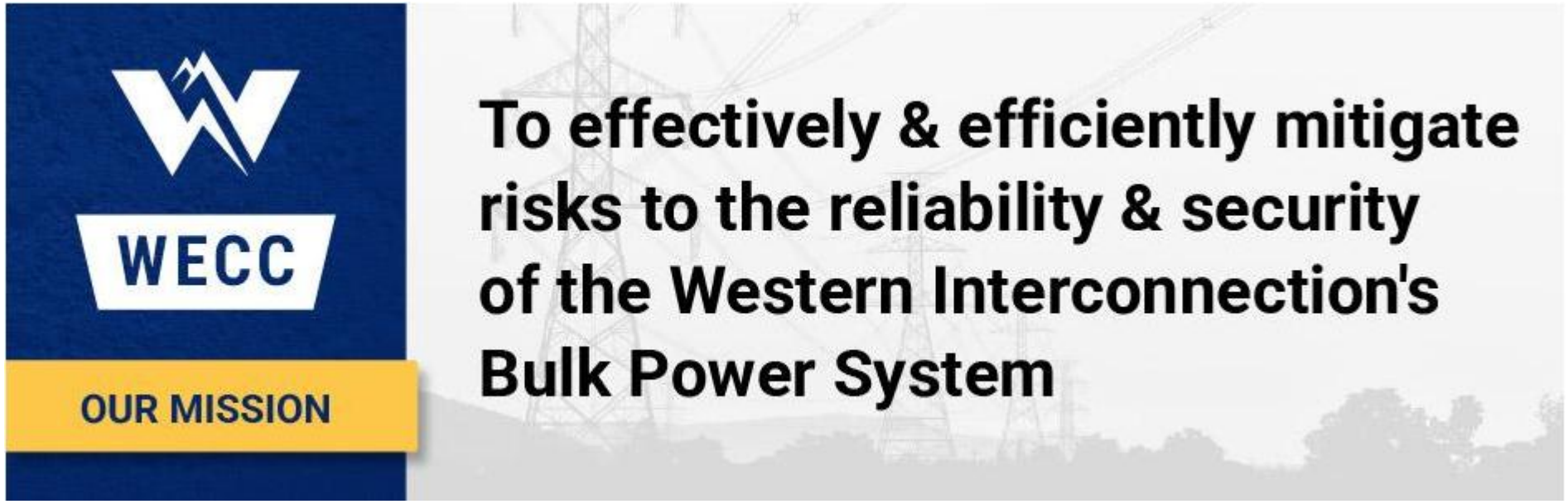
Electric Reliability
& Security for the West

Risk Management Program

Tim Reynolds
Director, Reliability Risk Management, WECC

WECC
OUR VISION
A reliable & secure
Bulk Power System in
the Western Interconnection


WECC
OUR MISSION
To effectively & efficiently mitigate
risks to the reliability & security
of the Western Interconnection's
Bulk Power System

Risk Management Program

Risk Analysis

- Intake (initiation)
- Categorization of risk
- Risk Register (tool)

Treatment

- Tolerability (appetite)
- Prioritizing actions and plans
- Tracking progress (Tracker Tool)

Monitoring

- Reporting
- Dashboards

Stakeholder

- Entity engagement (e.g., town halls)
- Industry involvement and progress

Risk Process Overview

From *Risk management — Guidelines* (ISO Standard No. 31000:2018), by International Organization for Standardization, 2018. Copyright 2018 by ISO.

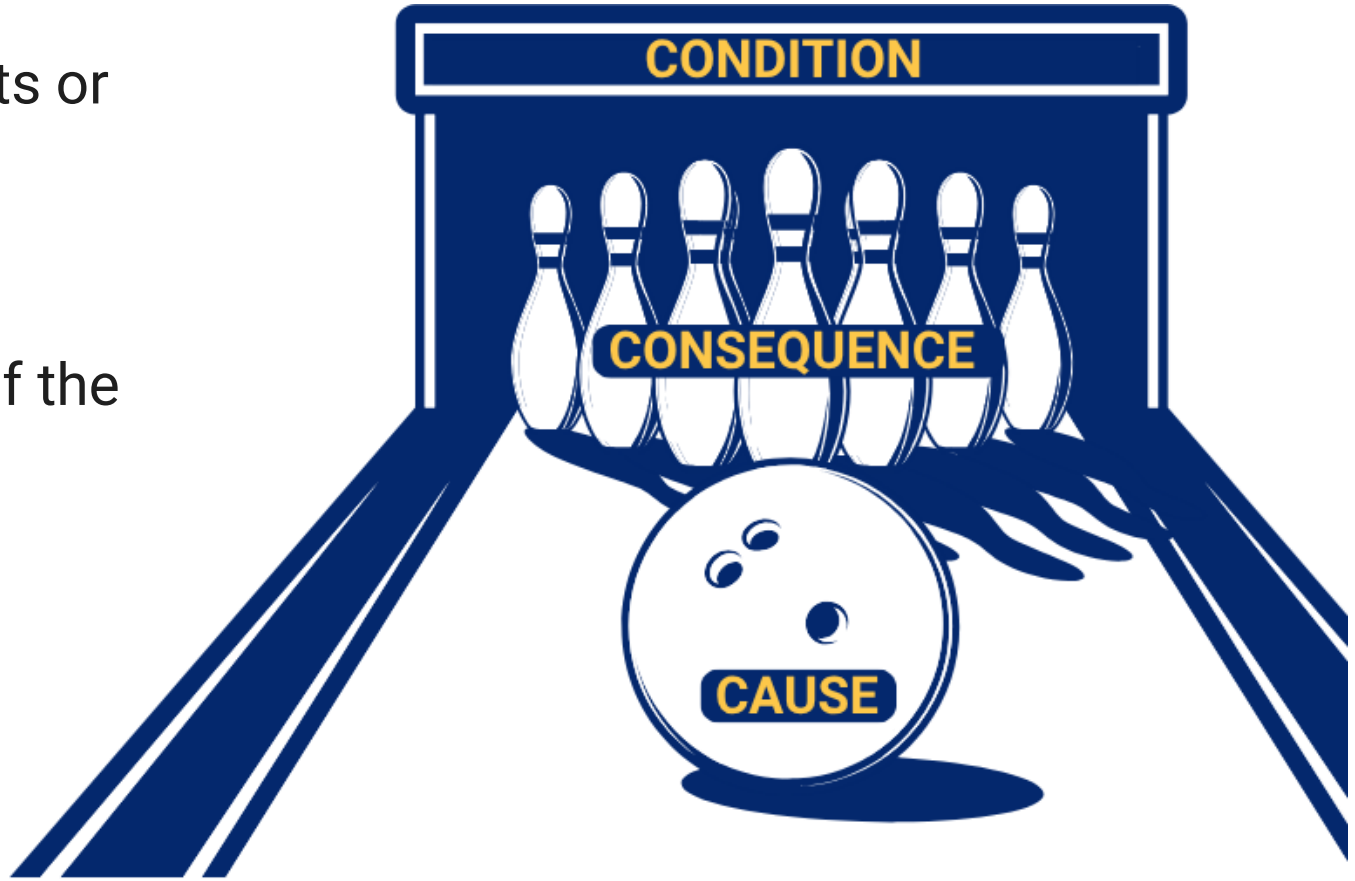
WECC Risk Management Process

Five Steps

1. **Risk Identification**: Identify existing and emerging risks to WI BPS reliability. Use diverse methods, using data-driven perspectives and partner input.
2. **Risk Analysis**: Understand risk attributes (causes, controls, time factors). Rate impact based on likelihood and consequence using the Risk Matrix.
3. **Risk Evaluation**: Support decisions by determining risk tolerability and ranking. Guides decisions; Accept, Reduce, Transfer, or Avoid.
4. **Risk Treatment**: Implement actions to address risks and achieve tolerable levels. Use an ongoing cycle of identifying, evaluating, and planning mitigation.
5. **Recording and Reporting**: Document and share risk information for planning and decision-making. Ensures accurate records and appropriate communication of each risk's status.

Risk Context – The Three C's

- Condition
  - Identifies known/potential events or risks of what can go wrong
- Consequence
  - Describes the result or impact of the condition, either immediate or delayed
- Cause
  - Identifies the root cause, the reason/factor that leads to the condition (If known)



Exercise

- Aliens have arrived!
  - What do the aliens want?
  - Why are they here?

Possible Responses

- To serve man
- Love
- Money
- Friends
- Mayonnaise
- Water or specialized minerals
- Research non developed planets
- Rare earth metals
- Water and food
- Knowledge
- To control humans
- Water
- LANGUAGES
- Oil
- Ranch dressing
- Take over everything
- They want proof of existence throughout the galaxy.
- Energy
- the cats
- To be friends
- Resources, aliens power their systems with gold.
- Conques
- Food
- Earth resources
- The land
- Resources
- Tacos
- Reality TV

Exercise

- Why do they want it? Why do they need it?

Reliability Adequacy — 3 Parts

- **Resource Adequacy** (Generation Assets)
- **Infrastructure Adequacy** (Transmission Assets)
- **Operational Adequacy** (Operations)

Reliability Risk Matrix Impact

Consequence/Impact—How could a typical event due to this risk affect BPS reliability in the Western Interconnection (WI)?	
Severe (C5)	Impacts may have widespread effects on the WI.
Major (C4)	Impacts may have widespread effects on multiple subregions 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.

Reliability Risk Matrix Likelihood

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. 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.

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	16	Extreme	21	Extreme	23	Extreme	24	Extreme	25
C4	**Major**	Medium	13	Medium	15	High	17	High	20	Extreme	22
C3	**Moderate**	Medium-Low	8	Medium-Low	10	Medium	11	High	18	High	19
C2	**Minor**	Low	5	Medium-Low	6	Medium-Low	7	Medium	12	Medium	14
C1	**Negligible**	Low	1	Low	2	Low	3	Low	4	Medium-Low	9

Online Engagement

[Risk Management Program | Western Electricity Coordinating Council]

WECC

Program Areas | Committees | Library | Toolbox | About | Search

Risk Management Program

The WECC Risk Management Program (RMP) is a collaborative initiative to address both established and emerging risks that could affect the reliability and security of the Western Interconnection's Bulk Power System (BPS). The program engages stakeholders — including utilities, system operators, regulators, and policymakers — to ensure a comprehensive approach to risk management.

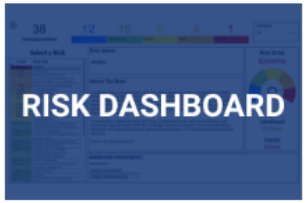
WECC engages with the industry through the RMP by sharing information about priority risks, gathering stakeholder input through its risk dashboard and other outreach opportunities including webinars, workshops, presentations, the Reliability in the West Discussion Series, the *State of the Interconnection* report, and more.

Key components of the RMP:

- Identification — Risks are identified by WECC (e.g., through assessments), stakeholders, or interested parties.
- Ranking — WECC and technical stakeholders analyze, rank, and sort the risks in accordance with WECC's ISO 31000-based risk management process and ranking methods.
- Prioritization — WECC works with stakeholders to prioritize the ranked risks through town halls and associated outreach based on risk tolerance, whether other entities (e.g., NERC) are already working to address them, etc.
- Strategy and Planning — WECC staff develops strategies and plans work to mitigate risks, including WECC scorecard initiatives, goals, stakeholder treatment plans, etc.
- Treatment — This is the work to address the risks through standards development, risk-based oversight, white papers, and other work products.

Ways to interact with the RMP:

- **Risk Dashboard:** Interact and learn about ranked risks within the Western Interconnection by risk category and severity.
- **Risk Register:** Download and review detailed data about identified risks to the Western Interconnection BPS, including results of the WECC RMP analysis and the WECC Reliability Risk Committee (RRC) evaluation of each risk.
- **System Performance Data Portal:** Get real-time information on grid conditions, including maps, graphics, and data related to the reliability of the Bulk Electric System.
- **State of the Interconnection:** This report, released in Q2 of each year, examines key indicators of system performance, providing an overview of the health of the system and challenges the Western Interconnection faced in the previous calendar year.



Risk Dashboard

38
Total Approved Risks

Low	Medium-Low	Medium	High	Extreme
12	15	6	4	1

Category: All

Select a Risk

Level	Risk Title
Extreme	Wildfire
High	Earthquake
High	Modeling, Performance, Interconnection Requirements, Data Availability, and Validation
High	Resource and Load Balance
High	Volcanic Eruption
Medium	Extreme Winds
Medium	Grid Transformation - IBRs and Inertia
Medium	Infrastructure Sabotage
Medium	Large Loads - Dynamic Modeling
Medium	Planning Case Accuracy
Medium	Time of Use / EV Charging Impacts to Grid
Medium-Low	Applicability of GO Registration and NERC Reliability Standards
Medium-Low	Artificial Intelligence
Medium-Low	Compromised Hardware/Software Supply Chain
Medium-Low	Drones and Unmanned Aircraft
Medium-Low	Drought (Aridification)
Medium-Low	Facility Rating - Ambient Temperature Impacts on Transmission Capacity
Medium-Low	Heat Wave/Dome
Medium-Low	Increasing number of long-term frequency deviations
Medium-Low	Insider Threat
Medium-Low	Malware
Medium-Low	Operational Network Breach

Risk Name:

Wildfire

About The Risk:

Condition: Major infrastructure (>230 kV) within close proximity and common corridors within one mile of large areas of dense, dry vegetation that have ignited, regardless of cause. (High-heat-level impact conditions, smoke density impact conditions, and facility designs vary by operating entity and should be considered.)(Entities' liability concerns may go beyond the NERC Reliability Standards and may employ more stringent wildfire management practices.)

Consequence: Implementation of Energy Emergency Alerts, up to and including load shedding of greater than 5,000 MW. Damage caused by unusual fire & wind conditions (firenado) and operational impact (possibly several days) from fire suppression/retardant methods.

Cause: Any ignition source.

Additional Information:

Document/Link

Wildfire Dashboard

Wildfire Weekly Report

Risk Scale

Extreme

Likelihood
Unlikely

Impact
Severe

Risk Register

WECC Risk Register | Western Electricity Coordinating Council

WECC WESTERN INTERCONNECTION RISK REGISTER Reliability Risk Inventory			
ID NO	CATEGORY	RISK TITLE	RISK STATEMENT (Double click to see more info)
CRM-001	GT: Changing Resource Mix	Generation Resource Mix Impacts to Future Transmission Congestion	**Condition:** Long-term regional transmission planning studies should be done to produce multiple reasonably likely scenarios and allow time to
CYB-001	Cybersecurity	Artificial Intelligence	**Condition:** Publicly available information about entities, including company organization/employees, products/services used, physical
CYB-002	Cybersecurity	Compromised Supply Chain	**Condition:** Compromised vendors can be a source of cyber-attacks on critical infrastructure.
CYB-003	Cybersecurity	Cybersecurity in Transmission Planning	**Condition:** Traditional transmission planning processes do not include cyber-informed transmission planning approaches that incorporate
CYB-004	Cybersecurity	Insider Threat	**Condition:** A trusted insider uses their authorized access to deliberately or accidentally harm assets.
CYB-005	Cybersecurity	Internet of Things (IoT)	**Condition:** Consumer Internet of Things (IoT) devices connected to the grid's distribution network.
CYB-006	Cybersecurity	Malware	**Condition:** Infection from any source on any entity's Corporate system of malicious program or code.
CYB-007	Cybersecurity	Perimeter Breach	**Condition:** Unauthorized actions on the digital assets within an organizational network.
CYB-008	Cybersecurity	Perimeterless Operational Technology	**Condition:** Systems and software used to peripherally interact or transmit into cyber assets that are not within an enterprise-owned network
CYB-009	Cybersecurity	Phishing and Social Engineering	**Condition:** Threat actor exploits trusted single insider access to harm critical cyber assets.
CYB-010	Cybersecurity	Physical Attacks on Cyber Assets	**Condition:** Insufficient physical controls to protect against unauthorized physical access to cyber assets.
CYB-011	Cybersecurity	Public Cloud / Cloud Computing	**Condition:** Cloud computing is a model for enabling universal, convenient, and on-demand network access to a shared pool of
CYB-012	Cybersecurity	Third Party Operations	**Condition:** Unvetted and unmonitored 3rd-parties operation of cyber assets.
CYB-013	Cybersecurity	Unauthorized Software & Hardware	**Condition:** Unauthorized software and hardware within an organizational network. This includes authorized software and hardware that is end-of-life
CYB-014	Cybersecurity	Zero-Day Exploit	**Condition:** A computer-software vulnerability previously unknown to those who interested in its mitigation.

Risk Register

WECC Risk Register | Western Electricity Coordinating Council

WECC Risk Management Program Analysis								
CONSEQUENCE / IMPACT LEVEL	MANDATORY CONTROLS	EMERGING TREND	EVENT HISTORY	LIKELIHOOD LEVEL	EXPECTED RISK TIMEFRAME	NATURE OF RISK	WEIGHTING SCORE	WEIGHTING VALUE
Minor	In Place	Increasing	Historical and generally published	Likely	Long Term (5+ yrs.)	Man-Made	13.0	Medium
Moderate	Some	Increasing	Historical and generally published	Almost Certain	Near Term (1-5 yrs.)	Man-Made	21.0	High
Moderate	Some	Increasing	Historical and generally published	Likely	Exists today	Man-Made	17.0	High
Insignificant	In Place	Neutral	No historical or minimally publicized	Unlikely	Exists today	Man-Made	1.0	Low
Moderate	Some	Neutral	Historical and highly publicized	Possible	Exists today	Man-Made	16.0	High
Minor	None	Increasing	Historical and generally published	Likely	Exists today	Man-Made	13.0	Medium
Moderate	In Place	Increasing	Historical and highly publicized	Likely	Exists today	Man-Made	17.0	High
Major	In Place	Neutral	Historical and highly publicized	Possible	Exists today	Man-Made	18.0	High
Moderate	Some	Increasing	No historical or minimally publicized	Possible	Exists today	Man-Made	16.0	High
Minor	Some	Increasing	Historical and highly publicized	Likely	Exists today	Man-Made	13.0	Medium
Minor	In Place	Neutral	Historical and generally published	Likely	Exists today	Man-Made	13.0	Medium
Moderate	Some	Increasing	Historical and generally published	Possible	Near Term (1-5 yrs.)	Man-Made	16.0	High
Minor	None	Increasing	No historical or minimally publicized	Likely	Exists today	Man-Made	13.0	Medium
Minor	In Place	Neutral	Historical and highly publicized	Unlikely	Exists today	Man-Made	1.0	Low
Moderate	Some	Increasing	Historical and highly publicized	Likely	Exists today	Man-Made	17.0	High

Inverter-based Resource (IBR) Risks

- Applicability of GO Registration and NERC Reliability Standards
- Increasing number of long-term frequency deviations
- Modeling, Performance, Interconnection Requirements, Data Availability, and Validation
- Grid Transformation — IBRs and Inertia
- IBR — System Restoration — GFM (BESS, PV, wind)

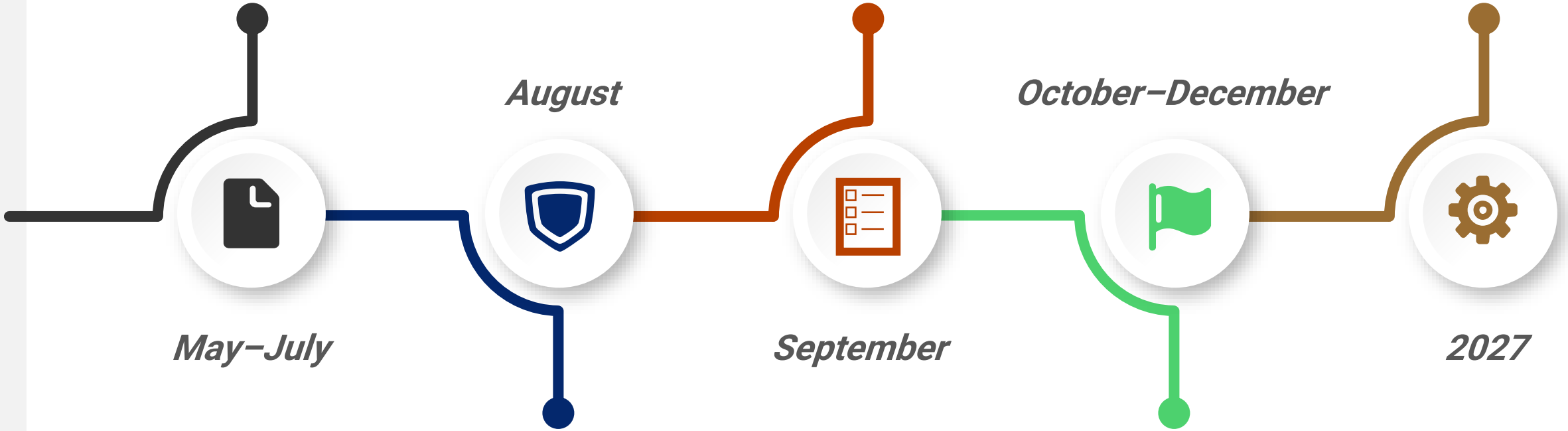
PRC-024 Purpose

"To verify and validate that the dynamic models and associated parameters used to assess Bulk Electric System (BES) reliability represent the in-service equipment of Bulk Power System (BPS) facilities including generating facilities, transmission connected dynamic reactive resources, and high-voltage direct current (HVDC) systems."

https://www.nerc.com/globalassets/standards/reliability-standards/mod/mod-026-2.pdf

Risk Management Program — 2026 Activity Timeline

Tolerance Outreach/Feedback
- **Reliability in the West**
- **WECC Town Hall**
- **Updated Website**



ELECTRIC RELIABILITY & SECURITY FOR THE WEST

ENGAGE WITH WECC

WECC

engage@wecc.org

www.wecc.org | 801-582-0353

155 N 400 W, Salt Lake City, Utah 84103, USA