid infrastructure improvements for reliable integration; and
- Development of credible and centralized data sharing along with the right tools to proactively analyze system conditions is becoming more critical.

Background and Introduction

This report documents the results of the RISC's continued work to identify key risks to the reliable planning and operation of the BPS and provide recommendations to mitigate those risks. This report includes recommendations regarding priorities to assist the Board and NERC management as well as industry and its stakeholders.

The RISC's efforts are both responsive to and in support of the Board's resolutions in connection with the initial 2013 RISC recommendations[4] that direct continued work by the RISC to define and prioritize risks, develop mitigating activities, and identify accountable parties for those risks.

There are important linkages between the risk priorities and the recommended actions for the ERO Enterprise and industry. While the risk profile recommendations in this report are presented individually, there are interdependencies between many of the risks that present unique challenges to the electric industry. These interdependencies have been acknowledged in the report. Further, many of these risks have been long recognized with commensurate NERC and industry monitoring for proper mitigation whereas others are newly emerging, requiring active management with a more aggressive immediate approach necessary for effective foresight and mitigation. The RISC acknowledges and appreciates the increased reliance of the Board and ERO Enterprise leadership on the results of the RISC's activities as an input for the ERO Enterprise's Long-Term Strategy Plan and Business Plan and Budget.

The RISC participants include representatives from the NERC committees, the Member Representatives Committee, and "at large" industry executives. The observations, findings, and guidance presented in this report include input from industry forums, trade associations, and other industry groups through multiple channels. The RISC also received feedback through both the Reliability Leadership Summit and an Emerging Risks Survey.

This report relies on and extends the comprehensive assessment and corresponding recommendations to the Board made in November 2019 that have been updated and refined. This report and recommendations also reflect discussions with representatives from the NERC committees, and the many technical reports and assessments conducted by NERC and industry.

[4] *See* minutes from the Board's February 7, 2013, meeting: http://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/BOT%20-%20February%207%202013%20Minutes.pdf

ERO Collaboration

The RISC has entered into a bilateral communication protocol with NERC's Reliability and Security Technical Committee (RSTC) whereby the RISC will communicate identified risks and mitigating activities and the RSTC will work with industry to implement strategic plans for executing those plans and developing commensurate timelines around those activities.

This framework is meant to guide the ERO in the prioritization of risks and provide guidance on the application of ERO Policies, Procedures, and Programs, to inform resource allocation and project prioritization in the mitigation of those risks. Additionally, the framework accommodates measuring residual risk after mitigation is in place, enabling the ERO to evaluate the success of its efforts in mitigating risk, which provides a necessary feedback for future prioritization, mitigation efforts, and program improvements.

The successful reduction of risk is a collaborative process between the ERO, industry, and the technical committees including the Reliability and Security Technical Committee (RSTC) and RISC. The framework provides a transparent process using industry experts in parallel with ERO experts throughout the process, from risk identification, deployment of mitigation strategies, to monitoring the success of these mitigations.

Six specific steps have been identified, consistent with risk management frameworks used by other organizations and industries: 1) Risk Identification; 2) Risk Prioritization; 3) Mitigation Identification and Evaluation; 4) Deployment; 5) Measurement of Success; and 6) Monitoring. Each of these steps will require process development, including stakeholder engagement, validation/triage approaches, residual risk monitoring, ERO's level of purview over a risk, etc. These processes will be developed once the framework has been finalized.

1. **Risk Identification and Validation:** As mentioned above, the ERO identifies risks using both leading and lagging approaches. The RISC biennial report and Long-Term and Seasonal Reliability Assessments (leading) have successfully brought together industry experts to identify and prioritize emerging risks, as well as suggest mitigation activities. A partnership between the ERO leadership and both the RISC and RSTC enables input from the ERO program areas, industry Forums and trade associations to provide additional context in risk identification.

   Once the ERO, NERC Committees, Forums, or industry subject matter experts identify and validate a risk, it is critical that the corresponding recommendation for mitigation describe, explain, and provide support for the basis for selecting the particular approach to mitigation. A template will be created, that mirrors the Standards Authorization Request template, that requires an explanation of the risk, approach(es) for mitigation, and estimate of residual risk.

Risk Identification: The ERO has a number of ways that it identifies risks:

- ERO stakeholder supported technical organizations, industry forums, and associated subject matter experts
- Focused Compliance monitoring activities
- Reliability and Risk Assessments
- Events Analysis
- State of Reliability Report, including the analysis of Availability Data Systems (BASS, TADS, GADS, DADS, MIDAS, etc.)
- Frequency Response, Inertia, and other essential reliability service measurements
- Interconnection simulation base case quality and fidelity metrics
- Reliability Issues Steering Committee (RISC) Biennial Risk Report
- Regional Risk Assessments
- Communication with external parties, such as DOE, DHS, Natural Resources Canada, CEA and EPRI
- Shared public and/or government intelligence with special emphasis on cyber security

Risk Validation: The ERO and industry subject matter experts continuously work together validating risks to the reliable and secure operation of the BPS based on analysis of ongoing performance of the system (lagging). Validation of the magnitude and priority of the risks includes analysis from the ERO databases of system performance and Events Analysis. These outputs are generally covered in NERC's State of Reliability Report. In addition, the risks are further validated through working with NERC Committees, and socializing them with Forums, government, and research organizations. Leading risk validation requires analysis of system simulations, forecasts, and performance projections.

2. **Risk Prioritization:** Prioritizing risks is accomplished through an analysis of their exposure, scope, and duration as well as impact and likelihood. The primary sources of data used to support this analysis come from the Risk Identification step. Deciding if the risk requires near-term mitigation or continued monitoring is informed by technical expertise. Depending on the complexity of the risk, new models, algorithms and processes may need to be developed to better understand the potential impacts of the risk, which is necessary to develop risk mitigation tactics. The process would be consistent with other risk management frameworks used by other industries, and was recently successfully tested in collaboration with industry through a survey issued by the RISC, based upon the risks that group prioritized in early 2019.

   An ERO risk registry and heat maps are being developed encompassing prior RISC report findings, ongoing technical committee activities, and risks being monitored. This registry is expected to be completed by the end of the third quarter of 2021. Work plans of the technical committees will then be periodically reviewed to ensure that ongoing activities are tied to identified risks in the risk registry. Further, if new risks emerge they can be added to the registry, and if it is deemed that the risks are sufficiently mitigated, they will be moved to the monitored portion of the risk registry. As the RSTC develops its annual work plan and following the publication of the biennial ERO Reliability Risk Priorities Report, the risk registry is reviewed by the RISC and the RSTC to evaluate how completed work addressed these identified risks, whether any new risks have been identified by either committee that need to be added to the risk register, and documenting monitored risks which require no additional mitigation.

3. **Remediation and Mitigation Identification and Evaluation:** The right mix of mitigation activities is balanced against both the effective and efficient use of resources and the potential risk impact and likelihood. Further,

the risk tolerances needs to be balanced against potential impacts so that the remediation/mitigation plans can be developed accordingly. Determining the best mix depends on a number of factors, such as:

- What is the potential impact or severity of the risk?
- How probable is the risk? Is it sustained, decreasing or growing?
- Is the risk here today or anticipated in the next 3-5 years?
- How pervasive is the risk?
- Is mitigation expected to be a one-time action, or ongoing?
- Have we had experience with events being exacerbated by the risks, or there is no experience, but the probability is growing (i.e. cyber or physical security)?
- Have previous mitigation efforts been deployed? If so, were they effective? Why or why not?
- What is an acceptable residual risk level after mitigating activities have been deployed?
- Is the risk man-made or by natural causes?
- Does the mix of mitigations vary based on jurisdictional or regional differences?
- Is the risk fully or partially within the purview of the ERO?

Input from, and allocation of, subject matter expertise through multiple sources is part of this consideration, including resources within the ERO and its stakeholders (such as standing technical committees and their subgroups, or standard drafting teams). External parties are important sources as well, such as the North American Transmission and Generation Forums (NATF and NAGF), North American Energy Standards Board (NAESB), the Institute of Electrical and Electronic Engineers (IEEE), and EPRI, to name a few.

Once a risk to the BES has been prioritized according to its impact and likelihood, the ERO, NERC Committees, Forums, and industry subject matter experts recommend and can take on potential mitigation activities and assess their anticipated effectiveness. Coordination is key to avoid duplication and provide supportive, rather than conflicting actions.

The ERO remains responsible for risks to the reliable and secure operation of the BES. Risk mitigation should still be followed by the ERO no matter which organization takes on activities. Examples of mitigation efforts include, but are not limited to:

- Reliability Standards, with Compliance and Enforcement for risks that are:
  - Sustained, moderate to severe impact, and likely
  - Sustained, severe impact, and unlikely
  - Focused monitoring based on risk, and in response to major events
- Reliability Guidelines for risks that are:
  - Sustained, low to moderate impact, and likely
- Lessons Learned for risks that are:
  - Sustained, low impact, and likely
- Assist Visits for risks that are:
  - Compliance-related

- Focused on a very specific situation or configuration
- Generally on specific industry or entity practices or conditions

- Analysis of Major Events for risks that are:
  - Identified after a Major Event (e.g., Category 3 or higher)
  - Discreet/one-time, severe impact, unlikely
  - identified through recommended reliability improvements or best practices and lessons learned
- Analysis of "Off-Normal" Events for risks that are
  - Identified after an unusual operational condition has occurred and likely not a categorized event.
  - Discreet/one-time, moderate impact, unlikely
  - Identified through recommended reliability improvements or best practices and lessons learned
- Advisories, Recommendations or Essential Actions[5]
- Alerts[6]
- Technical Conferences and Workshops

When reviewing the type and/or depth of remediation and mitigation, a form of cost-effectiveness analysis may be considered to understand impacts and potential burdens. This analysis can then be compared to potential impacts of the risk.

4. **Mitigation Deployment**: Mitigation projects will be deployed by the ERO and/or industry stakeholder groups, as determined by the "Mitigation Identification and Evaluation" step. A specific mitigation plan would involve a suitable mix of the ERO policies, procedures and programs discussed in Section I. These mitigations would be coordinated with Canadian, industry partners and stakeholders.

   From time-to-time, the Federal Energy Regulatory Commission (FERC) may order the development of Reliability Standards, which can occur in this step.

5. **Measurement of Success:** Once a set of solutions has been deployed, the effectiveness of the mitigation must be measured to determine if the residual risk has been reduced to an acceptable level. Effectively, if the desired level of risk mitigation is not met, the risk is fed back to Step 1, enabling a new prioritization of risks, factoring in historic mitigation, ensuring resource allocation is adapted to the changing risk landscape. This step also informs future mitigation efforts, as industry and the ERO learn from the effectiveness of mitigation mixes for reducing risk. A partnership between the ERO leadership and both the RISC/RSTC will enable input from the ERO program areas, industry Forums and trade associations to provide additional context in the measurement of success. That said, criteria and other related processes should be developed for determining risk severity, likelihood, and mitigation activity effectiveness.

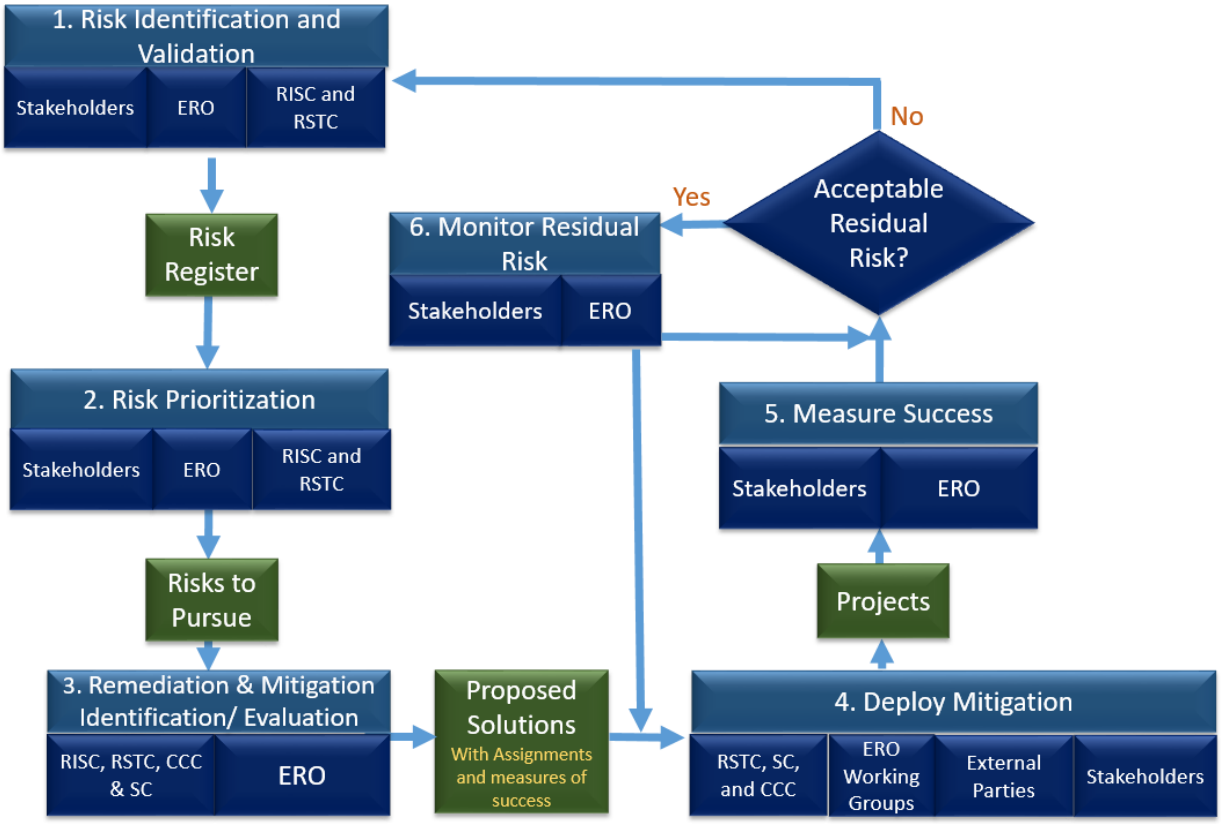
6. **Monitor Residual Risk:** Once the level of residual risk is at an acceptable level, the risk is monitored through ongoing performance measures to ensure that risk remains at acceptable risk levels. The residual risk should be monitored for progress and to ensure that the mitigations that are in place continue to address the risk

[5] LEVEL 1 (Advisories) – purely informational, intended to advise certain segments of the owners, operators and users of the Bulk Power System of findings and lessons learned; LEVEL 2 (Recommendations) – specific actions that NERC is recommending be considered on a particular topic by certain segments of owners, operators, and users of the Bulk Power System according to each entity's facts and circumstances; LEVEL 3 (Essential Actions) – specific actions that NERC has determined are essential for certain segments of owners, operators, or users of the Bulk Power System to take to ensure the reliability of the Bulk Power System. Such Essential Actions require NERC Board approval before issuance.

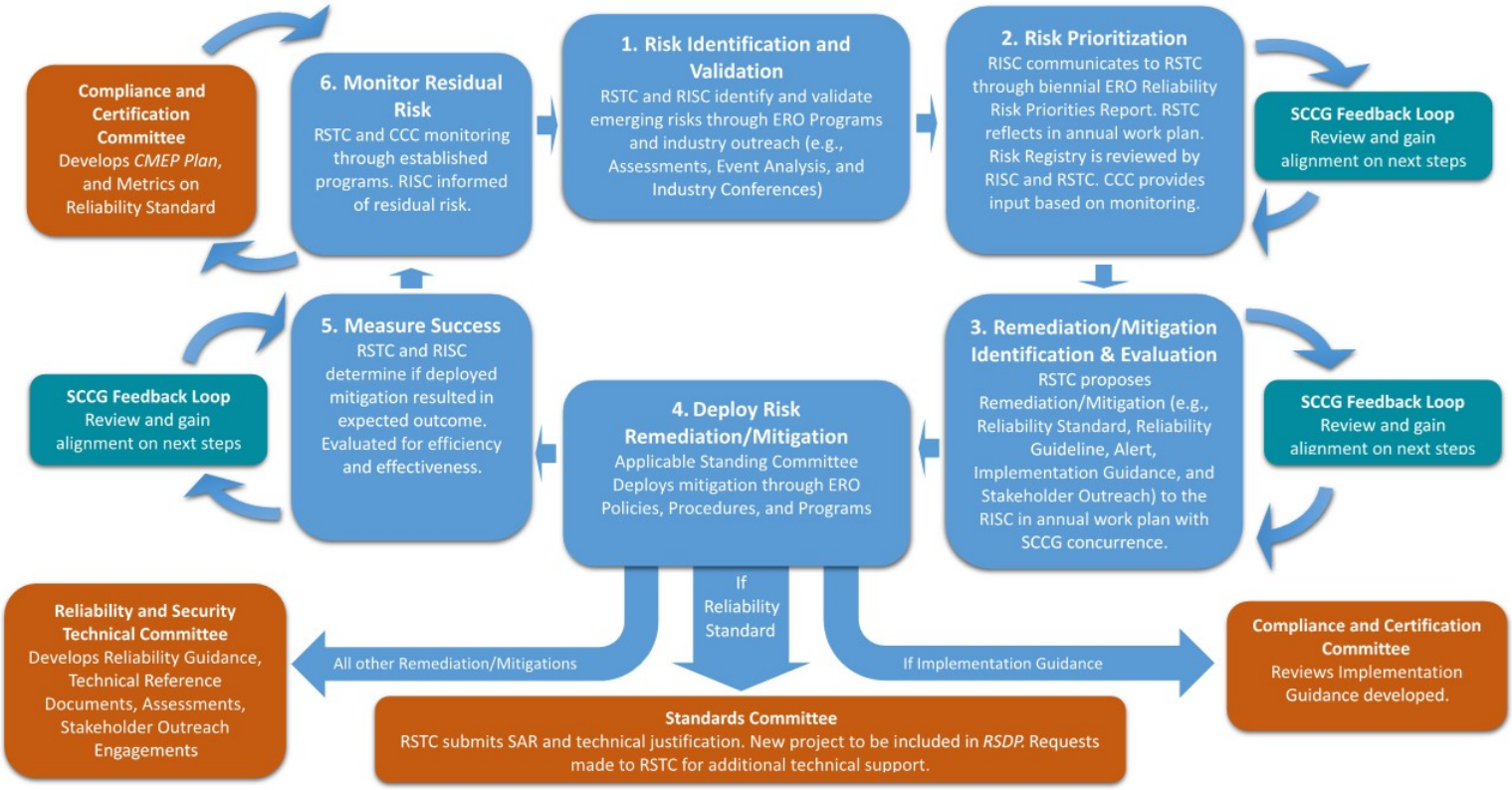
[6] ALERT 1: Industry Action Requested: Fast moving or recently detected, impacts moderate, ALERT 2: Industry Action Required: Fast moving or recently detected, impacts moderate to severe, ALERT 3: Industry Action Mandatory: Fast moving or recently detected, impacts moderate to severe.

(Step 5). At times, mitigations need to be deployed on a periodic basis (e.g. annual workshops, Reliability Guideline updates, etc.) to ensure continued success (Step 4). If the risk levels heighten, or increased mitigation efforts are necessary due to the changing nature of the BPS, the risk can be fed back (Step 1) for prioritization and the development of additional mitigation approaches. The ERO, working with its industry partners, technical committees, stakeholders and forums, would determine if the residual risk was acceptable of if additional mitigations required.

From-time-to-time risks are identified and validated which require an accelerated industry attention. The ERO risk framework can support quick implementation of industry awareness and mitigation activities. Figure 1 provides a pictorial flow chart of the ERO's risk management process.



This risk framework serves to ensure effective collaboration within the ERO and industry, appropriate identification of critical industry risks, and an effective establishment of work plans that ensure mitigating activities are implemented, measured, evaluated, and reevaluated in a strategic and effective manner.


1. Risk Identification and Validation
RSTC and RISC identify and validate emerging risks through ERO Programs and industry outreach (e.g., Assessments, Event Analysis, and Industry Conferences)
2. Risk Prioritization
RISC communicates to RSTC through biennial ERO Reliability Risk Priorities Report. RSTC reflects in annual work plan. Risk Registry is reviewed by RISC and RSTC. CCC provides input based on monitoring.
SCCG Feedback Loop
Review and gain alignment on next steps
3. Remediation/Mitigation Identification & Evaluation
RSTC proposes Remediation/Mitigation (e.g., Reliability Standard, Reliability Guideline, Alert, Implementation Guidance, and Stakeholder Outreach) to the RISC in annual work plan with SCCG concurrence.
SCCG Feedback Loop
Review and gain alignment on next steps
4. Deploy Risk Remediation/Mitigation
Applicable Standing Committee Deploys mitigation through ERO Policies, Procedures, and Programs
5. Measure Success
RSTC and RISC determine if deployed mitigation resulted in expected outcome. Evaluated for efficiency and effectiveness.
SCCG Feedback Loop
Review and gain alignment on next steps
6. Monitor Residual Risk
RSTC and CCC monitoring through established programs. RISC informed of residual risk.
Compliance and Certification Committee
Develops CMEP Plan, and Metrics on Reliability Standard
Reliability and Security Technical Committee
Develops Reliability Guidance, Technical Reference Documents, Assessments, Stakeholder Outreach Engagements
All other Remediation/Mitigations
If Reliability Standard
If Implementation Guidance
Compliance and Certification Committee
Reviews Implementation Guidance developed.
Standards Committee
RSTC submits SAR and technical justification. New project to be included in RSDP. Requests made to RSTC for additional technical support.

Inputs to the Risk Profiles

Reliability Leadership Summit

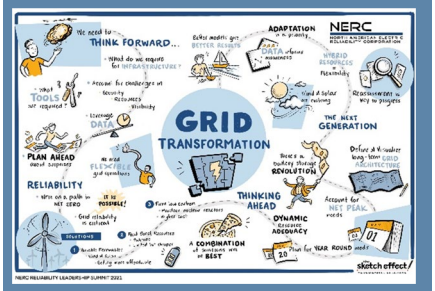
On January 26-27, 2021, NERC and the RISC hosted its first fully virtual summit with leaders of the reliability community, including top industry executives, state and federal regulators, along with NERC and Regional Entity senior leadership. The summit focused on four specific areas: 1) Grid Transformation, 2) Extreme Natural Events, 3) Security Risks, and 4) Critical Infrastructure Interdependencies. Open discussions at the end of each day addressed these and any other risks that required deeper discussion.

The panel discussions underscored the importance of conducting cross-sector coordination with other industries and covered such areas as the transformation of the grid, the challenges that they pose for their integration, and reliability and security impacts and considerations; lessons learned and unique challenges posed by extreme natural events, and ways to prepare for them; cyber and physical security risks, their evolution, and impacts that could cause assess damage; and implications of the increased critical infrastructure interdependencies, and how to address the jurisdictional issues that need to be tackled to address the risks they present.

In addition, a refined Emerging Risks Survey was issued in December 2020 (with responses due mid-January 2021) that sought stakeholder input on the continued relevancy of the eleven (11) individually identified risks, the overall risk profile groups, and the mitigating activities within each of the profile groups as detailed in the 2019 RISC Report. The objective of this year's survey was to gauge if the RISC Report is providing the correct level of information and recommendations to ultimately have an effect in the likelihood and impact to the BPS risks.

As part of the 2020 Emerging Risks Survey, respondents were asked if each of the eleven (11) identified risks from the 2019 RISC Report were still relevant and to rank them from 1-11, with 11 as highest and 1 as lowest. Each risk was identified as still relevant and in evaluating the rankings, the responses were classified as Low (1-4), Moderate (5-8), and High (9-11) to provide an overall view of each risk. The accompanying chart reveals that Changing Resource Mix followed by Cybersecurity Vulnerabilities lead industry perception on the criticality of these risks. This information is useful for industry as a whole to prioritize and dedicate resources and budget. The 2021 report has identified modified risks which will subsequently be incorporated into the 2023 Emerging Risks Survey.

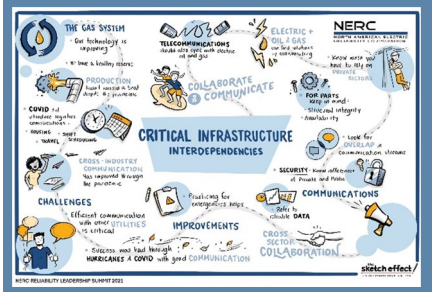
DAY 1: GRID TRANSFORMATION



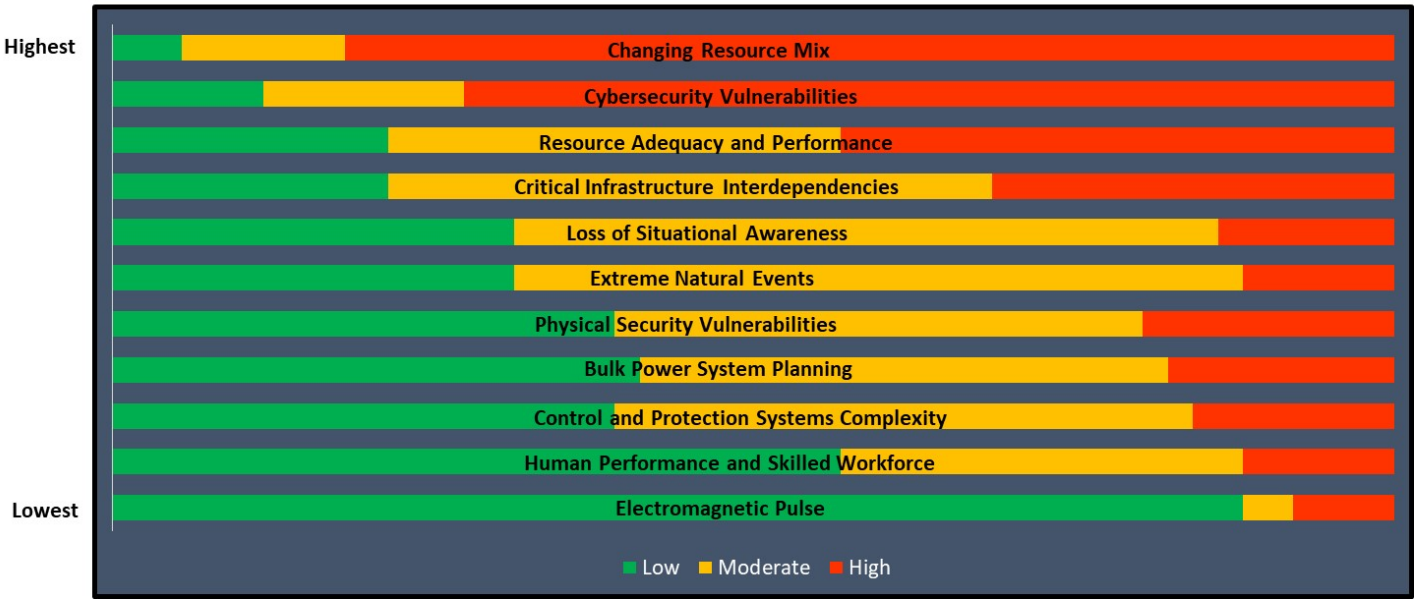
DAY 1 – EXTREME NATURAL EVENTS

DAY 2 – SECURITY RISKS

DAY 2 – CRITICAL INFRASTRUCTURE INTERDEPENDENCIES



Risk Ranking

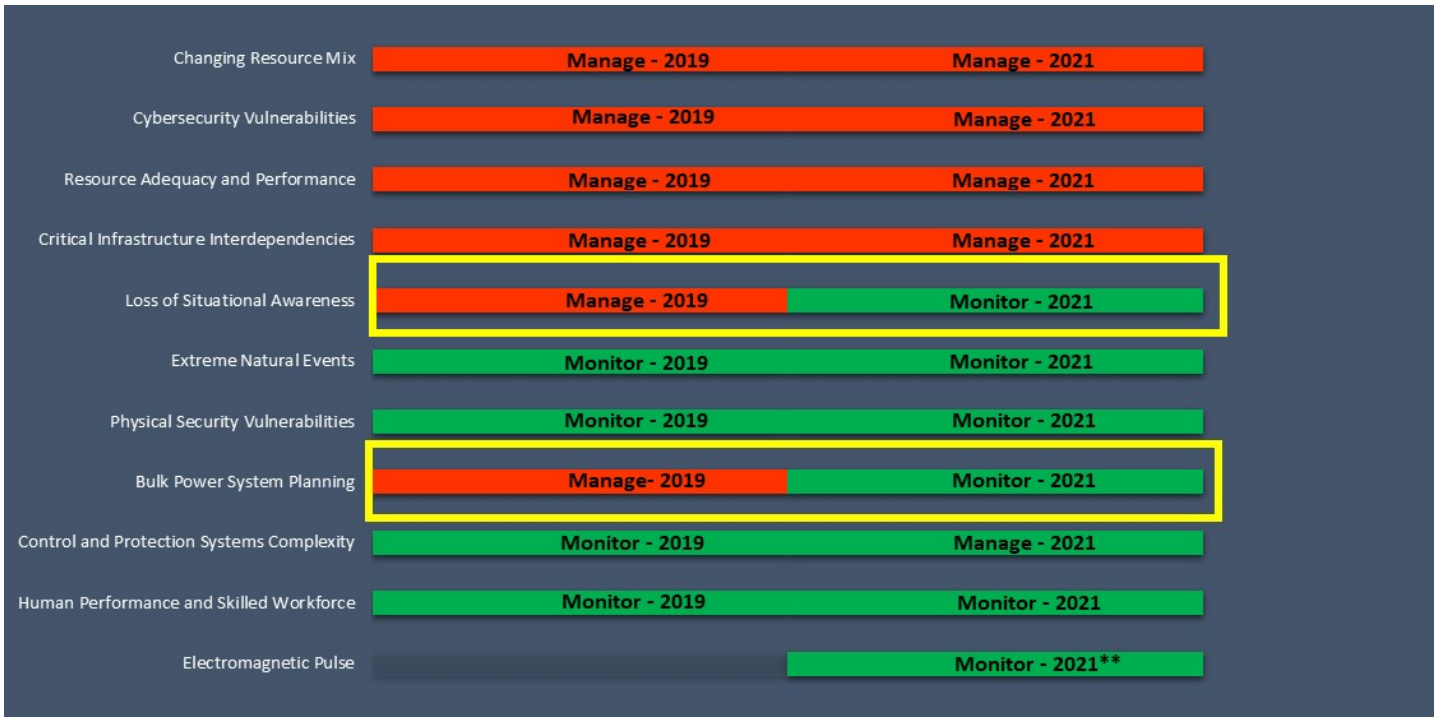


In addition, the graphic below depicts the classification of manage or monitor for each of the identified risks. Those risks identified as "**manage**" are emerging, imminent, and pose significant threats and where thorough strategic planning and industry collaboration are needed for risks mitigation. Those risks identified as "**monitor**" are risks that are of critical importance to BPS reliability, though are considered well managed with established industry practices in place to mitigate and lessen potential impacts to BPS reliability.

The graphic indicates that extreme events should be monitored going forward, which may seem counterintuitive with recent events. Extreme events though is made up of those events in which industry has a great deal of experience, for example hurricanes, tornadoes, derecho, etc., industry has put forth emergency operating plans, usual aid programs, drills, and studies.

With the recent grid transformation, the resource mix is increasingly characterized by one that is sensitive to extreme, widespread, and long duration temperatures as well as wind and solar droughts. For example, having sufficient capacity does not necessarily mean that adequate energy will be available as widespread extreme temperatures are experienced. Neighboring organizations may not necessarily always support each other as they are all experiencing the same conditions.

These risks need to be better understood with mitigation approaches developed to manage them. In the future the RISC may collect information from industry about both those extreme events for which a great deal of experience is available versus those that industry is gaining experience and understanding in due to the grid transformation.



***EMP was not individually surveyed as manage vs. monitor in the 2019 Risk Report.*

Finally, the report was posted for stakeholder comment in June 2021 and comments received were reviewed and incorporated as applicable.

Risk Groupings

Grid Transformation

A. Bulk Power System Planning
B. Resource Adequacy and Performance
C. Increased Complexity in Protection and Control Systems
D. Situational Awareness Challenges
E. Human Performance and Skilled Workforce
F. Changing Resource Mix

Extreme Natural Events

A. Extreme Natural Events, Widespread Impact
   • GMD
B. Other Extreme Natural Events

Security Risks

A. Physical
B. Cyber
C. Electromagnetic Pulse

Critical Infrastructure Interdependencies

A. Communications
B. Water/Wastewater
C. Oil
D. Natural Gas

Though there are fundamental system characteristics that are critical to support BPS reliability such as energy, frequency, voltage, and ramping capability, the sources of each of these are rapidly changing. The resource mix is transforming from large, remotely-located coal-fired and nuclear power plants, towards gas-fired, renewable, and distributed energy resources. The changing resource mix has resulted in a large magnitude of renewable variable energy resources, distributed energy resources, micro- and smart-grids, demand response technologies as well as an increasing reliance on just-in-time delivery of natural gas to fuel new generating capacity. This transformation is causing different utilization of the power lines and changing dynamic performance of the system. In parallel, the potential for cyber and physical attacks has increased as the adoption of advanced technologies compounds the reliance on digital controls and communication systems.

Electrification of many sectors such as transportation and technology continues to increase, which in turn will increase both demand for electricity and the importance of effective management of the significant changes the grid is presently undergoing. There are three main characteristics of this change: decarbonization, digitization and decentralization. Decarbonization is occurring as a result of improved technologies as well as governmental mandates. Increased digitization poses potential challenges from a cyber-security stand point. Decentralization, including proliferation of microgrids and behind the meter generation, is another grid development that necessitates proper system planning and effective deployment of risk mitigation strategies.

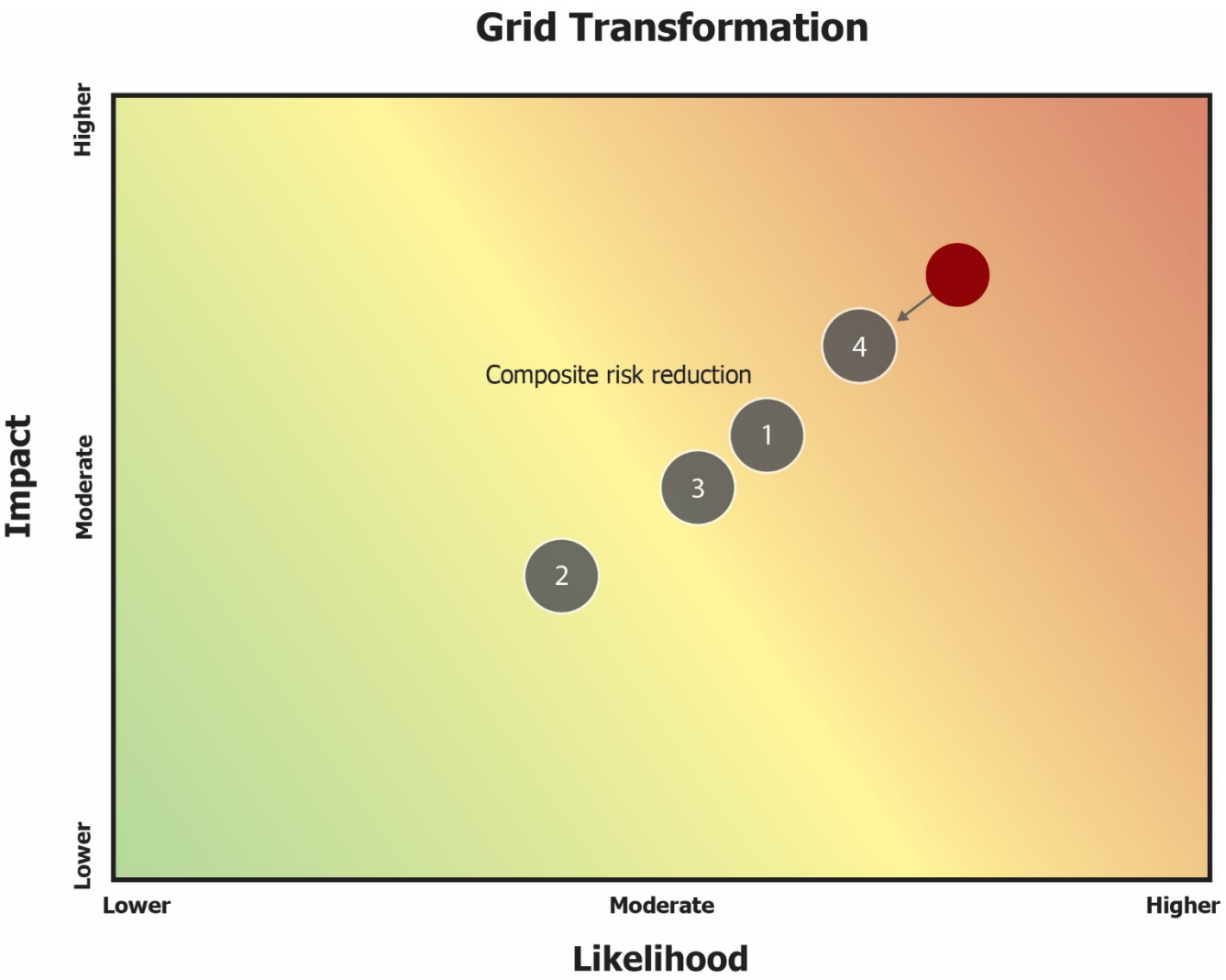
There are four significant evolving risks, which are not independent from each other, that result from these electric industry developments. The **Grid Transformation** includes the shift away from conventional synchronous central-station generators toward a new mix of resources which includes natural-gas-fired generation; unprecedented proportions of non-synchronous resources, including renewables and battery storage; demand response; smart- and micro-grids; and other emerging technologies which will be more dependent on communications and advanced coordinated controls which can increase the potential **Security Risks**. Collectively, these new resources are more susceptible to widespread **Extreme Events** impacting their ability to provide sufficient energy as their fuel supply is less certain. Further, there is an increase in **Critical Infrastructure Interdependencies**. For example, for natural-gas-fired generation, there is increased interdependency on delivery of fuel from the natural gas industry, which also depends on electricity to support its ability to operate.

Each of these risk areas requires steps to mitigate or control their impacts for the continued reliable planning and operation of the BPS. In this way, the goals of the transformation can be met, while at the same time ensuring a reliable, secure, and resilient BPS.

The following graphics, based on the Emerging Risks Survey results and input from the RISC, demonstrates the potential or actual effects that the mitigating activities from the 2019 RISC Report can have if implemented or did have when implemented on both the likelihood and impact of baseline risks. This can be used as a potential tool for industry to compare mitigating activities, their potential

effects, and best use of resources and budget. In addition, these results assisted in the development of the recommended mitigating activities in this 2021 RISC Report as provided below.

In this and the subsequent charts, successful mitigating activities would result in the activity migrating away from the red area and toward the green area (as shown by the direction of the arrow). The numbers identify the mitigating activities themselves as listed in the key below the chart. By implementing successful mitigation activities, survey results should ideally confirm that both likelihood and impact of the risk is reduced.



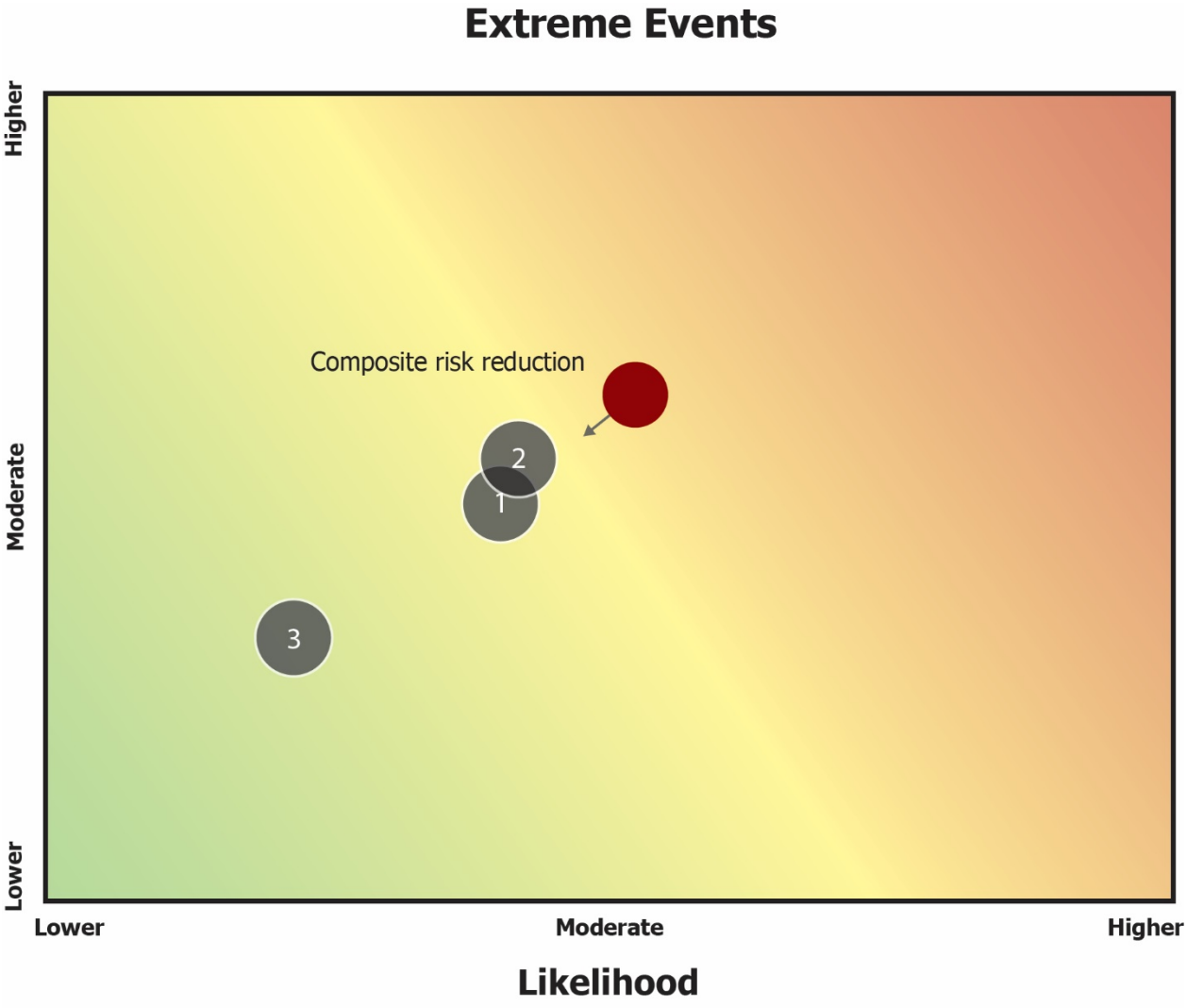
Mitigating Risks Key

1 Update data, modeling and assessment requirements to ensure valid and accurate results given resource and grid transformation (ongoing effort).

2 The technical committees should establish and implement an approach to evaluate the potential impacts of energy storage on reliability.

3 Improve inverter-based resource BPS interconnection and operation and stay abreast of new technologies, such as storage/hybrid resources.

4 Ensure sufficient operating flexibility at all stages of resource and grid transformation.

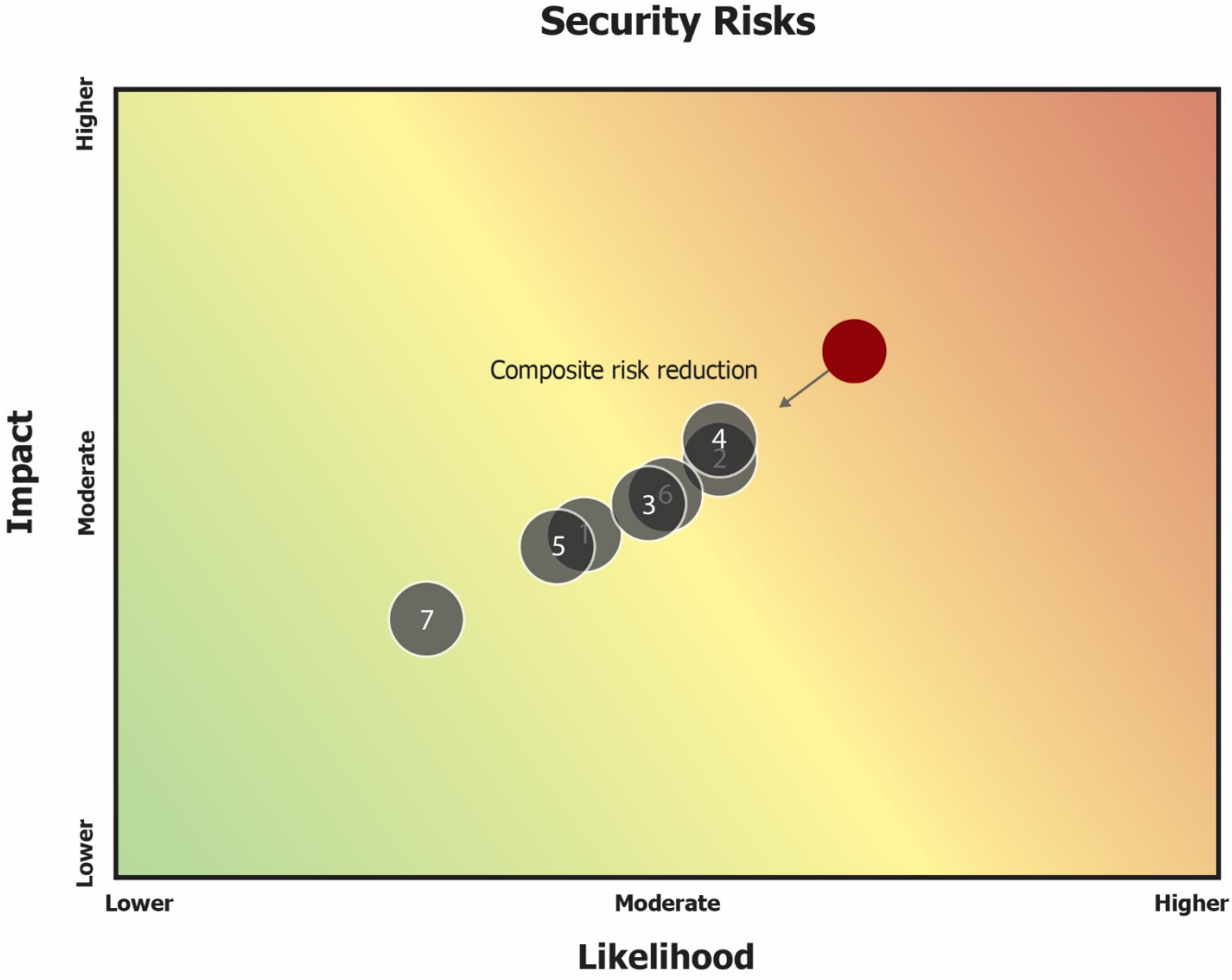


Mitigating Risks Key

1 Special assessments of extreme natural event impacts, including capturing lessons learned, creating simulation models, and establishing protocols and procedures for system recovery and resiliency."

2 Development of tools for BPS resiliency.

3 Understanding of Geomagnetic Disturbance (GMD) events on BPS.



Mitigating Risks Key

1 NERC, in collaboration with industry, should evaluate the need for additional assessments of the risks of attack scenarios e.g., vulnerabilities related to drone activity, attacks on midstream or interstate natural gas pipelines or other critical infrastructure).

2 The E-ISAC should encourage continued industry efforts on workforce cyber education to raise awareness of methods and tactics used by cyber attackers (e.g., email phishing, credential theft).

3 NATF and NAGF should develop supply chain cyber security superior practices.

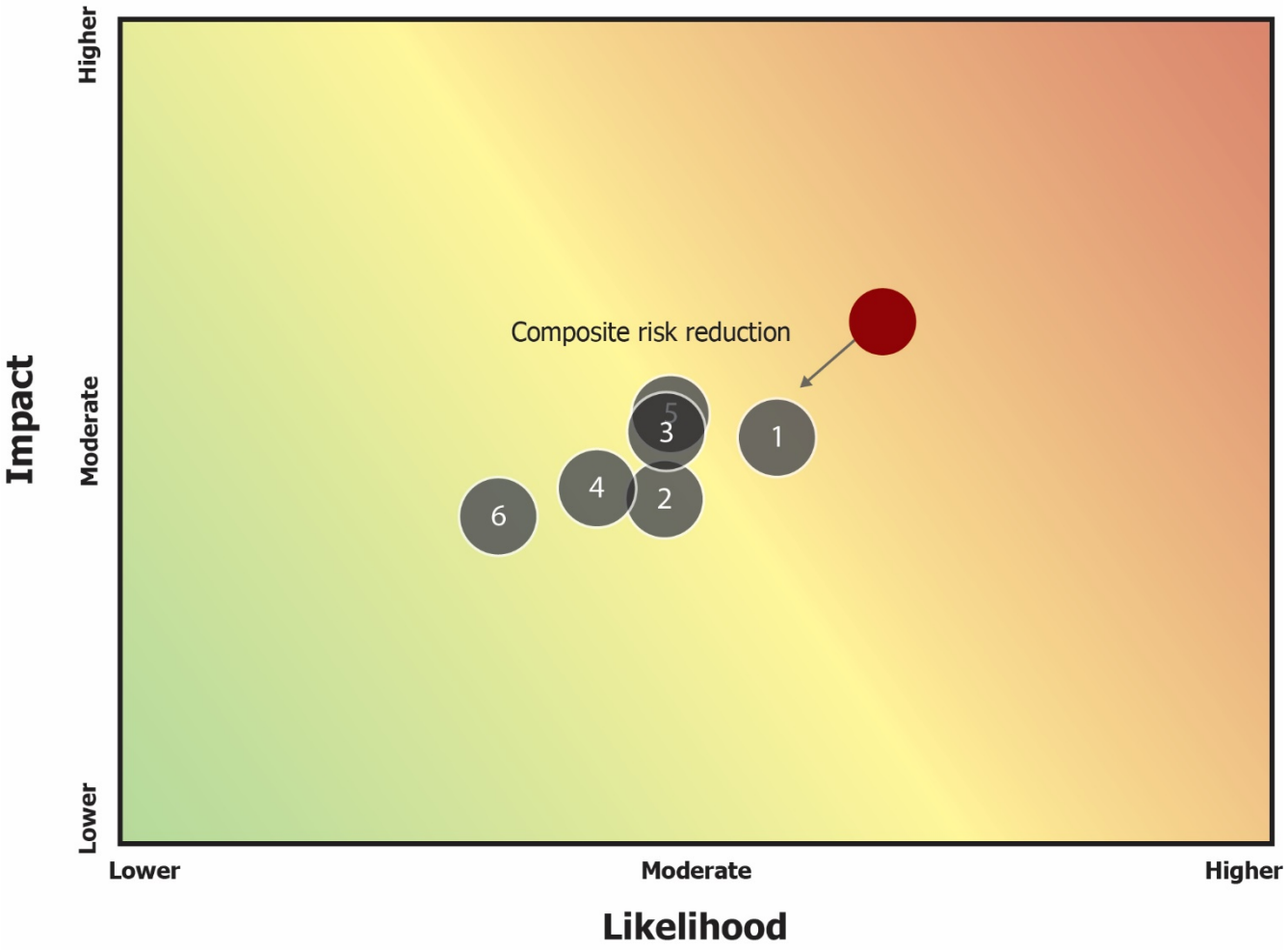
4 E-ISAC should execute a long-term strategy to improve cyber and physical security information-sharing, protection, risk analysis, and increase engagement within the electric sector as well as with other ISACs.

5 NATF, NAGF, Trades Associations, and E-ISAC should develop tiered security performance metrics. Such metrics would track and evaluate events and use predictive analysis to identify and address prospective vulnerabilities on a risk prioritized basis.

6 NERC should facilitate the development of planning approaches, models, and simulation approaches that reduce the number of critical facilities and mitigate the impact relative to the exposure to attack.

7 NERC's EMP taskforce should highlight key risk areas that arise from the EPRI's EMP analysis for timely industry action.

Critical Infrastructure Interdependencies



Mitigating Risks Key

1 NERC, in collaboration with industry and industry partners, should identify and prioritize limiting conditions and/or contingencies that arise from other sectors that affect the BPS.

2 NERC and industry partners should host strategic interactions among critical infrastructure partners (e.g., industry and regulators) to identify and align on mutual priorities.

3 NERC and industry partners should increase emphasis on cross-sector considerations in industry drills (e.g., NERC Grid-Ex, DOE drills, utility exercises (e.g., Southern California Edison (SCE) Resilient Grid Exercise)).

4 NERC should evaluate the need to conduct special regional assessments that address natural gas availability and pipeline impacts under cyber and physical attack scenarios.

5 EPRI and the DOE should continue their work on communication alternatives but also the use of same or similar technologies for critical SCADA data. New technologies should be explored that could assist in providing unique and hardened back-up telecommunication methods for the most critical data.

6 NERC and industry partners should conduct various meetings and conferences to highlight the importance of cross-sector interdependence and coordination, such as the NERC Reliability Summit, NATF/EPRI resiliency summits, and FERC/DOE technical conferences.

Risk Profile #1: Grid Transformation

Statement of the Risk

Changes in generating resources, fuel sources and fuel deliverability, energy deliverability to the load, and load characteristics are accelerating, challenging the traditional methods of long-term planning, short-term planning and real-time operations.

Regulatory and socioeconomic policies for grid transformation have significantly increased since the prior report, initially driven by the decarbonization goals of states, utilities and customers. Now, the new federal administration appears likely to further accelerate the significant evolution of grid resources with infrastructure improvements. The shift away from conventional synchronous central-station generators toward a new mix of resources continues to challenge generation and grid planners and operators. This new paradigm of the resource mix includes natural-gas-fired generation; unprecedented proportions of non-synchronous resources, including renewables and battery storage; demand response; smart- and micro-grids; and other emerging technologies. Recent events have raised awareness of how extreme events and fuel supply interdependencies may result in energy sufficiency issues for all types of resources, and it becomes even more important to revisit resource adequacy concepts, modeling methods, operating practices, and the data that are needed for reliable planning both on generation and transmission, modeling and operation of the rapidly transforming grid. Looking forward, policy requirements to decarbonize the energy systems, changes in the economics of various energy sources, deployment of storage in many configurations, participation of distribution-connected resources and the aging of existing infrastructure will alter the nature and dispatch of generation, leading to further resource and grid transformation.

This transformation presents a number of potential challenges and opportunities when it comes to reliability of the BPS as detailed in the risk descriptors below. Grid transformation has broad implications across the other risk profiles, as it catalyzes other changes and often amplifies their effects. As such, while the grid transformation risks and recommendations are broad in nature, they provide a vital framework for all of the RISC recommendations in this report.

Descriptors of the Risk

- **Changing Resource Mix, Bulk Power System Planning, and Resource Adequacy and Performance**
  - **Resource Adequacy Assessment Scopes – Network Realities versus Political Boundaries**: Current resource planning and resource adequacy assessments are often performed with a limited scope (political or utility boundary) that does not take into account potentially significant electrical impacts and interactions due to the interconnected nature of the bulk grid outside of that limited scope. The result may be resource or energy or transmission capacity insufficiencies in operational timeframe.
  - **Consideration of Weather, Forecasting and Combined Effects**: With the changing resource mix, traditional analytical methods do not fully account for system characteristics associated with the uncertainty of variable resources, interactions of inverters and dynamic power system devices, declining performance of fossil fueled resources that are nearing retirement, uncertainties associated with emerging technologies, and increased sensitivity to widespread common weather such as extreme temperatures. The result may be resource or energy or transmission capacity insufficiencies in the operational horizon. Forecasts of weather and energy demand, and the implications of such forecasts on the increasingly interrelated combined effects with resources, fuel supplies and extreme events, must continue to be improved and advanced.
  - **Resource Adequacy does not necessarily equal Energy Adequacy:** Resource adequacy assessments have mostly focused on generation and transmission capacity available to serve peak demand. With the previous resource mix, real-time energy adequacy was assumed under that capacity umbrella and transmission was not highlighted as a requirement; however recent extreme temperature events have shown energy adequacy to be a new dimension of risk given the changing resource mix and actual performance of the grid versus assumptions used in previous resource mix studies.
  - **Potential Impact on Essential Reliability Services:** Transformation of the resource mix can alter the provision of and need for Essential Reliability Services and other ancillary services needed for BPS reliability and system operations, such as voltage control and reactive support, frequency response, and ramping/balancing. Restoration services, such as blackstart capabilities and procedures, could be affected as well. Organized and bilateral markets must recognize and incent resources which are capable of providing Essential Reliability Services to ensure reliable operations.
  - **Technology with Different Design and Performance Characteristics:** The continued integration of large amounts of new resource technologies (e.g., DERs, grid and distribution system-connected inverter-based resources, and energy storage) could lead to inaccurate forecasting of anticipated net demand. The dynamic and transient performance and response of these technologies also brings new challenges. Changing technology also has implications for control and protection systems complexity as is further described below.
  - **New Data and Information Requirements:** The need for data and information about new and changing resource characteristics must be incorporated into the long-term planning, operational planning, and operating time horizons. Further, this integration can also result in other planning and operational challenges if these resource additions are not observable or predictable or are otherwise not accounted for. Some of this new information will be from nontraditional sources (e.g., DERs and inverter operating parameters) that may present challenges to those responsible for incorporating the information into models representing future conditions.
  - **Energy Storage Technologies:** Storage capabilities and uses will likely transform both distribution and bulk system operations. Whether in combination with renewable or conventional resources and whether connected to distribution systems or the BPS, storage and hybrid technologies will further magnify the pace of innovation and the evolution of resource capabilities during both steady state and transient conditions.

- **Fuel Supply Considerations:** Fuel sourcing and disruption, such as from weather events and other extreme natural events, are driving new scenarios and case studies and broadening the range of dependencies for reliability planning and operations. Fuel constraints and environmental limitations might not be sufficiently reflected in current assessments of resource adequacy.
- **Resource Adequacy Elements Timeline Consideration:** In addition to fuel sourcing, other elements of resource adequacy (e.g., transmission development, generator retirements, pipeline construction, and environmental permitting, right away acquisition) may require long-lead time to assure future reliability and resource adequacy of the system. Various elements may also need to be carefully sequenced to ensure reliability throughout the transition, and the interrelated nature and contribution of transmission, generation and fuel sources must be appreciated and considered in resource adequacy assessments, timelines and deployments.
- **Ensuring Sufficiently Flexible Resources to Meet Demand:** With the expected volume of wind and solar resources and their characteristic fuel-driven commitment and dispatch capabilities, as well as the characteristics of other resources that may constrain their near-term ability to respond, sufficient amounts of flexible resources will be needed to meet demand when the less flexible resources are unavailable. The flexible resources will need to be dispatchable within the forecasting period of the fuel-driven or less flexible resources becoming unavailable.
- **Coordination of Behind-the-Meter DERs with the BPS:** Distributed generation, distributed storage and other DER technologies currently follow local interconnection requirements and operational protocols, posing potential challenges to the BPS from a planning and forecasting perspective as penetration levels increase.

- **Human Performance and Skilled Workforce:** The BPS is becoming more complex, and the industry will have difficulty staffing and maintaining necessary skilled workers as it faces turnover in technical expertise. The proliferation of entities providing services and grid transforming technologies will compete for available skilled workers
- **Loss of Situational Awareness:** Loss or degradation of situational awareness poses BPS challenges as it affects the ability of personnel or automatic control systems to perceive and anticipate degradation of system reliability and take preemptive action. Maintaining situational awareness will become increasingly complex as the numbers and types of resources expands from the Bulk Electric System to the distribution system.
- **Control and Protection Systems Complexity:** The interaction and performance of control systems during transient events, including the control systems in remedial action schemes (RAS) and other protection systems, must be understood to prevent new common-mode failures that may not have been anticipated (e.g., the inverter performance as demonstrated during the Blue Cut Fire and related events, misoperation of RAS logic and control systems, interdependencies of RAS operations in sequence and follow through).
- **Cybersecurity Risks:** With the expansion of resources and participants down to the consumer level, the number and types of Cybersecurity Risks will evolve and expand. Awareness of this threat, improved planning approaches to build in cyber robustness, and application of best practices will be necessary to promote reliable operations.

Recommendations for Mitigating the Risk

As a result of this complex set of factors, the traditional methods of assessing resource adequacy (i.e., by focusing primarily on generating capacity, transmission and pipeline capacity, and fuel availability at traditional peak load times) may not accurately or fully reflect the ability of the new resource mix to supply energy and reserves for all operating conditions. Historic methods of assessing and allocating ancillary services (e.g., regulation, ramping, frequency response, and voltage support during transient, recovery and follow through) may no longer ensure that sufficient Essential Reliability Services and contingency reserves are available at all times during real time, next hour, and next day operations. Balancing and ramping concerns that up to now have been largely confined to limited

locations will likely expand regionally as solar and wind generation continues to grow and provides a larger portion of the energy mix. Changes in resources will increasingly challenge concepts of available capacity in traditional integrated resource planning models and methods, likely leading to a need to revise resource adequacy, energy adequacy, and transmission adequacy concepts to assure reliability of the BPS in near-term to long-term planning horizons.

The combination of these many factors related to resource and grid transformation offer both challenges and opportunities as a result of the transformation and call for a planned set of NERC activities as described in the following action plan.

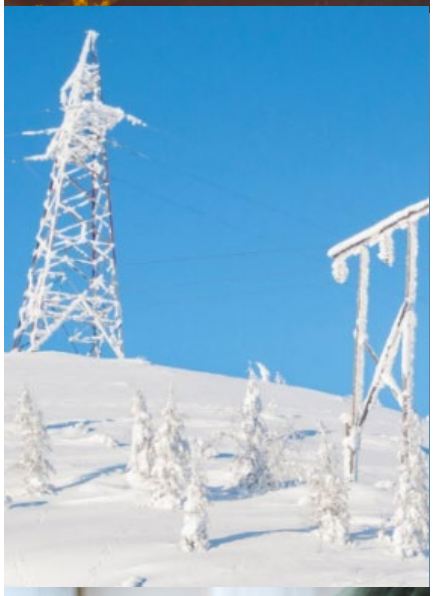
Resource and grid transformation will require new and updated tools, methods, and strategies that are used in planning, modeling, and operating the BPS. To best achieve those goals, the RISC encourages the following actions:

- **Ensure sufficient operating flexibility at all stages of resource and grid transformation:** System operators and planners should ensure sufficiently flexible ramping/balancing capacity is available as a tool to meet the needs of changing patterns of variability and new characteristics of system performance. Traditional concepts of resource adequacy may need to evolve to consider adequacy and flexibility during all hours, including consideration of correlated outages, transmission availability and common-mode fuel supply dependencies.
- **Update data, modeling and assessment requirements to ensure valid and accurate results given resource and grid transformation (ongoing effort):** The Reliability and Security Technical Committee (RSTC) should identify the information and modeling capabilities needed to ensure the efficacy of assessments while taking into consideration the complex and interrelated aspects of the ongoing transformation, including the evolving nature of resource adequacy itself. The ERO should continue to pay attention to settings of controllable devices, remedial action schemes, and power electronics installed to stabilize the system.
- **The RSTC should establish and implement an approach to evaluate the potential impacts and benefits of energy storage, hybrid/storage resources, aggregated DER resources and other emerging technologies on reliability:** Work with industry stakeholders to use available information and experience to support an evaluation of these rapidly emerging and evolving technologies. It is important that the operators of these emerging technologies participate in the ERO process to provide input and implement these recommendations, especially at the distribution level.
- **Improve inverter-based resource BPS interconnection and operation and stay abreast of new inverter technologies:** The ERO Enterprise should continue its effort to address the recommendations of the Inverter-Based Resource Performance Working Group (IRPWG).[7] Ongoing advances in inverter technologies, including those resulting from encouraging work of the IEEE P2800 equipment standard and grid-forming inverter research, should also be reflected in ongoing efforts of the IRPWG and related aspects of the ERO Enterprise. With future adoption of technical guidelines and equipment standards, and soon with selective deployment of emerging grid-forming inverter technology when needed, inverter-based resources will make important contributions to BPS reliability during grid transformation.

- **Development of methods, process, tools, metrics, and/or standards are needed to address energy security:** Recent experiences have demonstrated that capacity alone, given the grid transformation, is not sufficient to ensure sufficient energy is available to serve consumer needs. Capacity analysis is vital, but now must be buttressed with energy assessments to ensure that the system is planned and operated in a way that provides sufficient energy event during widespread, long duration extreme conditions.

[7] IRPTF Recommendations - https://www.nerc.com/comm/PC_Reliability_Guidelines_DL/Reliability_Guideline_IBR_Interconnection_Requirements_Improvements.pdf

Risk Profile #2: Extreme Events



Statement of the Risk

Extreme events (e.g., storms, wildfire, extreme temperatures etc.) cause a significant proportion of major BPS impacts. For example, NERC's 2019 *State of Reliability* report[8] noted weather was responsible for both Category 3 events (there were no Category 4 or 5 events) across the ERO Enterprise's footprint in 2018. Extreme weather events tend to be regional in nature. Natural events may affect BES equipment, resources, or infrastructure required to operate the BES. Certain events are unique to areas that they impact while others may occur in any area of the BPS. Extreme weather events historically have been regional in nature. Planning studies confined to regional boundaries may not account for events that cross regional boundaries. Recent cold weather events in ERCOT, MISO, and SPP, as well as heat events like 2020 California event, underscore that not only do extreme events pose challenges due to the nature and frequency of the extreme event itself, but that the grid transformation that is occurring also heightens the effects and complicates mitigation of an extreme event. Each type of event brings unique challenges from energy supply sufficiency, spare-parts availability, delivery, and restoration perspectives. Impacts from recent weather-related events have resulted in longer duration load loss, exacerbating human impacts due to the inability to access other needed critical infrastructure. Preparation and proactive planning of procedures and protocols are critical for utilities to assess and determine appropriate steps for both reliability and resiliency.

Other extreme events such as pandemics and threats to national security can pose challenges to grid reliability. Most notably, the Covid-19 Pandemic altered almost all aspects of management of the power grid in one way, shape, or form. For these reasons the 2021 Risk Report reflects this profile as Extreme Events rather than specifically to extreme natural events as identified in the 2019 Risk Report.

The performance and solutions relied upon historically are not always an indicator of future performance as events of the recent past and resulting outages indicate. The BPS now has new technologies and resources that have often times not experienced extreme weather phenomena in the quantities seen on the BES today. Further, the performance of the evolving resource mix appears to be more sensitive to extreme events.

While this does not signal that new technologies and resources are not capable of operating in extreme conditions, it does underscore the need for analysis as inverter based resources, distributed energy resources and behind the meter generation become more prevalent. The precise risk of these having widespread impacts cannot yet be proven because the full penetration of these resources is yet to be realized. However from a planning and preparation perspective these cannot be ignored. Other risks described in this report can be "driven" by extreme events. Grid Transformation, Cyber Threats, and Critical Infrastructure Interdependencies all have underlying issues that can be exacerbated with the advent of extreme events.

[8] https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2019.pdf

Descriptors of the Risk

Various North American regions routinely incur severe events, such as hurricanes and extreme cold weather. While the risk of these events in those regions is high, the relative impact on the BPS is low. See the following examples:

- **Hurricanes:** They can cause widespread destruction to BES equipment, degradation of communication capabilities, loss of load, and damage to generation resources. Recovery and restoration efforts can be hampered due to the size or scope of the storm and damage to interdependent infrastructure.
- **Tornados/Derecho:** They can cause localized destruction to BES equipment, local degradation of communication capabilities, loss of load, and damage to generation resources. Recovery and restoration efforts can be hampered due to local damage to interdependent infrastructure
- **Extreme Heat and Drought:** They can cause higher than anticipated demand, overloading and failure of BES equipment, and degradation of resource availability. There can be limited water available for operating hydroelectric generation or reduced cooling water capacity. Drought can also be a precursor to wild fire risk as described in the next bullet.
- **Wild Fires:** They can be a direct threat to BES equipment. Pre-emptive actions must be taken to de-energize equipment without causing additional cascading effects in areas where wild fire risk is significant.
- **Flooding:** This can occur in any area and in any season of the year. The impacts from flooding include mechanical damage to BES equipment, degradation of clearances, fuel infrastructure, personnel access, and communications capabilities.
- **Extreme Cold Weather (Polar Vortices):** This can cause higher than anticipated demand, overloading and stress failure of BES equipment, increased reliance on interdependent critical infrastructures, and degradation of energy availability via resource mechanical failure or fuel supply interruption.
- **Ice Storms:** They can be a direct threat to BES equipment. The impacts from these storms, combined with high winds, include infrastructure damage, personnel access and communication capabilities.

Other types of severe natural events, though less likely, could have a higher impact given the potentially broader geographic footprint. See the following examples:

- **Earthquakes:** These are possible in many areas of the United States and Canada. Depending on the scope and magnitude of the event, mechanical damage may occur to BES facilities and interdependent critical infrastructure (e.g., communications, fuel, transportation). The duration to recover from earthquakes could be long, and further assessment and coordination is required among utilities and the ERO Enterprise.
- **Geomagnetic Disturbances:** These can induce harmonic currents in BES circuits and equipment. In addition the impacts of these disturbances result in induced currents that may overheat of transformers, result in relay misoperations, and increased reactive demand or damage to reactive resources. GMD events can also affect communications capabilities, fuel delivery, and GPS systems.
- **Pandemics:** The Covid19 Pandemic forever altered the way the BPS is operated. Effective telecommuting and cloud-based data exchanges enabled the grid to almost seamlessly continue reliable operation, resulting in no major disruptions to power deliveries. However, this new paradigm also underscores the necessity to maintain proper controls and protocols for security around both systems and human capital.
- **National Security Risks**: Civil unrest, riots, and other events could create potential issues around physical security of the BPS as well as safety of critical personnel necessary to carry out the actions needed to maintain the reliable operation of the BPS.

Recommendations for Mitigating the Risk

Extreme events and their potential impacts on BPS reliability should be monitored and addressed to maintain reliability and improve resiliency. Based on uncertainties predicting some events, it is important for operations and

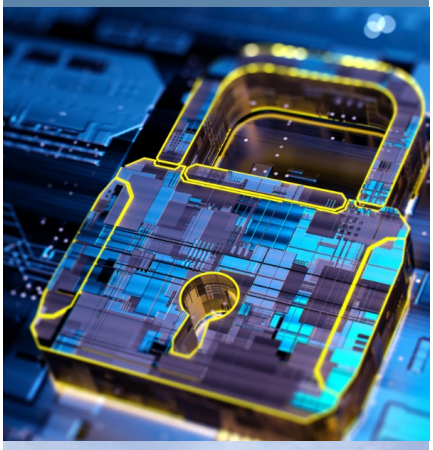
planning personnel to remain vigilant and prepare for high-risk seasons by learning from prior events, practicing recovery efforts, and anticipating impacts of an event to critical infrastructure. Seasonal reliability assessments should consider how more prolonged and widespread natural events may stress the system. Sufficient capacity and energy is needed to prepare for, operate, or when necessary, restore the BES. NERC and industry have taken actions to mitigate some of these risks by recent efforts in developing a Cold Weather standard for generators, the development of a joint NERC/WECC guide on effective management of wildfire, and the formation of the Energy Resource Adequacy Task Force. Further, certain regions may become more dependent on neighboring regions if greater than anticipated forced generator outages occur. These dependencies should be identified.

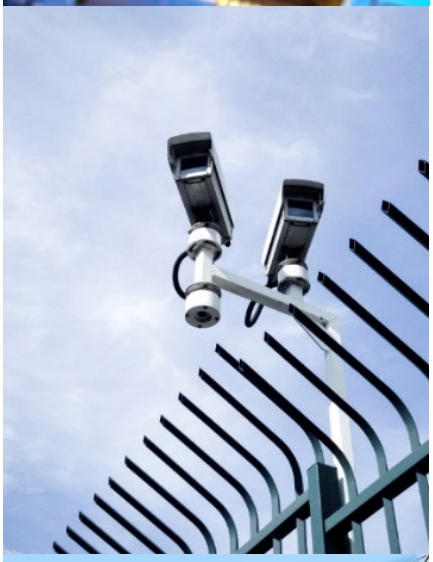
In order to continue the efforts toward mitigating the effects of extreme events, the RISC encourages the following actions:

- **Special assessments of extreme event impacts, including capturing lessons learned, creating simulation models, and establishing protocols and procedures for system recovery and resiliency:** The ERO Enterprise should conduct detailed special assessments of extreme event impacts by geographical areas that integrate the following:
  - Critical Infrastructure interdependencies (e.g., telecommunications, water supply, generator fuel supply)
  - Analytic data and insights regarding resilience under extreme events

  Based on those assessments, the ERO Enterprise should develop detailed special assessments on possible mitigation plans and provide a roadmap for their implementation. The roadmap should include specific protocols and procedures for system restoration and system resiliency.
- **Development of tools for BPS resiliency:** The Department of Energy (DOE) is in process of developing the North American Energy Resilience Model (NAERM) to evaluate both static, dynamic, and real time scenarios that affect grid reliability. NERC should continue to work with DOE on this effort to ensure a robust tool that can be used industry wide to evaluate potential threats to generation, transmission, and fuel supplies.
- **Understanding of Geomagnetic Disturbance (GMD) events on BPS:** The ERO Enterprise should assist the industry to implement the necessary protocols and mitigation plans to reduce the risk and maintain reliability and security for the BPS.
- **FERC/NERC joint inquiry on cold weather outages in ERCOT, MISO, SPP:** The ERO Enterprise should continue to work with FERC to better understand the root causes of the cold weather outages in ERCOT, MISO, and SPP. Actions in the final report, when released, should be implemented and facilitated by NERC and the ERO. NERC should conduct analysis to determine the effects of the existing cold weather event to other cold weather events in the past, taking into account the difference in the resource mix over time and the performance of those resources during these widespread extreme temperature events.
- **Regional coordination:** States should meet, discuss, and understand impacts to ensure a part of the resiliency discussion. This coordination will ensure the acknowledgement of roles in understanding the impacts and implementing mitigating activities.
- **Industry forums** should share and coordinate information sharing on best practices around resiliency efforts related to design considerations and identification and response to major storm events. Sharing experiences and best practices is critical.

Risk Profile #3: Security Risks





Statement of the Risk

Operational security is an essential element of a highly reliable BPS (BPS). Cyber and physical security are interdependent aspects, as exploitation of either physical or cyber security vulnerabilities could be used to compromise the other dimension. Resultant impacts could cause asset damage, functionality loss, or limit the situational awareness needed to reliably operate or promptly restore the BPS. Additionally, the operational and technological environment of the BPS is evolving significantly and rapidly, potentially thereby increasing the potential cyberattack surface. Sources of potential exploitation include increasingly sophisticated attacks by nation states, terrorist, and criminal organizations. Vulnerability to such exploits are exacerbated by insider threats, poor cyber hygiene, supply-chain considerations, and dramatic transformation of the grid's operational and technological environment. These transformative changes include convergence of information and operational technology (IT/OT), reliance on cloud-based technology, and potential workforce knowledge gaps. Additional automation and integration of OT networks is increasing the attack surface of cyber risk, while the use of cloud-based hosting or services introduces the risk of code and/or data breach vulnerabilities through the use of third party software and/or hardware.

Exploitation could occur directly against equipment used to monitor, protect, and control the BPS or indirectly through supporting systems, such as voice communications or interdependent critical infrastructure sectors[9] and subsectors (e.g., water supply and natural gas used for electrical power generation). A coordinated cyber and physical attack scenario that is, potentially targeted to occur simultaneously with an extreme natural event, could further impact reliability and/or complicate recovery activities. A man-made electromagnetic pulse (EMP) event targeted at the BPS may impact operations and result in damaged equipment that may require extensive time to replace

[9] https://www.dhs.gov/cisa/critical-infrastructure-sectors

The following graphic, based on the Emerging Risks Survey results, as well as input from the RISC, demonstrates the potential effects that the mitigating activities from the 2019 RISC Report can have on both the likelihood and impact of baseline risks and can be used as a potential tool for industry to compare mitigating activities, their potential effects, and best use of resources. In addition, these results assisted in the development of the recommended mitigating activities provided below.

Descriptors of the Risk

Whereas the incidence of both cyber and physical security attacks specifically targeted against the BPS have to date not shown any clearly increasing trend, recent threats in other industries underscore a need for increased vigilance and a much more concerted effort to develop counter- measures to prevent and/or recover from more serious attacks against the electric industry.

- **Physical Security Risks:** The nature and impact of physical vulnerabilities are better understood than other security risks (e.g., cyber or EMP). The impacts from significant physical attacks are likely to be more localized geographically. There is modest, ongoing evolution of the physical security risk via drones. The largest risk considerations are considered to be the co-dependence with cyber security (e.g., computer controls for physical access) and the prospective impact of replacing long lead-time equipment (e.g., large power transformers) damaged during an attack.
- **Cyber Security Risks:** Exploitation of cyber security risks could arise from a variety of external and/or internal sources. Additionally, the operational and technological environment of the electrical grid is evolving significantly and rapidly, potentially increasing the potential cyberattack-surface. Sources of potential exploitation include increasingly sophisticated attacks by nation states, terrorist, and criminal organizations. Vulnerability to such exploits are exacerbated by insider threats, poor cyber hygiene, supply-chain considerations, and dramatic transformation of the grid's operational and technological environment. These transformative changes include convergence of information and operational technology (IT/OT), increasing reliance on cloud-based technology, and potential workforce knowledge gaps.
  - Potential for increasing cyber attacks across all sectors: The SolarWinds and Colonial pipeline attacks that occurred in 2020 accentuate supply chain vulnerabilities as well as threats from both foreign actors and domestic adversaries.
  - Artificial Intelligence and Machine Learning can also be used as tools that cyber criminals employ.
  - The potential trend toward virtualization and the housing of critical systems in the cloud could expose the electric industry to additional risks for which industry must both account and plan.
  - Supply chains are a targeted opportunity for nation states, terrorists and criminals to penetrate organizations without regard to whether the purchase is for IT, OT, software, firmware, hardware, equipment, components, or services.
- **Electromagnetic Pulse Risk:** An EMP is a short-duration, high-energy burst that may be disruptive or damaging to electronic equipment. For security purposes, EMP refers to man-made sources. A high-altitude EMP (HEMP) is an electromagnetic pulse stimulated by a nuclear blast in the atmosphere and such action would likely be initiated by a nation-state and thus have clear national security implications. HEMP concerns include the large geographic footprint susceptible to the pulse, range of electric grid equipment at risk (generation, transmission, distribution, and load), and lack of definitive forewarning. Smaller, handheld devices are relatively limited in potential impact and can be considered analogous to the physical attack vector.

Recommendations for Mitigating the Risk

- NERC should facilitate the development of planning approaches, models, and simulation approaches that reduce the number of critical facilities and mitigate the impact relative to the exposure to attack.

- NERC, in collaboration with industry, should evaluate the need for additional assessments of the risks from attack scenarios (e.g., vulnerabilities related to drone activity, attacks on midstream or interstate natural gas pipelines or other critical infrastructure).
- NERC has been conducting an annual industry exercise, GridEx, which helps industry both prepare and react to potential BPS security threats. GridEx, a distributed play grid exercise that enables participants to engage remotely, simulates a cyber and physical attack on the North American electricity grid and other critical infrastructure. Led by NERC's E-ISAC, GridEx gives participants a forum to demonstrate how they would respond to and recover from coordinated cyber and physical security threats and incidents. Other activities that NERC and the E-ISAC have undertaken include enhancements to the Cybersecurity Risk Information Sharing Program (CRISP) as well as outreach transcending borders and industries. NERC should expand the scope of GridEx to include and collaborate with cross-sector industries such as natural gas, telecom, and water.
- The Electricity Information Sharing and Analysis Center (E-ISAC) should encourage continued industry efforts on workforce cyber education to raise awareness of methods and tactics used by cyber attackers (e.g., email phishing, credential theft).
- E-ISAC should execute a long-term strategy to improve cyber and physical security information-sharing, protection, risk analysis, and increase engagement within the electric sector as well as with other ISACs.
- NATF and NAGF should develop supply chain cyber and apply security superior practices. NATF has developed and publicly issued supply chain cyber security framework and detailed criteria that envelops applicable NERC standards and maps to existing security frameworks used by many vendors. NATF is leading an Industry Organizations Team (IOT) comprised of electric utilities, vendors, and solution providers to help promote convergence on the use to the criteria and framework.
- Supply chain risk management and the threats from components and sub-components developed by potential foreign adversaries should continue to be addressed by NERC and industry with evaluation of CIP-013 standard for any needed improvements.
- Many additional efforts to develop cyber security tools are underway with NATF and Trade Associations. For example in 2020, American Public Power Association (APPA) entered into a new three-year cooperative agreement with the Department of Energy to develop and deploy operational technology (OT) cybersecurity technology to public power utilities. These type of efforts should continue.
- NATF, NAGF, Trades Associations, and E-ISAC should develop tiered security performance metrics. Such metrics would track and evaluate events and use predictive analysis to identify and address prospective vulnerabilities on a risk-prioritized basis. Security metrics are included in NATF 2021 work plan.
- NERC’s EMP taskforce should highlight key risk areas that arise from the EPRI’s EMP analysis for timely industry action.

Risk Profile #4: Critical Infrastructure Interdependencies

Statement of the Risk

Significant and evolving critical infrastructure sector (e.g., communications, water/wastewater, financial) and subsector (e.g., oil, natural gas) interdependencies are not fully or accurately characterized, resulting in incomplete information about prospective BPS response to disruptions originating from or impacting other sectors or subsectors and resultant reliability and security implications. Further, as there is increasing interdependencies between these critical infrastructures, impacts on one can have a rippling effect on another.

The following graphic, based on the Emerging Risks Survey results, as well as input from the RISC, demonstrates the potential effects that the mitigating activities from the 2019 RISC Report can have on both the likelihood and impact of baseline risks and can be used as a potential tool for industry to compare mitigating activities, their potential effects, and best use of resources. In addition, these results assisted in the development of the recommended mitigating activities provided below.

Descriptors of the Risk

- Recent BPS events have highlighted that sector interdependence is becoming more critical particularly during emergency events. Digital communications for electric system protection and control, and voice communications, particularly cellular, for emergency response and restoration are critical. Remote work arrangements by critical electric sector employees further underscores the need for seamless and uninterrupted communications during emergency events.
- Subsector interdependence continues to increase and has reached an inflection point with the natural gas subsector. Growing reliance on natural gas as an electrical generation fuel source creates the potential for common-mode failures that could have widespread reliability impacts. The dependence of BPS reliability on natural gas-fired generation does not align with service priorities within the natural gas delivery system and weatherization requirements for gas gathering and delivery systems. Furthermore, the natural gas delivery system depends on reliable electric service to deliver natural gas at acceptable pressures, and the foreseeable growth and dependence of BPS reliability on natural gas-fired generation does not align with the expected pace of pipeline development.
- The financial sector could also be impacted by major outages resulting in failure to approve everyday transactions and provide the necessary financial capital needed to ensure restoration.
- Cross-sector and subsector implications and coordination are not routinely socialized or thoroughly tested during drills or fully understood by both industry participants and regulators
- State and federal governmental oversight and regulatory constructs differ widely among the sectors and subsectors, impeding information sharing and alignment on the criticality of service.
- Grid Transformation also plays a significant role in evaluating critical infrastructure interdependencies. A grid that relies more on renewables and natural gas with less coal and nuclear may face different challenges. Furthermore, the reaction to extreme events that may have been managed in a particular way given the old resource paradigm must now be managed under an entirely different set of circumstances.
- Electric subsector is dependent on other infrastructures such as water, sewer, transportation roads, and communications. If they become unavailable due to widespread power outages could impact the reliable operation of the BPS. Furthermore, electrified transportation will be challenged to bring materials, supplies and equipment supplies to areas with widespread outages (e.g. after a hurricane) which could hamper restoration efforts.

Recommendations for Mitigating the Risk

- NERC, in collaboration with industry and industry partners, should identify and prioritize limiting conditions and/or contingencies that arise from other sectors that affect the BPS.
- NERC and industry partners should host strategic interactions among critical infrastructure partners (e.g., industry and regulators) to identify and align on mutual priorities.
- NERC and industry partners should increase emphasis on cross-sector coordination in industry drills (e.g., NERC Grid-Ex, DOE drills, utility exercises (e.g., Southern California Edison (SCE) Resilient Grid Exercise)).
- NERC should conduct special assessments that address natural gas availability and pipeline common mode failures.
- Electric and natural gas sub-sectors should create and enforce weatherization standards.
- EPRI and the DOE should continue their work on communication alternatives but also the use of same or similar technologies for critical SCADA data. New technologies should be explored that could assist in providing unique and hardened back-up telecommunication methods for the most critical data.

- NERC and industry partners should conduct various meetings and conferences to highlight the importance of cross-sector interdependence and coordination, such as the NERC Reliability Summit, NATF/EPRI resiliency summits, and FERC/DOE technical conferences.
- NERC should communicate to every state and federal regulator of natural gas of the critical interdependence of this fuel source with the other infrastructure sectors.
- NERC should communicate to every state the need for their intrastate gas infrastructure to explicitly classify power generation Firm Transportation services as critical and ensure its curtailment prioritization is ahead of non-essential Firm Commercial and Industrial gas loads.
- NERC and industry partners should evaluate voice communication interdependencies and strategies for ensuring continuous communications during an emergency event particularly as remote working arrangements grow.
- NERC and industry partners should evaluate processes and assumptions around identification of critical loads in load shed and load restoration plans.
- NERC and registered entities should develop and study extreme event scenarios under a future resource mix to ensure that both generation and transmission systems can ensure energy delivery is adequate to meet peak conditions in extreme event scenarios, also taking into account the interdependencies between power and other industries that may pose challenges.
- NERC and industry should consider the unavailability of other infrastructures such as water, sewer, roads, and communications in their emergency plans.
- NERC and industry should develop seasonal extreme temperature energy management plans along with rolling 21-day operational planning plans that accommodate the ongoing weather forecasts and projections.