WECC

WECC Risk Management Process

Risk Analysis & Data Services

June XX, 2025

Table of Contents

Introduction

The reliability of the Bulk Power System (BPS) is critical to today's society. As the largest human-made machine in the world, the BPS has various risks that could affect its reliability and security, which may have adverse consequences on society. A structured risk management process is necessary to effectively and efficiently mitigate and address these unique risks. The WECC Risk Management Process (RMP) provides an industry-standard structured approach to address known and emerging reliability risks of the BPS within the Western Interconnection (WI). In collaboration with industry, this process allows for risks to be identified, prioritized, monitored, and treated to improve the reliability and security of the WI BPS.

The WECC RMP is based on ISO 31000 Risk Management Process principles. Using these principles, an electric utility industry-based process was developed to align with the core activities and associated responsibilities already established at WECC and with the industry. This approach:

- Provides a framework for collaborating on prioritization efforts to address risks and monitor the effectiveness of those actions.
- Avoids duplication of known work and allows WECC to build on the successes of others by working with other organizations and industry experts.
- Develops a data-driven decision-making process with defined parameters, metrics, and factors.
- Provides a feedback process for additional prioritization or treatment efforts and overall process improvements.
- Strives for a consistent, defendable, durable, and repeatable RMP.

Purpose

The WECC RMP provides an industry-standard structured risk approach to address known and emerging reliability and security risks of the WI BPS.

According to WECC's Bylaws, WECC's Mission is "To effectively and efficiently mitigate risks to the reliability and security of the Western Interconnection Bulk Power System while carrying out the responsibilities of the Regional Entity."

The WECC RMP enforces WECC's independent voice of BPS reliability in the WI as part of WECC's Long-Term Strategy.

Document Owner and RMP Updates

The WECC staff, specifically the Risk Analysis team, owns this document. The WECC RMP is a living document; WECC staff will review this process biennially and make any necessary improvements. WECC staff will update this document to reflect those changes and convey them to WECC committees and other stakeholders for awareness. WECC will review the appendices in this document as changes are made to the process.

Industry Representatives

In support of WECC's Risk Analysis team, a Strategic Partner Risk Advisory Group (SPRAG) will represent the industry. This SPRAG will comprise representatives with company authority and technical background to partner with the Risk Analysis team, the WECC Board, and executives to succeed in WECC's Mission.

The considerations for membership in the SPRAG will include:

- Senior leadership or principal decision-maker (C-suite, vice president, director) with demonstrated technical expertise;
- Collaboration with chairs/vice chairs of WECC committees for participation and or recommendation for participation
- Partners that plan, own, and/or operate in the WI BPS;
- Partners from investor-owned utilities, publicly owned utilities, power marketing administrations, and independent power producers;
- Additional limited senior-level partners from regulators, NGOs, etc., will be included with technical expertise to the extent feasible; and
- Broad areas of BPS technical expertise must include, but are not limited to:
    - Infrastructure,
    - Operations,
    - Planning,
    - Resources, and
    - Security (cyber and physical).

Foundation

This foundation sets the scope, context, and criteria under which WECC will operate and apply its RMP.

For this RMP, the definition of reliability is crucial, specifically with respect to the BPS. The NERC Glossary of Terms defines the BPS as:

- Facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and
- Electric energy from generation facilities needed to maintain transmission system reliability.

Note: The term does not include facilities in the local distribution of electric energy.

References:

- NERC BES Definition
- NERC BPS BES FAQ

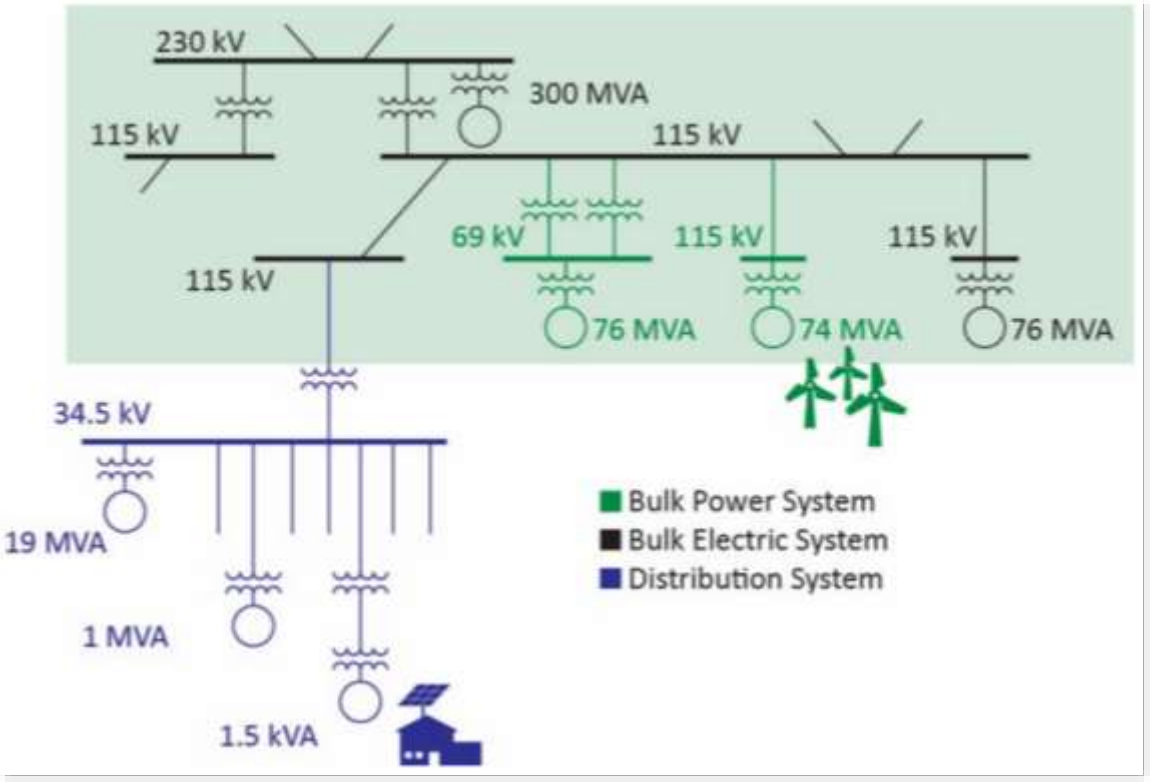


Figure 1: Representation and relationships of BPS, BES, and the distribution system.

There are a number of examples that are not within the reliability of the BPS, which may include state and county jurisdictions, energy commissions, coastal commissions, air resource boards, air-quality management districts, public utility commissions, etc.

Scope

The scope of WECC's risk management program is contained within WECC's Mission Statement, specifically: "To effectively and efficiently mitigate risks to the reliability and security of the Western Interconnection Bulk Power System while carrying out the responsibilities of the Regional Entity."

"Western Interconnection" and "Bulk Power System" are capitalized and defined terms elsewhere, and the RMP will not change or interpret their meaning.

For the purposes of the RMP, the term "risk" is defined as "The effect of uncertainty on the reliability of the Western Interconnection BPS," where "effect" is a deviation from what was expected, and "uncertainty" is lack of information or knowledge concerning a real or potential event, its consequences, or its likelihood.

Context

To achieve WECC's objective of mitigating risks to the reliability of the WI BPS, WECC operates within the context given by and authority given through FERC and NERC, namely:

- NERC Bylaws,

- NERC Delegation Agreement,
- NERC Rules of Procedure, and
- Registered entities.

WECC may educate and influence, but not control, other organizations, commissions, boards, etc., that also have authority and responsibilities regarding aspects of the WI BPS.

Criteria

This defined criterion evaluates the risk's significance and supports decision-making processes.

Reliability Adequacy: For the purposes of WECC's RMP, "reliability and security" are defined through the term "Reliability Adequacy," which is the overarching term for its three parts: Resource Adequacy, Infrastructure Adequacy, and Operational Adequacy. (Hereafter, *Reliability Adequacy* and *reliability* are synonymous.) The term "security" supports the reliability of the BPS and is included in the definition of reliability.

- **Resource Adequacy:** Ensuring sufficient resources to support the WI BPS. (WI (or subregional) resource capability with the infrastructure (BES))
  - *Capacity Factor*: Percentage of total WI generation (in MW) deficit that, if unavailable or unplanned, would affect the WI BPS.
  - *Energy Factor*: Percentage of total Demand-At-Risk Hours (in TWh) that would affect the WI BPS.
- **Infrastructure Adequacy:** Ensuring sufficient infrastructure (transmission facilities, substations, etc.) to transmit energy to the Load-Serving Entity (LSE).
  - *Physical Transmission Factor*: Transmission assets and facilities (rated by kV and MW/MVA) that, if unavailable or unplanned, would affect the WI BPS.
- **Operational Adequacy:** Ensuring the operation of the BPS (people, processes, tools, and best practices) is reliable[1], secure, and compliant for normal and reasonable emergency operations.
  - *Generation Factor*: Instantaneous loss (in MW) that would affect the WI BPS.
  - *Frequency Factor*: Frequency below nominal (60Hz) that would affect the WI BPS.
  - *Transmission Factor*: Transmission assets and facilities (rated by kV and MW/MVA) that, if unavailable, would affect the WI BPS.

[1] *Reliable Operations from NERC Glossary of Terms: https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf

"Operating the elements of the [Bulk-Power System] within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements."

- *Inoperability Factor*: Operational impacts leading to adverse effects on monitoring or controlling significant (by function, kV, and percentage WI load) operational assets that would affect the WI BPS.
- *Resource Factor*: Percentage of online non-dispatchable generation that would affect the WI BPS.

WECC uses a five-point scale for both Consequence/Impact and Likelihood as follows:

Consequence/Impact—How could a Typical Event* due to this risk affect BPS reliability in the Western Interconnection?	
Severe (C5)	Impacts may have widespread effects on the WI.
Major (C4)	Impacts may have widespread effects on multiple subregions[2] within the WI.
Moderate (C3)	Impacts may have widespread effects on a subregion within the WI.
Minor (C2)	Impacts may have effects on an entity within the WI.
Negligible (C1)	Impacts may have small or non-existent effects within the WI.

Likelihood—What is the reasonable probability that consequences will occur?	
Almost Certain (L5)	Mandatory Controls—No NERC Reliability Standards in place for mitigation. Emerging Trends—Increasing trends have been identified. Event History—Documented events or widely publicized exploits have been recorded. Probability—Frequent (or) multiple times per year (or) >90% chance.
Likely (L4)	Mandatory Controls—No NERC Reliability Standards in place for mitigation. Emerging Trends—Some trends have been identified. Event History—Documented events, or generally publicized exploits have been recorded. Probability—Probable (or) 1 to 2 times per year (or) 50%–90% chance.
Possible (L3)	Mandatory Controls—NERC Reliability Standards in place for limited mitigation. Emerging Trends—Some trends have been identified.

[2] See Appendix 1

	Event History—No documented events, or moderately publicized exploits have been recorded. Probability—Occasional (or) Once in 1 to 5 years (or) 15%–50% chance.
Unlikely (L2)	Mandatory Controls—NERC Reliability Standards are in place for mitigation. Emerging Trends—Some trends have been identified. Event History—No documented events, or minimally publicized exploits have been recorded. Probability—Remote (or) Once in >5 years (or) 5%–15% chance.
Very Unlikely (L1)	Mandatory Controls—NERC Reliability Standards in place for mitigation. Emerging Trends—No known trends identified. Event History—No documented events or publicized exploits have been recorded. Probability—Improbable (or) once in >20 years to almost never (or) <5% chance.

*A Typical Event is defined as:

- **Type:**
  - Natural: The most impactful event likely to occur in the next 50 years (1-in-50-year event).
  - Human-made: The most impactful event likely to occur within 10 years.
  - Inherent: The most impactful event likely to occur based on the current or planned BPS design (if the risk is based on a potential future state, i.e., 10- to 20-year planning).
- **Plausibility:**
  - System assets or threats must have a commonality or relationship or be deemed credible.
  - Common mode failure (unrealistic-related events are not plausible).
- **Assumptions:**
  - Good utility practice, NERC Reliability Standards, and the inherent risk-averse design of the BPS are the baseline assumptions of the Reliability Adequacy Framework for the RMP.
  - In addition, contracts, interconnection agreements, state regulations, tariffs, and other associated obligations must be met with the best effort.
  - Exceptions:
    - Risks that identify an extended or different time frame should be defined within the “condition” statement (i.e., the Typical Event will be presumed in the condition of any risk in the WECC Risk Register unless clearly stated otherwise).

Process

The WECC RMP is based on the ISO 31000 Risk Management Process industry standard risk framework shown in Figure 2.

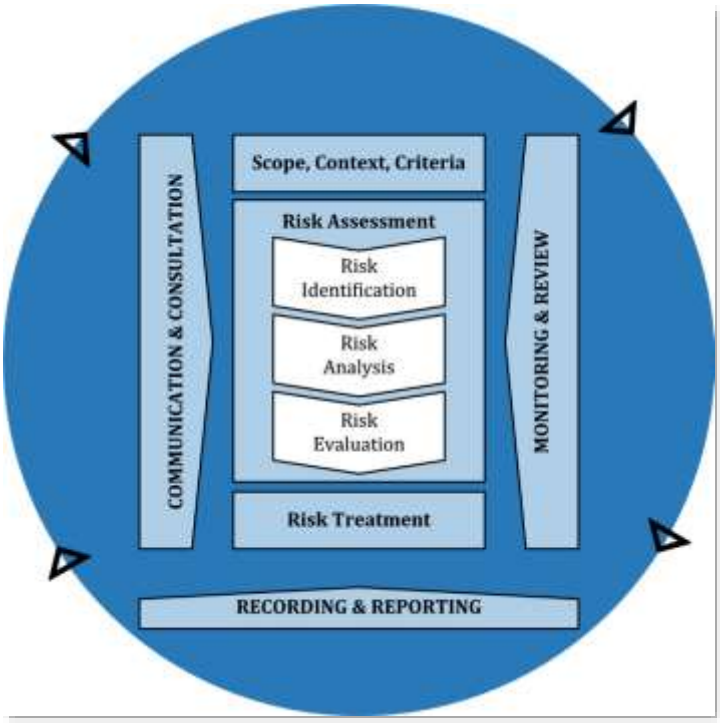


Figure 2: ISO 31000: 2018 risk management process.[3]

This framework diagram contains a set of steps in the center, flanked by processes that occur throughout the ISO 31000 RMP. While the WECC RMP closely aligns with the ISO 31000 framework, it has been customized to meet WECC's needs.

The WECC RMP contains steps, periodic activities, and ongoing activities.

The five steps reflect the middle of the framework diagram:

1. Risk Identification;
2. Risk Analysis;
3. Risk Evaluation;
4. Risk Treatment; and
5. Recording and Reporting.

The ongoing activities reflect the right-hand portion of the framework diagram, "Monitoring and Review," and include ongoing monitoring and review of:

- The risks examined through the RMP; and

[3] https://www.iso.org.

- The effectiveness of the RMP itself.

The periodic activities reflect the left-hand portion of the framework diagram, “Communication and Consultation,” and include communication and consultation to:

1. Develop periodic risk reporting; and
2. Carry out periodic risk prioritization.

The RMP references and uses several other supporting documents found on the WECC Risk webpage. These include:

- WECC Risk Register Initiation Form;
- WECC Risk Register; and
- WECC Risk Process Flowchart

Five Steps of Risk Management

Each reliability and security risk examined through the WECC RMP progresses through the five steps in the diagram below. Each step includes responsibilities for WECC staff and potentially Strategic Risk Partners.

Figure 3: Five risk management steps.

Step 1: Risk Identification

Overview

This step aims to develop a comprehensive and tailored list of existing and potential risks that may adversely affect the reliability and security of the WI BPS. The list is documented with important information identified for each risk, including the potential event or condition, the consequences, and, if known, the cause of the risk. Several approaches can be used during the risk identification step. These can be sophisticated and highly structured or more informal, such as a consensus of industry experts, while following the criteria of the RMP.

It is important that the risk process identifies a wide array of risks to the WI BPS and is not too narrow or constrained. The Risk Identification step can suffer from focusing on only today's challenges and not considering risks that could emerge in the future.

No single group or entity completely understands the WI BPS's known and emerging reliability and security risks; every individual or group understands risks based on their perspective. Therefore, the WECC RMP must consider many data-driven perspectives to capture the complete picture of risks across the WI BPS.

Because the success of the RMP depends on this breadth of perspective, the Risk Identification step relies heavily on partner input. Without active partner participation, the RMP will be limited in how effectively WECC accomplishes its reliability mission as given in its Mission Statement:

> *"To effectively and efficiently mitigate risks to the reliability and security of the Western Interconnection Bulk Power System."*

One way this breadth of perspective is achieved is through WECC's collaboration with other partners working within existing processes to identify risks. Through this partnership, WECC can help prevent duplication of work and use existing processes and programs to identify and analyze the risks to be documented in the WECC Risk Register. This includes working with partners to determine the likelihood and impact of the risk as it applies to the WI. Some of these existing processes and partners that WECC can use to help identify risks are:

- WECC/NERC technical committees, industry forums, and associated subject matter experts;
- Compliance monitoring activities;
- Inherent risk assessments;
- Reliability assessments;
- ERO events analysis;
- Analysis of availability data systems (e.g., ADS, BASS, DADS, GADS, MIDAS);
- Essential Reliability Services, such as frequency response, balancing, voltage control, and other metrics and their associated reports;
- Interconnection simulation base case quality and accuracy metrics;
- NERC's Reliability Issues Steering Committee (RISC) Biennial Risk Report;
- Regional risk assessments;
- Communication with external parties (e.g., DHS, DOE, E-ISAC, WIRAB); and

- Shared public or government intelligence with special emphasis on cybersecurity.

WECC staff may request an existing WECC committee to study or provide expertise to help understand a given risk, or they may also create a task force or partnerships.

Risk Identification Process

General responsibilities for WECC staff include:

- Employ and coordinate expertise from across the organization, examine risks comprehensively, consolidate risks identified across multiple groups, and bring them for review.
- Ensure that data confidentiality is upheld with any risks it submits through the processes.
- Facilitate Risk Identification as outlined herein.
- Ensure that documentation is complete, accurate, and orderly archived.

General responsibilities for partners include:

- Coordinate discussions within their organizations about known and emerging reliability and security risks the organization is experiencing or sees on the horizon.
- Engage in forums, work groups, and initiatives in and outside of WECC to understand known and emerging risks.
- Risks identified in these interactions should be brought to WECC for consideration.

Submission of New or Updated Risks

- Reliability and security risks are submitted for consideration by sending a request to risk@wecc.org. Basic details of the condition, consequences, and cause of the risk should be included in the initial request, as well as the contact details of the subject matter experts.
- Anyone may submit risks to WECC.
- WECC staff will review the request and respond with an acknowledgment of receipt within five business days.
- WECC staff will work with the submitters and their subject matter experts to set up an interview to discuss the details and document for screening and potential inclusion or updating of the Risk Register.
- WECC staff will review each submission against the WECC Risk Register to ensure there is no duplication or overlap with existing entries.
- An internal reliability risk committee will conduct a final review of the screened risk for disposition.

Risk Entry into the WECC Risk Register

- WECC staff will enter each screened risk into the WECC Risk Register.
- Entry into the WECC Risk Register triggers subsequent steps in the WECC Risk Management process for that risk.
- The public WECC Risk Register is on the Risk Management Program webpage and will be updated periodically, as changes are made.

Step 2: Risk Analysis

Overview

Risk Analysis aims to understand and document the causes, nature, complexity, existing controls, and time-related factors associated with the risk and to rate the potential impact of each risk according to its likelihood of occurrence. The combination of impact and likelihood determines the severity of the risk. The WECC RMP uses the following Reliability Risk Matrix:

Reliability Risk Matrix						
Consequence/Impact (C)		Likelihood (L)				
		L1	L2	L3	L4	L5
		Very Unlikely	**Unlikely**	**Possible**	**Likely**	**Almost Certain**
C5	**Severe**	High	Extreme	Extreme	Extreme	Extreme
C4	**Major**	Medium	Medium	High	High	Extreme
C3	**Moderate**	Medium-Low	Medium-Low	Medium	High	High
C2	**Minor**	Low	Medium-Low	Medium-Low	Medium	Medium
C1	**Negligible**	Low	Low	Low	Low	Medium-Low

As there are different data-driven inputs for analyzing the impact and likelihood of the risk, each risk must be assessed consistently based on a constant set of criteria. Where risks are identified in other organizations, good communication is required to ensure each Strategic Risk Partner understands the ownership and severity of the risks.

The Risk Analysis step also includes an analysis of time-related factors, which may include:

- Risk timing—Is the risk prevalent today? Is it expected to occur five years from now or more than 10 years from now?
- Risk velocity—How long does a risk event take to materialize? In other words, the time between the occurrence of an event and the point at which its effects are realized.
- Risk trending—Is the risk increasing or decreasing over time?

Risk Analysis Process

General responsibilities for WECC staff:

- Lead the Risk Analysis step with support and collaboration from Strategic Risk Partners.
- Obtain and incorporate partner feedback as needed throughout the step.

- Facilitate successful Risk Identification.
- Ensure that documentation is complete, accurate, and orderly archived.

General responsibilities for Strategic Risk Partners and points of contact:

- Work with WECC staff to understand the causes, nature, and time-related factors associated with the risk.
- Provide feedback and support in assessing the likelihood and impact of the risk.
- Review the documents resulting from the Risk Analysis step, discuss with subject matter experts within your organization (and others as needed), and provide feedback.

The primary sources of information used to support this analysis should be provided during submission in Step 1: Risk Identification. Depending on the complexity of the risk, additional data and analysis may be required to better understand the potential impacts of the risk. Such changes should be performed as necessary but include potential risk mitigation tactics. If data is unavailable, input from subject matter experts (e.g., Cyber Security Forum, industry survey) may be used to help with risk analysis. If similar risks are shared among the ERO, the Strategic Risk Partners should ensure communication with the appropriate partners (e.g., NERC RISC) to understand the severity of the risk and coordinate efforts to address it.

Ranking the Risk

Ranking the risk involves ordering the set of risks within its category from most significant to least significant based on the outcome of the Risk Analysis step.

Step 3: Risk Evaluation

Overview

The purpose of Risk Evaluation is to support decisions. This step builds on Risk Analysis to determine activities already underway to mitigate the risk, to determine the tolerability of the risk, and to rank the risk relative to other risks. Tolerability is different than the severity identified in Risk Analysis, as it helps determine which risks need treatment and their ranking. This evaluation includes comparing the risk's severity to the acceptable risk level. Decisions on risk prioritization should include a broad range of factors and be vetted by partners or experts within the interconnection for their feedback.

When determining risk tolerability, the evaluation should consider common factors to be tracked in the Risk Register or other documentation. These factors help WECC and Registered Entities make informed decisions about ranking various risks. Some factors to consider when determining risk tolerability are:

- The result and documentation from Risk Analysis;
- How the risk may be combined with other similar risks in the Risk Register;
- Whether mitigation is expected to be a one-time action or ongoing (e.g., required processes or standards)
- Whether there is previous experience with the known events to understand the cause or exacerbation of the risks, or whether no experience exists but the probability is growing (e.g., cybersecurity or physical security);
- Whether (and the extent to which) the risk is being addressed by other groups (NERC, IEEE, etc.);
- Whether previous mitigation efforts have been used and, if so, why they were not effective;
- Whether there are actions that can be taken that can help to mitigate the risk (ability to have an impact);
- How the risk might change if no mitigations occur; and
- Whether the risk is caused by human activity or by natural causes.

These are only a few sample factors to consider when determining risk tolerability. Decision-makers should carefully consider a broad range of factors when determining risk tolerability.

Risk Evaluation Process

General responsibilities for WECC staff:

- Lead the Risk Evaluation, with support and collaboration from partners.
- Obtain and incorporate partner feedback as needed throughout the step.
- Facilitate successful Risk Identification.
- Ensure that documentation is complete, accurate, and orderly archived.

General responsibilities for partners:

- Assist WECC staff to determine whether any activity is already underway addressing this risk.
- Assist WECC staff to determine the tolerability of the risk and rank the risk.
- Review the documents from the Risk Evaluation, discuss the evaluation with subject matter experts within your organization (and others as needed), and provide feedback.

The Risk Evaluation Process has three primary components:

1. Identify activities underway to mitigate the risk;
2. Determine the tolerability of the risk; and
3. Rank the risk.

Identify Activities Underway to Mitigate the Risk

- Determine whether any activity is already underway that is addressing this risk, either directly or indirectly. This can include activities within industry groups (such as NERC, E-ISAC, IEEE, and CIGRE), within WECC Member entities, or other groups outside the electric power industry (natural gas, telecommunications, and others).
- The research should determine the overall objectives of the activity and the degree to which the activity addresses the risk.
- Determine whether any partners are involved in the activity. If not, strong consideration should be given to having partner representation in the activity. It is important that there are no duplicate efforts and that existing efforts are joined to mitigate known or emerging risks.

Determine the Tolerability of the Risk

- This is done by evaluating the outcome of the Risk Analysis and any activity already underway to mitigate the risk, and assessing the factors considered for determining risk tolerability.
- Determining risk tolerability can lead to a decision to:
    - **Accept:** Retain the risk by making an informed decision. Take or increase the risk to pursue an opportunity. This includes accepting the current activities that address the risk.
    - **Reduce:** Further action is required to remove the risk source, change the likelihood, or change the consequences.
    - **Transfer:** Sharing the risk (e.g., buying insurance, efforts led by others).
    - **Avoid:** Avoid the risk by deciding not to start or continue with the activity that gives rise to the risk.

Step 4: Risk Treatment

Step Overview

Risk treatment is the action taken in response to the risk evaluation. The purpose of the risk treatment step is to select and implement options for addressing risk[4].

Risk treatment is an ongoing process in which individual risk treatments (or combinations of treatments) are assessed to determine whether they are adequate to bring the residual risks to a tolerable level. If not, then new risk treatments are generated and assessed until a satisfactory level of residual risk is achieved. Partner feedback in Step 3 will be used to provide support or ideas when developing treatment options or if treatments can be implemented collaboratively among other groups.

Examples of treatment activities can include the support or development of:

- NERC/WECC Activities:
  - NERC Reliability Standards;
  - WECC Criteria;
  - NERC Reliability Guidelines;
  - Lessons learned;
  - WECC assist visits;
  - Technical conferences, workshops, and educational programs;
  - CMEP activities;
- Industry Activities:
  - Operations practices;
  - Lessons learned;
  - Best practices;
  - Studies or assessments;
  - Recommendations for action involving other groups; and
  - Specific plans of action.

Risk Treatment Process

Risk treatment involves a process of:

1. Identifying activities that could mitigate the risk;
2. Evaluating the expected effectiveness of each activity;
3. Determining the expected reduction in risk resulting from each activity;
4. Deciding whether the expected remaining risk is acceptable for each activity;
5. Selecting the activities to be undertaken;
6. Planning the activities; and
7. Carrying out and tracking the activities.

[4] ISO 31000 reference

WECC will track the identified treatments using a centralized method. The information for the treatments that will be tracked can include:

- Reasons for treatment selection, including expected benefits and potential challenges;
- Accountabilities for approving the plan and responsibility for its enactment;
- Resource requirements;
- Reporting, assurance, and monitoring requirements; and
- Priorities, timing, and schedules.

Roles and responsibilities for the Risk Treatment step can vary for each risk. In general, WECC staff will help administer and track activities and ensure that documentation is complete, accurate, and archived. WECC committee/forum members, industry subject matter experts, or potentially NERC or ERO Enterprise members may be used in any of the risk treatment process steps above.

Step 5: Recording and Reporting

Recording and reporting are the last formal steps in the lifecycle of each risk entered into the Risk Register. A risk management process is most effective when well-documented and shared. Reporting should consider the informational needs of partners and the usefulness of information for industry planning and decision-making. While the word “reporting” is in this step, it does not refer to a periodic published report. Instead, it refers to reporting that is determined appropriate for the specific risk, whether it be to the other WECC or NERC committees, decision-makers, or the WECC Board of Directors.

WECC staff will determine the appropriate level of reporting for each risk, progressing through the five steps of the WECC RMP. WECC will maintain a public copy of the RMP, its related documentation, and the WECC Risk Register and keep it up to date.

Recording

WECC staff is responsible for documentation associated with each step of the WECC RMP. Because this step concludes the activity for each risk, all the documentation for each risk reaching this step must be accurate, orderly, and complete. This documentation is a record of and justification for decisions and preserves the assessment results for future use. The types of documentation for each risk may vary; however, each risk will have a core set of documents in common.

WECC staff is responsible for:

- Recording these documents and any others.
- Ensuring that data is handled appropriately regarding confidentiality.
- Facilitating transparency by posting documents on a WECC webpage.

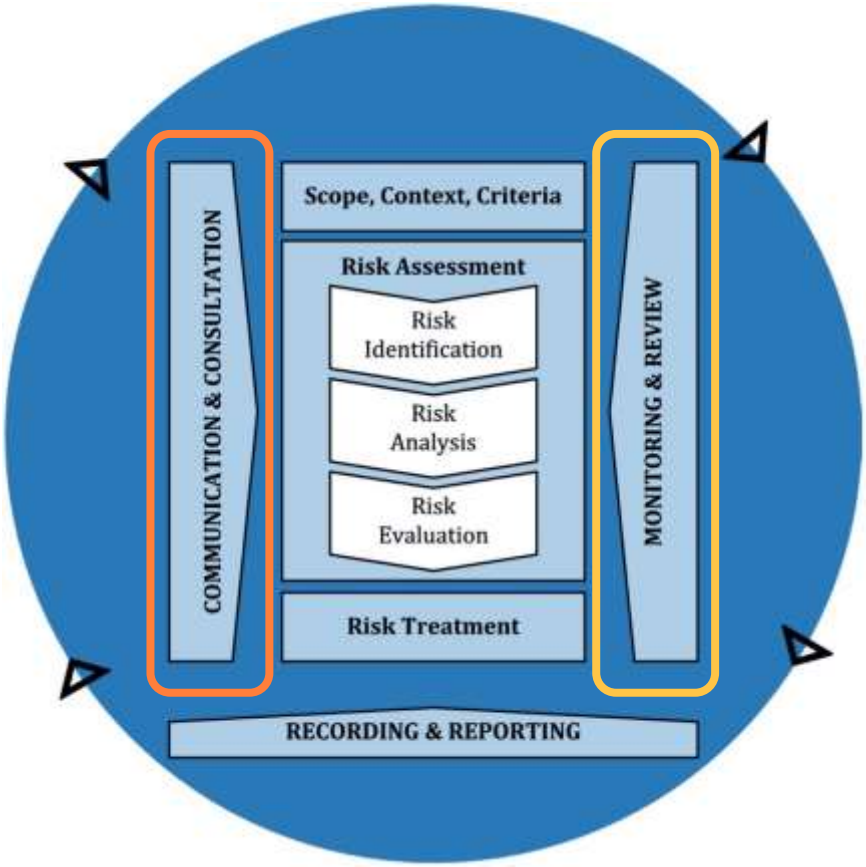
Reporting

Information about each risk reaching this step should be reported appropriately. Each risk is unique and could require different communication. WECC staff and Strategic Risk Partners must determine the information sharing required for each risk at this stage and carry out that communication.

Ongoing and Periodic Activities

While each risk progresses through the five steps, other activities occur periodically or continuously.

The ongoing activities reflect the right-hand portion of the framework diagram "Monitoring and Review," indicated in gold, and the periodic activities reflect the left-hand portion of the framework diagram "Communication and Consultation," indicated in orange.



Ongoing Activities—Monitoring and Review

These activities include ongoing monitoring and review of:

1. The risks examined through the WECC RMP; and
2. The effectiveness of the WECC RMP itself.

Ongoing Monitoring and Review of Risks

Because risks can change over time, continuing to monitor and review certain risks can help determine the effectiveness of mitigation activities and ensure that the risks remain at acceptable levels. The level of review should be appropriate to the rate at which the risk is occurring or changing. Risks at each stage of the RMP should be reviewed continually.

As actions are performed to reduce the risk, the risks will be monitored and reviewed through ongoing performance measures to ensure those risk mitigation activities are effective and that the residual risk is acceptable.

All approved risks on the Risk Register will be formally reviewed periodically at a minimum as follows:

- Extreme and High: Annually
- Medium: Biennially
- Medium-Low and Low: Triennially

The review will assess the risks based on the five steps to determine whether any changes are necessary. The reassessment can also be conducted at any time based on management, subject matter expert, or partner request based on new, updated, or trending information.

An important aspect of reviewing risks continually is ensuring that the Risk Register is updated. WECC staff will be responsible for ensuring the Risk Register is updated continually.

Ongoing Monitoring and Review of the WECC RMP

The WECC RMP helps WECC and partners identify and address known and emerging risks to the reliability and security of the WI BPS. It is important that WECC staff continually review the WECC RMP and make changes as necessary to increase its effectiveness.

The WECC RMP will be reviewed and updated biennially. The RMP can be reviewed and updated at any time based on management, subject matter expert, or partner request.

Periodic Activities—Communication and Consultation

Communication and consultation occur throughout the WECC RMP. The WECC Risk Framework Drawing contains a diagram and a corresponding table that describe interactions that occur throughout the RMP. Although communication and consultation are ongoing, certain activities are periodic. These include communication and consultation to:

- Develop a periodic risk reporting; and
- Carry out a periodic risk prioritization activity.

Communication and Engagement

Communication with experts within the industry is an essential part of a risk management process. Because the WECC RMP relies on input, engagement and participation in the RMP are critical to its success. Participants are encouraged to engage with others in the industry to better understand the known and emerging reliability and security risks and to bring that knowledge for input and discussion. There are several opportunities in this process to reach out to the industry for input. The RMP does not specify how or when this should be done; rather, it allows the participants to decide the best ways to gather input.

As various participants will have different communication needs and expectations, WECC staff will tailor its communications to these needs whenever possible. These communications will:

- Encourage engagement and accountability;
- Share information to reduce uncertainty;
- Distribute notifications through an online resource;
- Ensure that relevant expertise is used to inform each step of the process; and
- Inform other entity processes, such as corporate planning and resource allocation.

Periodic Risk Reporting

WECC staff will develop periodic reporting showing the progress in identifying and addressing known and emerging reliability and security risks.

To the greatest extent, recommendations and suggestions for risk mitigation should be included or referenced in the report to help partners become more aware of and reduce risk to their systems. Some of the objectives of the reporting may include:

- Bring awareness of the current risks and associated activities or outcomes.
- Provide information on industry recommendations or lessons learned.
- Provide information for partners to understand the RMP and how to engage with it.

Appendix 1: Subregions

WECC maintains a subregional view of the Western Interconnection to support risk analysis. Subregions are not meant to be an exact or equal division of the Western Interconnection. Still, they are a best effort to divide based on many considerations—geographic differences, country and state boundaries, load regions, Balancing Authorities, and other factors—while maintaining simplicity in collecting and assessing risk data. The subregional map may change as needed based on further analysis. This is the current version as of this writing:

Appendix 2: Reliability Adequacy Addendum

Further information to add context and clarity to the intent behind these terms and their factors.

Reliability Adequacy: Risks that can affect one or more factors are considered risks to the WI BPS's Reliability Adequacy. In other words, any single factor can affect reliability; it is not required to demonstrate any given risk as having multiple impacts. For any risk that affects more than one factor, the highest rated factor will be used in deciding a risk ranking and in decision-making (the highest common denominator).

- **Resource Adequacy:** Considered long-term unavailability of resources through an event or lack of planning.
    - *Capacity Factor*: Where long-term capacity is unavailable to meet current or forecast demand.
    - *Energy Factor*: Where long-term energy is unavailable to meet current or forecast demand.
- **Infrastructure Adequacy:** Considered the long-term unavailability of infrastructure through an event or lack of planning.
    - *Physical Transmission Factor*: Where long-term transmission assets are unavailable to meet generation or load requirements, either current or forecast.
- **Operational Adequacy:** Considered short-term unavailability due to operational loss. This assumes both resources and transmission remain sound, but due to operational risk events, are or become unavailable.
    - *Unplanned Generation Factor*: Where active-day or day-ahead generation is unavailable.
    - *Frequency Factor*: Operational risks creating off-nominal frequency conditions.
    - *Transmission Factor*: Transmission assets are operationally unavailable but otherwise remain sound.
    - *Inoperability Factor*: Support systems, technology, telecommunications, personnel, etc., are not available in the short-term for operational function.
    - *Resource Mix Factor*: In combination, resources are inadequate for the active-day or day-ahead operations but otherwise remain sound.

Appendix 3: Risk Roles and Responsibilities

Group	Roles
Board of Directors	• Review the prioritized list of Western Interconnection risks and associated activities, then provide strategic direction as needed
Strategic Partner Risk Advisory Group	• Review identified risks and provide industry perspective • Participate in Risk Evaluation reviews and advise on industry activities
Reliability Risk Committee (RRC)	• RRC members coordinate inside and outside their organization to understand reliability and security risks and share those risks for a holistic view of risks facing the Western Interconnection • Evaluate risks and determine where WECC partners require additional action • Develop risk treatment plans based on risk evaluation • Track and report progress of treatment plans
RRC sub-groups	• Execute strategic initiatives and projects assigned by the RRC • Identify, monitor, and manage reliability and security risks in its area • Work closely with the industry to formulate, create, or help implement mitigating procedures or practices, and monitor the effectiveness of those activities • Provide updates and information to the RRC regarding key risks (new or existing) to the interconnection and describe any mitigation efforts to address those risks • Execute on any assigned treatment plans
Reliability Assessment Committee (RAC)	• Coordinate and collaborate with the RRC to develop the list of known and emerging reliability and security risks and to address those risks as appropriate
Key Partner groups (e.g., MAC, WIRAB, NERC, E-ISAC)	• Achieve a high-level understanding of WECC's approach to reliability and security risk management • Engage with WECC to help identify and address known and emerging risks
WECC staff	• Oversee the WECC Risk Management Process to identify and address known and emerging reliability and security risks to the Western Interconnection • Work with partners to develop and maintain the WECC Risk Management process

	• Develop the master list of risks and identify and execute activities to address priority risks • Maintain the WECC Risk register • Provide input to the list of known and emerging reliability and security risks and associated mitigation activities for priority risks • Support and contribute to the execution of its risk management process through data gathering, risk analysis, assessments, evaluation, tracking, and other relevant activities • Maintain an ongoing dialogue with NERC on risk activities • Facilitate crossover between RRC and RAC • Provide guidance, training, and other outreach activities on the risk management process and risk priorities
NERC	• Provide regular updates to WECC on NERC Reliability and Security Technical Committee (RSTC) activities • Maintain an awareness of WECC risk activities

Approving Committee, Entity, or Person	Approval Date
Reliability Risk Committee	February 14, 2023

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.