2024 Western Interconnection Reliability Risk Report (Draft)

March XX, 2024

[Please review within your organization and send comments to risk@wecc.org by March 15th, 2024.
Note: Document is restricted for editing but allows for comments.]

Executive Summary

The inaugural Western Interconnection Reliability Risk Report has identified 31 risks across nine general risk categories using the ISO 31000 Risk Management Framework. Through collaboration with the Reliability Risk Committee (RRC) and the Reliability Assessment Committee (RAC), WECC staff has assessed the following as the top four risk categories of the Western Interconnection:

1. Extreme Natural Events (ENE)
2. Inverter-based Resources (IBR), as part of Grid Transformation
3. Resource Adequacy (RES), as part of Grid Transformation
4. Cybersecurity (CYB)

Within these risk categories, the top 10 identified individual risks are:

1. ENE: Large and Prolonged Heat Waves
2. IBR: Performance and Validation Issues
3. IBR: Applicability of GO/GOP Registration and NERC Reliability Standards
4. ENE: Cold Weather Preparedness
5. ENE: Wildfire
6. ENE: Drought (Aridification)
7. RES: Energy Policy
8. IBR: Inadequate Interconnection Requirements and Commissioning
9. IBR: Modeling Quality Issues
10. CYB: Artificial Intelligence

WECC, the RRC, RAC, and individual registered entities throughout the Western Interconnection must collectively assess further treatment options for the identified top risks. Due to the variation of risks, from natural to human-made, all stakeholders reading this report should determine the top risks applicable to their situation and evaluate the best mitigation efforts to address their needs. It is not expected that entities adequately remediate these risks in the near term (less than five years)—they may require effort that spans decades to plan, prepare, and execute.

Table of Contents

Introduction

This report is an analysis of the WECC Risk Register developed based on the RRC Risk Management Process. The terminology throughout this report is consistent with the ISO 31000 Risk Management Framework.

This report summarizes the 2024 risks the RRC and RAC developed and risk-ranked by WECC's Risk Analysis department. Because the Risk Register is an effort of continuous risk monitoring of the Western Interconnection, any actions taken should be after consultation with subject matter experts on the current risk state.

Identified risks are in summary form. A more thorough analysis of each risk is either contained in external documents or will be necessary in the future to inform the risk identification process more accurately. Additional risks can be identified and submitted for consideration using the Risk Register Initiation Form.

Purpose

The Western Interconnection Risk Report is an overview of the risk facing the Western Interconnection for the 2024 calendar year, identified through continuous monitoring efforts, and serves the following purposes:

1. To set priorities for 2024 and beyond by WECC, RRC, RAC, and stakeholders/members.
2. A concise report of risks without the variability of the ongoing Western Interconnection Risk Register.
3. A historical record of risks for future tracking of progress.
4. A report that can be easily shared with stakeholders across the Western Interconnection or others as needed.

Ranked Risk Categories

The risk category rankings are based on having the highest-ranked individual risks. The ranking methodology is explained in the RRC Risk Management Process; however, a summary of the Reliability Risk Matrix is included in the Appendix. Category definitions are also contained in the Appendix.

Extreme Natural Events (ENE)

The top risk category for the Western Interconnection ranges from prolonged summer heat waves to winter cold weather. The Earth's climate is changing and trending toward higher global ambient air temperatures and increasing severe weather events. In addition, basic physical forces in Earth and space will continue to create extreme risks. These two categories of natural events, changing climates

and physical forces in Earth and space, are useful umbrellas to enumerate specific risks to the reliable operation of the Western electric system.

Grid Transformation:

The following three risk categories are separate but ultimately part of the carbon-to-non-carbon grid transformation driving risk to the Grid. As such, they are grouped in this report under one theme. Combined, grid transformation could arguably be the highest risk to the Western Interconnection.

Changing Resource Mix (CRM)

Due to regulatory and consumer pressure to address the impacts of the changing climate, the Western Interconnection has been transforming its generation fleet. This transformation is focused on the retirement or repowering of coal-fueled power plants and the construction and operation of wind and photovoltaic-generating resources and energy-storage systems. There are also emerging pressures on the effects of existing hydro systems on other environmental issues. New technologies do not duplicate the essential reliability services provided by conventional resources, and the dependence on energy storage systems to deal with the variability of the carbon-free forms of energy are providing unique challenges never addressed by our industry. The Changing Resource Mix is a singularly identified risk but has a high potential impact on reliability.

Inverter-based Resources (IBR)

Generating and energy storage systems that use inverters in their operation are creating exceptional hurdles regarding reliable operation in the Western Interconnection. Facilities like these have operating concerns that differ from conventional synchronous generation facilities, including fault tolerance, voltage and frequency control, and fault duty. Equipment in these facilities is much more flexible with their programmability, which has benefits and risks associated with this flexibility. Additionally, these types of facilities are more difficult to model, and more advanced techniques of system studies are necessary to ensure reliability is maintained at acceptable levels. The inverter-based resource category identified medium-impact risks focused on an emerging category expected to affect the Grid for the long term.

Resource Adequacy (RES)

As our industry transitions to more variable and intermittent generating resources, more robust and complex planning methodologies are needed to identify shortfalls in meeting customer demand in hours and seasons that traditionally were unnecessary. The challenges associated with planning and forecasting variability in energy sources, fuel supplies, demand response, capacity critical hours, and competing regulatory policies, among others, are in this risk

category. Issues associated with Resource Adequacy constitute a medium-impact risk that is expected to become more necessary as our grid transformation continues.

Cybersecurity (CYB)

This risk category has more risks than any other, with 14 identified and one being researched. Seven risks are considered high, five medium, and two low. Emerging risks, such as artificial intelligence and cloud computing, continue to be transformative trends in technology, making this risk category an ongoing concern.

Risks are focused primarily on the risk to the operations network controlling the Grid. However, corporate network cybersecurity can still pose a threat either to grid operations or to the stability of the entities affected. An example is an attack on an entity's financial system, which could affect its ability to pay employees and suppliers or collect revenue and thus undermine confidence in the utility and its ability to operate.

Personnel (PER)

The potential challenges and vulnerabilities related to personnel include retiring workforce, inadequate training, and pandemic impacts. Workforces are expected to continue evolving post-COVID and through generational differences; automation and artificial intelligence are also shaping the personnel landscape.

Physical Security (PHY)

Entities need to safeguard the tangible infrastructure and assets associated with generating, transmitting, and distributing electricity. The ERO Enterprise has long recognized the risks of securing the physical perimeter and reducing unauthorized intrusion. This includes resilient designs, effective monitoring measures, and effective response plans. We continue to see regular events related to the physical breach of critical assets, often resulting in low monetary loss without any significant impact on the Grid. This could change in the event of a coordinated attack.

Infrastructure (INF)

Due to physical limitations, settings, configuration, or supply availability changes, infrastructure changes create a potential for instability and uncontrolled cascading outages. Changes are typically slow over time, and planning and communication are often the best reducers of risk.

Extreme Risks

These are the highest identified individual risks to the Western Interconnection. Extreme risks are very likely to occur and have a severe impact.

1. **ENE: Large and prolonged heat waves:** Prolonged heat wave events cause stress on the interconnection as BAs ensure enough generation to meet the demand and transmission available to transfer it. The impact can also be more significant depending on the magnitude and regional scope of the heat wave. As experienced during the 2020 and 2022 heat waves, prolonged high temperatures impact transmission availability and most classes of generation. As the ambient temperature rises, facility derates will occur, causing a lack of transmission and generation availability.

Ranking Score: 24

2. **IBR: Performance and Validation Issues:** Validation and studying the actual performance of IBRs is not being consistently performed by applicable entities to avoid large-scale outages and to address systemic performance issues.

   Multiple large-scale disturbances on the bulk power system have resulted from the abnormal performance of IBRs across several generating facilities. These disturbances have resulted from systemic performance issues that have caused unexpected losses of inverter-based generation, with the potential to cause widespread or cascading outages.

   Few inverter-based Generator Owners are conducting performance validation activities to capture how the generating facility responds to grid disturbances with adequate and expected performance. Many of these inverter-based generating facilities lack the monitoring and data collection capability to perform post-fault-event analysis.

Ranking Score: 24

IBR: Applicability of Generator Owner/Generator Operator Registration and NERC Reliability Standards: Inverter-based generation technologies currently connected, and other future technologies may not be covered explicitly by Reliability Standards as recognized by FERC Order 901. The reliability risks of those generation facilities will remain until more

structure that clarifies responsibilities is provided. As generating facilities using IBRs may not be required to follow some or all of NERC's mandatory standards, the impacts currently experienced by these devices will continue to increase as the amount of facility penetration as the Grid grows.

An increasing number of generating facilities using IBRs are below the threshold for applicability of NERC criteria to register as a Generator Owner/Generator Operator and are not required to follow the NERC Reliability Standards.

Ranking Score: 23

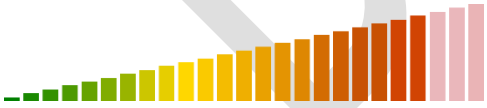
High Risks

High risks are probable to occur and have a major impact.

1. **ENE: Cold Weather Preparedness:** Applicable Western Interconnection entities may not have adequate plans for winter preparedness. Generation assets are affected by cold weather and may trip offline, experience significant derates, or be unable to start if they are not prepared for cold ambient temperatures. Transmission assets can also be affected due to icing on facilities that will eventually cause them to be derated or forced out of service (e.g., arcing, line sagging, icing of manual and motor-operated switches). High voltage substation equipment is also susceptible to issues arising from cold ambient temperatures (e.g., PCB tank heater failures, low SF6 pressure, low operating air pressure, etc.).

Ranking Score: 22

2. **ENE: Wildfire:** Wildfires continue to be a risk in the West, creating potential service disruptions and loss of load. Wildfires can impact the electric Grid, causing service disruptions to transmission and generation assets by affecting the equipment directly (e.g., fire burning equipment) and indirectly (e.g., atmospheric ionization resulting in transmission line phase-to-phase or phase-to-ground faults, and contamination of insulators by smoke or fire retardant): Depending on different factors of the fire, like the magnitude or location, the disruptions can be prolonged (e.g., remote areas): In addition, extreme wildfires can create their own climates which can cause unsafe mitigation conditions slowing restoration, or exacerbating its impact and damage caused. Transmission facilities may be forced out of service to facilitate nearby firefighting activities.



Ranking Score: 22

3. **ENE: Drought (Aridification):** Severe and extended drought conditions. Aridification can cause a region to become drier through decreased precipitation and/or rising temperatures due to climate change. This results in hotter climate extremes, drier soil conditions, more severe drought, and the impacts of hydrologic stress on rivers, forests, agriculture, and other systems. Reduction in the availability of some hydro resources in the West and limiting the cooling capacity of thermal generation.

Ranking Score: 22

RES: Energy Policy: Energy Policy can drive changes in the planning and operation of the BPS. Implementing policy decisions can significantly affect the reliability and resilience of the BPS. Decarbonization, decentralization, and electrification have been active policy areas. Implementation of policies in these areas is accelerating, and reliability implications are emerging with changes in the resource mix, extreme weather events, and physical and cyber security challenges.

Ranking Score: 22

3. **IBR: Inadequate interconnection requirements and commissioning:** Active interconnection and commissioning requirements set and enforced by applicable entities may not be adequate to provide clarity and consistency for IBRs.

   A critical component of the interconnection process is the commissioning and operation period immediately before commercial operation. These activities ensure the facility has been modeled, studied, designed, constructed, and configured to match the expectations and requirements of the local interconnecting utility (and per the interconnection procedures). Industry stakeholders from both generation and transmission have concerns about the commission testing procedures, seeking clarity and consistency on what these processes entail.

   Applicable entities may not be implementing the recommendations outlined by NERC and continue to rely mostly on the pro forma Generator Interconnect Agreements (GIAs) with some modifications for specific topics, which are not comprehensive. Mandatory NERC reliability standards have minimal requirements that do not necessarily support the need for explicit, complete, and accurate data to support mitigation of this risk.

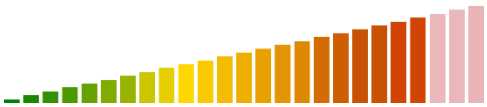
Ranking Score: 22

4. **IBR: Modeling quality issues:** Model simulations do not adequately represent how IBRs will respond during transient events, faults, and other disturbances.

   This risk can lead to unforeseen actions in real-time operations, such as loss of generating resources or load shedding. This same risk exists for hybrid resources (e.g., battery and solar),

though the modeling can be more nuanced. In addition, due to this inadequacy, the effectiveness of the WECC Off Nominal Frequency Load Shedding Plan[1] could not be verified in the 2022 Underfrequency Load Shedding Program Assessment [2] due to factors related to voltage support that are potentially caused by inaccuracies with the current inverter-based models in transmission planning data sets.

Third-party developers and applicable entities that use inverter-based technology are not correcting and updating their models as needed. This is due to multiple factors, such as proprietary limitations and/or lack of NERC reliability standards and requirements.

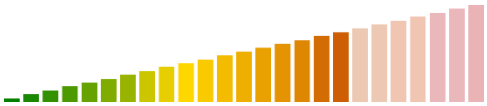


Ranking Score: 22

5. **CYB: Artificial Intelligence:** Publicly available information about entities, including company organization/employees, products/services used, physical layout, and operating models, can be easily collated by AI. This creates a current condition where reconnaissance of an entity is made trivial for a threat actor. Weaponization and delivery of exploits are getting easier to generate due to AI. The public development of AI is a rapidly growing online sector and is out of the entity's control.

Ranking Score: 21

6. **PER: Future Pandemics:** "In the future, it is predicted that pandemics will emerge more often, spread more rapidly, cause more damage to the global economy, and lead to greater global morbidity and mortality." - World Health Organization. The industry should capture lessons learned and best practices developed during the COVID-19 pandemic to ensure plans are developed and maintained to mitigate future risks. Load forecasting practice could be enhanced if/when future pandemics occur.



Ranking Score: 18

[1] https://www.wecc.org/Reliability/Off-Nominal%20Frequency%20Load%20Shedding%20Plan.pdf

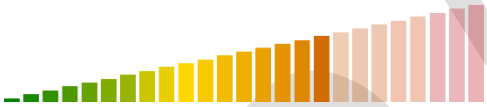
[2] https://www.wecc.org/Administrative/2022%20UFLS%20Assessment%20Report_Nov%202022.pdf

7. **CYB: Perimeter Breach:** Unauthorized actions on the digital assets within an organizational network. Upon infiltration, malicious parties may use other attack vectors, such as malware and endpoint attacks, to attack the entity network.

Ranking Score: 18

8. **CYB: Malware:** Infection from any source of an entity's system through malicious program or code. Hostile, intrusive, and intentionally nefarious malware seeks to compromise, misuse, invade, damage, or disable computers, computer systems, networks, tablets, and mobile devices, often by taking partial control over a device's operations.

   Malware affecting the corporate network, which may not have the same level of controls required for the operations network, can undermine the stability of the entity. Given the interconnectivity of the commonly implemented Purdue Model, entities should extend their anti-malware technologies beyond their operation network zones to their corporate network zone to reduce the risk of infection.

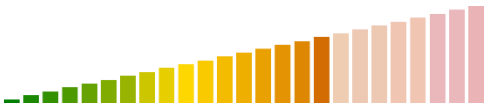


Ranking Score: 17

9. **CYB: Compromised Supply Chain:** Compromised vendors can be a vector of cyber-attacks on critical infrastructure. This can include the loss of confidential information stored by the vendor, the delivery of malware or compromised systems, or a compromised vendor connected to a customer's critical systems being used as a conduit for unauthorized disclosure.

Ranking Score: 17

10. **CYB: Zero-Day Exploit:** A vulnerability in a system or device that has been disclosed but not patched. An exploit that attacks a zero-day vulnerability is called a zero-day exploit. Until the vulnerability is mitigated, threat actors can exploit it to adversely affect programs, data, additional computers, or a network.



Ranking Score: 17

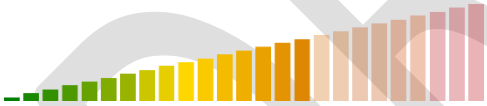
11. **RES: Resource Adequacy Forecast Planning:** Existing approaches to Resource Adequacy may not account for a broader range of possibilities and ensure they reflect the full range of probable outcomes. By not including a broader range of possibilities, resource adequacy studies can lead to a misperception of the future. This misperception can include inadequate capacity requirements during peak times, leading to energy emergency alerts and firm load shedding.

    Increasing variability in weather, demand, generation, and import constraints requires changing existing approaches. According to the WECC 2022 Western Assessment of Resource Adequacy report, the Planning Reserve Margin Indicator (PRMI) for the West increased from 16.9% in 2021 to 18.3% in 2023 due to increasing demand and Variable Energy Resources (VERs) on the interconnection over the next ten years and may require entities to plan for more reserves or take other actions to account for this increase.

    Ranking Score: 17

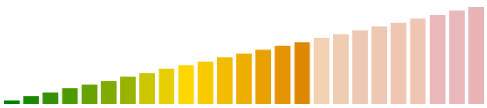
12. **CYB: Insider Threat:** An insider is any person who has authorized access to or knowledge of an organization's resources, including personnel, facilities, information, equipment, networks, and systems. A trusted insider uses their authorized access to wittingly or unwittingly compromise assets. It would likely require collusion across insiders at multiple entities to impact the Grid significantly. However, an authorized user with elevated privilege could have a significant and lasting impact on a single entity.

    Ranking Score: 16

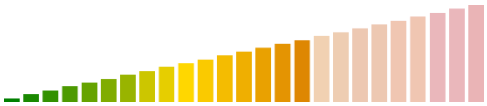
13. **CYB: Perimeterless Operational Technology:** Systems and software used to peripherally interact or transmit into cyber assets that are not within an enterprise-owned network boundary. Untrusted assets may lead to unintended misoperation of cyber assets.

    Integrating Bring-Your-Own-Device, Internet of Things, or other external operational technology assets as an extension of the electric Grid is a growing trend and potentially necessary for future operation.

    Ranking Score: 16

14. **CYB: Public Cloud / Cloud Computing:** Cloud computing is a model for enabling universal, convenient, and on-demand network access to a shared pool of configurable computing resources, such as networks, servers, storage (data), applications, and services that can be quickly provisioned and discarded with minimal internal management effort or interaction with the cloud services provider. Using such services to maintain or control Western Interconnection BPS resources can introduce a new threat vector for threat actors to exploit outside the ownership of Registered Entities.

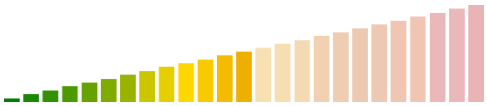


Ranking Score: 16

Medium Risks

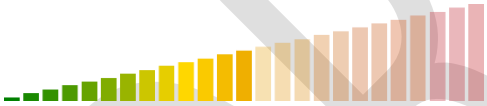
Medium risks are unlikely to occur and would have a moderate impact.

1. **CRM: Generation Resource Mix Impacts to Future Transmission Congestion (reduce):** Additional long-term regional transmission planning studies should be done to produce multiple reasonably likely scenarios and allow time to mitigate any risks. As resources continue to change, studies done by WECC in 2022 and 2023 show current transmission paths in the future with higher utilization and, in some cases, exceeding their facility rating or Total Transmission Capacity. Building new transmission facilities takes years to decades to complete due to several factors (e.g., regulatory approval, right-of-way permitting, supply chain)



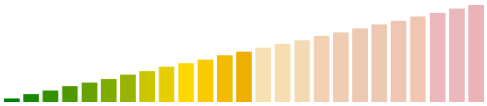
Ranking Score: 13

2. **CYB: Phishing and Social Engineering:** Threat actor exploits trusted insider access to harm or facilitate unauthorized cyber asset operations. A single socially engineered insider with the proper access could cause significant harm; however, it would likely require exploitation across several insiders to impact more than one entity in the Western Interconnection.



Ranking Score: 13

3. **CYB: Internet of Things (IoT):** Consumer Internet of Things (IoT) devices connected to the Grid's distribution network create an environment for threat actors to compromise many high-wattage IoT devices (such as air conditioners, heaters, charging stations, Distributed Energy Resource (DER), etc.) and turn them into a botnet (a compromised string of connected computers where a cyber-criminal gains control without the owner being aware). The malicious actors could then use the botnet to launch a coordinated attack to manipulate the demand across distribution grids.

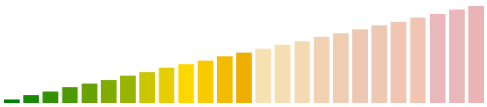


Ranking Score: 13

4. **INF: Supply Chain Constraints:** The industry is experiencing supply chain constraints, making purchasing equipment more difficult within historically expected timeframes. This constraint

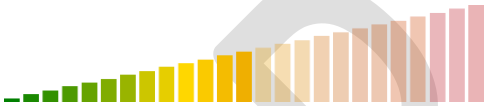
causes delays in receiving new equipment. It causes entities to prioritize between installing new projects or delaying maintenance and replacing failed equipment, ultimately affecting the reliability of the BPS.

Several factors, such as the effects of the COVID-19 pandemic, raw material and labor shortages, competition for resources for other applications (EV, rooftop solar, etc.), and global events have impacted the supply and costs of new equipment. In addition, policies set by regulators (e.g., clean energy policies) make new projects designed to meet these regulations compete with maintenance and replacing failed equipment.



Ranking Score: 13

PER: Workforce Skillset Shortage: Entities in the West have a workforce close to retirement and are finding it difficult to hire technical skill sets (entry-level and expert) to replace open positions. This is symptomatic across the industry and can affect an organization's ability to design, construct, operate, and maintain the physical and cyber assets needed for reliability and to prevent, detect, and respond to physical security and cybersecurity events. Data is not readily available to adequately determine the magnitude or scope of this risk.

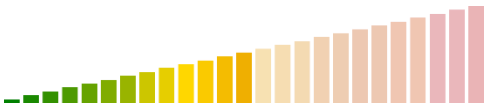


Ranking Score: 13

5. **PHY: Drones and Unmanned Aircraft:** The use and number of drones have increased exponentially in North America, and these devices can easily bypass traditional security perimeters for 1. Surveillance and negative publicity 2. Injury to personnel 3. Attacks on infrastructure, or 4. Cybersecurity vulnerabilities.

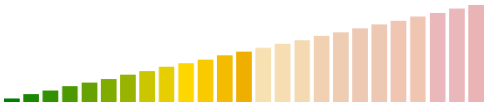
Ranking Score: 13

6. **CYB: Third-Party Operations:** Unvetted and unmonitored third-party operations of cyber assets. Unverified security controls of third parties can lead to unintended operation of cyber assets. Third-party operation of cyber assets may be necessary as a cost-benefit and may have improved security controls over what a Registered Entity could afford to implement.



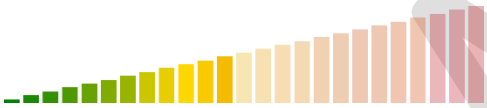
Ranking Score: 13

7. **CYB: Physical Attacks on Cyber Assets:** Insufficient physical controls to protect against unauthorized physical access to cyber assets. Threat actors can exploit hardware and software to which they can gain physical access.



Ranking Score: 13

8. **PHY: Substation Sabotage:** Substations, primarily unattended, are increasingly targeted for physical attack and damaging facilities. Although a primarily financial loss, there is potential for increasing attack severity to adversely affect the operation of a substation beyond acceptable entity thresholds.



Ranking Score: 12

9. **IBR: System Restoration:** With the continued retirement of thermal plants and increased IBR, system restoration will depend more on IBR. Battery energy storage systems (BESS) have significant unique capabilities. Grid-following versus grid-forming technologies should be considered in designing and constructing new IBR facilities. Grid-forming battery energy storage systems can provide resources during Black Start restoration[3].

   Current guidelines and standards do not or may not fully address the integration of IBRs into restoration plans (as blackstart resources or as destination plants).

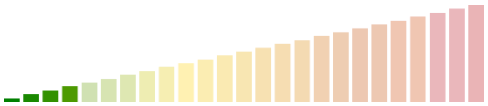
Ranking Score: 12

[3] https://www.energy-storage.news/california-batterys-black-start-capability-hailed-as-major-accomplishment-in-the-energy-industry/#:~:text=A%20utility%20in%20Southern%20California,turbine%20from%20an%20idle%20state.

Low Risks

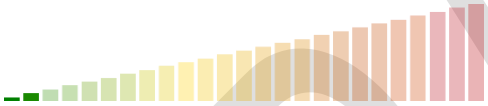
Low risks are improbable to occur and have a minor impact.

1. **CYB: Unauthorized Software & Hardware:** Unauthorized software and hardware within an organizational network. This includes authorized software and hardware that is end-of-life or unmaintained to the point of vulnerability. Threat actors can exploit hardware and software vulnerabilities unknown to entity personnel, leading to attacks on the entity network.



Ranking Score: 4

2. **CYB: Cybersecurity in Transmission Planning:** Traditional transmission planning processes do not include cyber-informed transmission planning approaches to incorporate cybersecurity risks. Excluding these approaches in transmission planning activities can prevent the industry from more effectively mitigating the reliability impacts of cyberattacks.



Ranking Score: 2

Conclusion

Each organization should assess the risks identified in this report to determine where to apply further treatment options to reduce them. Where risk reduction may be a collective effort, work groups and committees should review these risks to determine where collective mitigation efforts are most effective.

Further analysis will be required for some risks to understand where the likelihood can be reduced (for controllable risks), where the impact can be reduced (for uncontrollable risks), or both.

Appendix

Risk Category Definitions

Category Title	Definition
Cybersecurity	An effect of uncertainty on or within information and technology used to control the BPS. Cybersecurity risks relate to the loss of confidentiality, integrity, or availability of BPS information, networks, or control systems and reflect the potential adverse impacts to operations and assets, individuals, other registered entities, and the Western Interconnection.
Changing Resource Mix	The rate of change (penetration rates of certain resources) and the type of change (the specific resources) are influenced by state, provincial, and federal initiatives, which sometimes impact one region, province, or state more than another.
Extreme Natural Events	A time and place in which weather, climate, or environmental conditions—such as temperature, precipitation, drought, or flooding—rank above a threshold value near the upper or lower ends of the range of historical measurements.
Frequency Performance	The instantaneous balance between generation and load is directly reflected in an interconnected electric power system's frequency. Reliable power system operation depends on controlling frequency within predetermined boundaries above and below a nominal value. In North America, this value is 60 cycles per second (or 60 Hertz (Hz)).
Grid Transformation	Transformation of the Grid continues to accelerate toward generation and load resources that are increasingly non-synchronous, diverse, digital, and dynamic— while dependence on uninterrupted electric energy increases.
Inverter-based Resources (IBR)	A source—or sink in the case of a charging battery energy storage system (BESS)—of electric power that is connected to the electric power system (transmission, sub-transmission, or distribution system), and that consists of one or more IBR Unit(s) operated as a single resource at a common point of interconnection. IBRs include solar photovoltaic (PV), Type 3 and Type 4 wind, BESS, and fuel cells. Technological advances in IBRs are majorly affecting existing generation, transmission, and distribution systems.

Infrastructure	The potential for loss due to failure of basic services, organizational structures, and facilities.
Personnel	Losses arising from the death, injury, disability, or departure of employees. Also includes the possibility of mistakes or errors made by individuals in their roles, which can lead to operational disruptions.
Physical Security	The potential threats and vulnerabilities associated with protecting tangible assets, such as control centers, substations, data centers, equipment, and personnel.
Resource Adequacy	An assessment of whether the current or projected resource mix is sufficient to meet an entity's capacity and energy needs and to ensure the resilient operation of the Grid occurs in real-time.
Other	Any risk not applicable to the above categories. New risk categories that were originally assigned as "other" may be developed.

Reliability Risk Matrix

Risks are ranked based on a 25-point likelihood/consequence scale.

Reliability Risk Matrix											
Consequence/Impact (C)		Likelihood (L)									
		L1		L2		L3		L4		L5	
		Very Unlikely		Unlikely		Possible		Likely		Almost Certain	
C5	Severe	Medium	10	High	15	High	19	Extreme	24	Extreme	25
C4	Major	Medium	8	Medium	9	High	18	High	22	Extreme	23
C3	Moderate	Low	5	Medium	7	High	16	High	17	High	21
C2	Minor	Low	3	Low	4	Medium	12	Medium	13	High	20
C1	Negligible	Low	1	Low	2	Low	6	Medium	11	Medium	14

Approving Committee, Entity, or Person	Approval Date

WECC receives data used in its analyses from a wide variety of sources. WECC strives to source its data from reliable entities and undertakes reasonable efforts to validate the accuracy of the data used. WECC believes the data contained herein and used in its analyses is accurate and reliable. However, WECC disclaims any and all representations, guarantees, warranties, and liability for the information contained herein and any use thereof. Persons who use and rely on the information contained herein do so at their own risk.