Electric Reliability
& Security for the West

Risk Management as an Organizational Obligation

Joshua Yang
Enforcement Attorney

Risk Overview

- **What is Risk?**
  - Possibility of Adverse Consequences.
  - Exposure to danger or the chance that an unwanted event may occur.
- **What is Risk Assessment?**
  - Systematic process used to identify potential adverse consequences, analyze likelihood, and evaluate potential impact.
- **What does Risk Management look like?**
  - Prioritization, targeting, and implementation of strategies to mitigate, transfer, accept, or avoid risk.
  - Continual tracking of risk landscape and effectiveness of current measures.

What is Risk?

What is Risk?

Risk
What risk is being managed?
Likelihood
What is possibility of the risk occurring?
Impact
What is the potential for harm?

Conceptual Example

Commercial Airline Incident

Likelihood: Remote

Impact: Extreme

Risk: Moderate

Minor Car Accident

Likelihood: Moderate

Impact: Intermediate

Risk: Moderate

Inherent vs. Residual Risk

Inherent Risk

The baseline risk that exists before any controls or mitigations are applied.

- Function
- Size
- Asset configuration
- Reliability impact

High

Medium

Low

Residual Risk

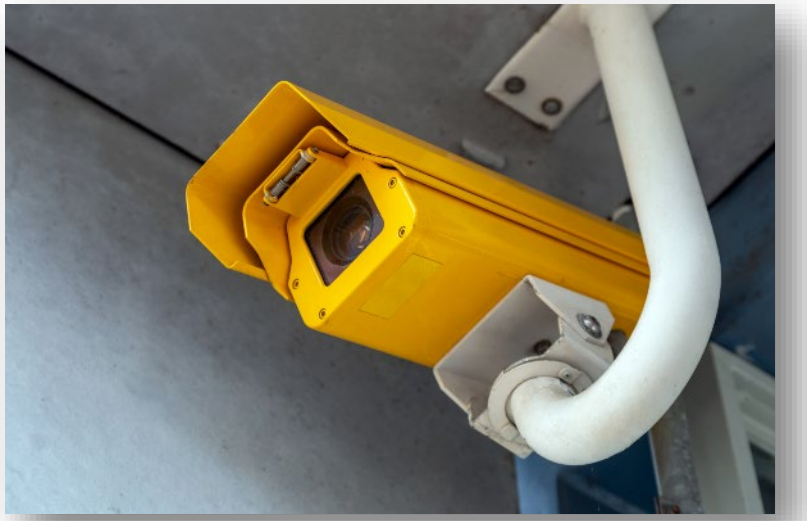
Remains after mandatory controls, mitigation measures, and compliance standards have been implemented.

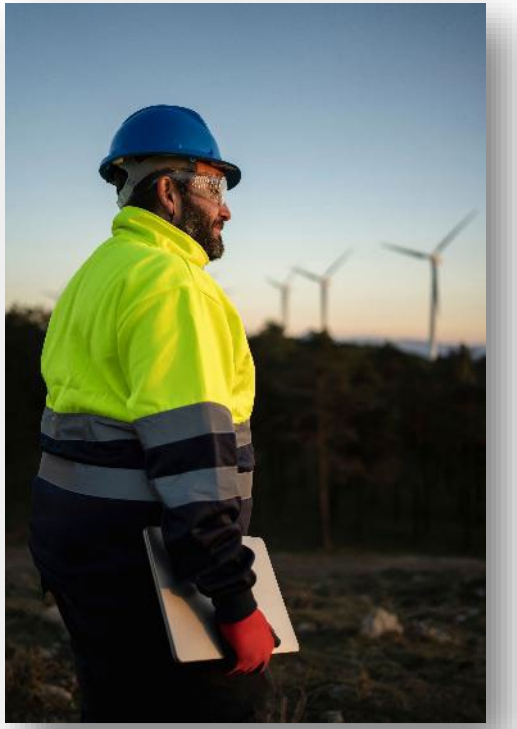
- Have the remaining vulnerabilities and subsequent impacts been identified?
- Is the remaining exposure acceptable?
- Requires continuous monitoring, as the threat landscape changes and is dynamic in nature

Inherent Risk

Examples of Inherent Risk

- Cybersecurity
- System complexity
- Third-party vendors





Residual Risk

Examples of Residual Risk

- Cybersecurity threats
- Third-party/supply chain risks
- Insider threats
- Physical safety/hazards
- Financial risks
- Operational risk

Conceptual Example

Minor Car Accident

- Inherent risks:
  - Capable speed
  - Number of passengers
- Residual risks:
  - Other drivers
  - Road conditions

Risk Highlight – Third Parties

Third Party

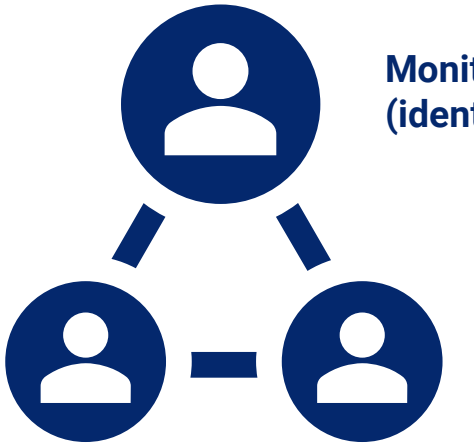
- Outsourced compliance services
- Vendors
- Consulting

Your compliance obligations are YOUR responsibility!

Risk Assessment

Identification of Current, Potential, and Emerging Risks

- What are the current landscapes and risk profiles created by your business operations and infrastructure?
- How are you monitoring and tracking risks?
- Are there resources committed to these tasks?



Monitoring methodology (identification/analysis)

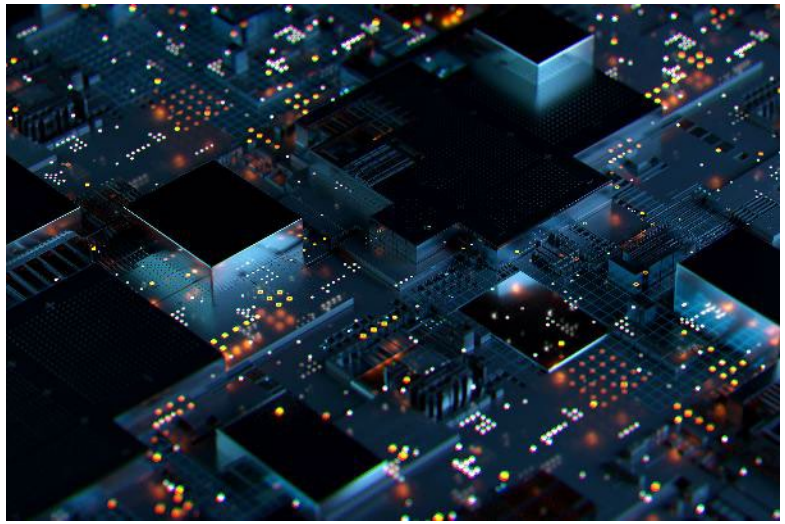
Compliance department; task forces; Steering committees; notification to board/executives/leadership

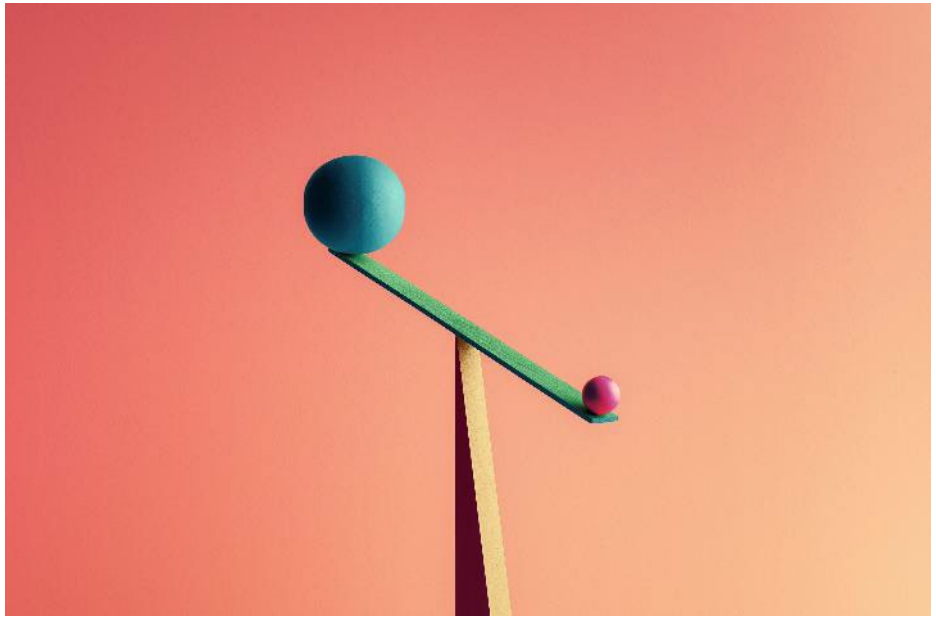
Periodic review and discussion of risks

Risk Assessment

Likelihood and Consequence

- How likely are the risks to occur?
- What is likely to be the outcome?
- What is the worst-case scenario that could feasibly happen?





Remember, Risk is based on Probability and Impact

Risk Assessment — Tools

The COSO Framework

- The Committee of Sponsoring Organizations of the Treadway commission
- Guidelines to design, implement, and evaluate internal controls
- WECC evaluation of Registered Entity internal controls using five components: Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring

The ISO 31000

- The International Organization for Standardization
- Principles and guidelines for Risk Management
- Used by WECC Reliability Planning and Performance Analysis (RPPA) along with the Reliability Risk Committee (RRC) composed of WECC and industry stakeholders to identify, analyze, and provide situation awareness for reliability risks through the Risk Register

Risk Assessment — ISO 31000

Identify the internal and external risks associated with the organization's ability to achieve its goals.

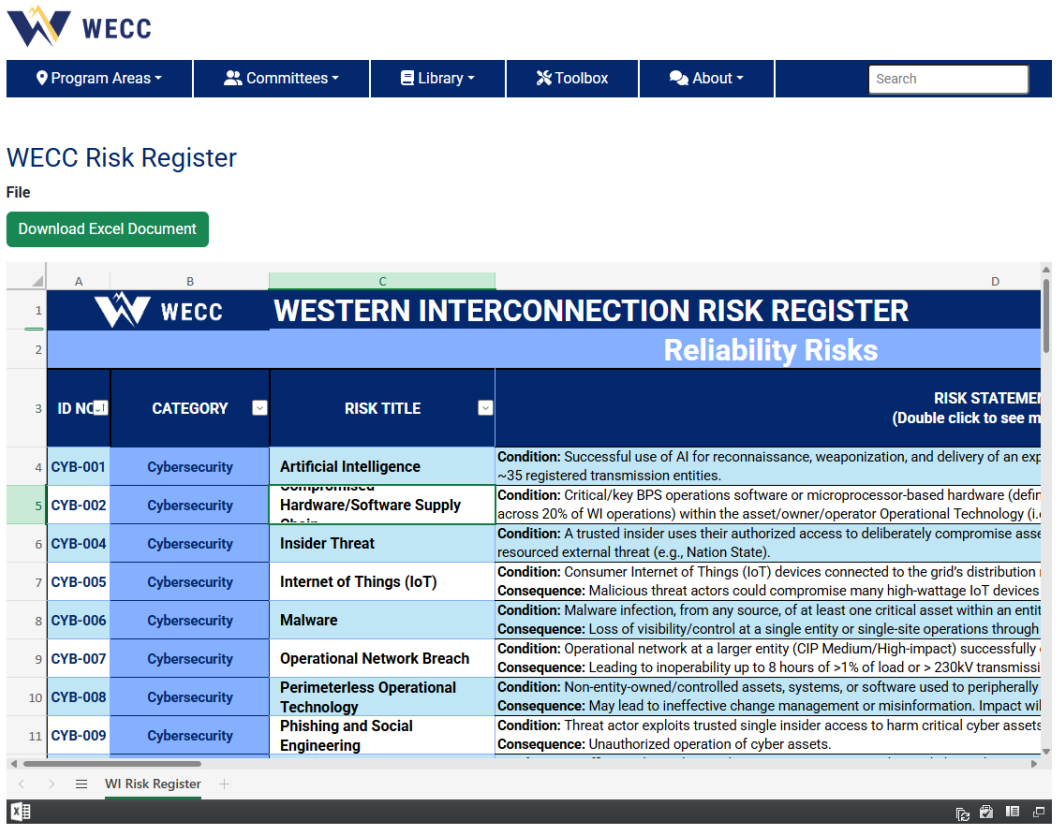
Use a risk assessment to evaluate the likelihood and impact of the identified risk, including the evaluation of the existing controls and processes used to manage the risk.

Mitigation includes designing, improving, and implementing internal controls to address assessed risks.

Continuously track organizational risks and adjust your internal controls as needed.

Risk Registers and Program Awareness

- Reliability Risk Committee
  - WECC
  - Industry stakeholders
- Tracks and provides situation awareness for current and emerging reliability risks
- Industry input is appreciated



Mapping Standards to Risk Scenarios

Standards and Requirements exist to mitigate a specific reliability risk.

Identify Standard-specific failure points and risks

Internal Controls Guidance And Compliance Failure Points

File Type	Title	Modified
PDF	CIP-003-8 Controls Guidance and Compliance Failure Points	2024-07-09
PDF	CIP-005-7 Controls Guidance and Compliance Failure Points	2024-07-09
PDF	CIP-007-6 Controls Guidance and Compliance Failure Points	2024-11-07
PDF	CIP-008-6 Controls Guidance and Compliance Failure Points	2024-07-09
PDF	CIP-010-4 Controls Guidance and Compliance Failure Points	2024-08-30
PDF	CIP-012-1 Controls Guidance and Compliance Failure Points	2024-07-09
PDF	CIP-012-2 Controls Guidance and Compliance Failure Points	2025-03-25
PDF	CIP-013-2 Controls Guidance and Compliance Failure Points	2024-07-09
PDF	CIP-014-3 Controls Guidance and Compliance Failure Points	2024-07-09
PDF	COM-001-3 Controls Guidance and Compliance Failure Points	2024-07-09
PDF	EOP-004-4 Controls Guidance and Compliance Failure Points	2024-07-09
PDF	EOP-011-4 Controls Guidance and Compliance Failure Points	2025-05-22
PDF	EOP-012-2 Controls Guidance and Compliance Failure Points	2025-02-04

Mapping Standards to Risk Scenarios

Risk

What specific risk are you trying to control or mitigate?

☐ Reliability Standard Development Plan	☐ Industry Stakeholder Identified
What is the risk to the Bulk Electric System (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):	
Multiple winter storm events since 2011 have demonstrated the risk to the Bulk Power System when generators fail to prepare adequately for extreme cold weather conditions. The EOP-012 Reliability Standard provides a comprehensive framework of requirements for generator cold weather preparedness to ensure that more generators are available during extreme cold weather conditions and not forced offline due to foreseeable freezing issues. FERC, however, has identified several ambiguities and other reliability issues which could reduce the effectiveness of this standard. FERC directed NERC to revise EOP-012-2 and associated definitions to address these issues by March 2025.	
Purpose or Goal (What are the reliability gap(s) or risk(s) to the Bulk Electric System being addressed, and how does this proposed project provide the reliability-related benefit described above?):	
The purpose of this project is to address the directives identified by FERC in its June 27, 2024 order approving Reliability Standard EOP-012-2 and directing further modifications. *N. Am. Elec. Reliability Corp.*, 187 FERC ¶ 61,204 (2024). In that order, FERC found that further improvements needed to be made to address ambiguous language and address other reliability gaps/implementation issues in the	

EOP-012-2 – Extreme Cold Weather Preparedness and Operations

A. Introduction

1. **Title:** **Extreme Cold Weather Preparedness and Operations**
2. **Number:** EOP-012-2
3. **Purpose:** To address the effects of operating in extreme cold weather by ensuring each Generator Owner has developed and implemented plan(s) to mitigate the reliability impacts of extreme cold weather on its applicable generating units.

17

Risk Assessment — Example

Your company is in the midst of a procurement process for a third-party consulting firm to provide NERC compliance services for your Category 2 IBR solar facility. Your company will maintain the registration for its GO and GOP functions. During the Request for Proposal process, the top-choice consulting firms all indicated that they operate remotely (with periodic on-site work) and share and store files on a cloud-based server.

Do not edit
How to change the design

What kind of risks are posed by using the services of the third-party consulting firm?

ⓘ The Slido app must be installed on every computer you're presenting from

slido

Risk Management

How do Organizations Manage Risk?

1. Stay ahead of ongoing and upcoming issues
2. Identify and categorize risks
3. Document, implement, and update procedures

Culminating in a strong internal compliance program

DOJ Evaluation of Corporate Compliance Programs

Three Fundamental Questions

Question 1: Is the corporation's compliance program well designed?

- Risk Assessment
- Policies and Procedures
- Training and Communications
- Confidential Reporting Structure and Investigation Process
- Third Party Management
- Mergers and Acquisitions

Three Fundamental Questions

Question 2: Is the program being applied earnestly and in good faith? In other words, is the program adequately resourced and empowered to function effectively?

- Commitment by senior and middle management
- Autonomy and resources
- Compensation structure and consequence management

Three Fundamental Questions

Question 3: Does the corporation's compliance program work in practice?

- Continuous improvement, periodic testing, and review
- Investigation of misconduct
- Analysis and remediation of any underlying misconduct

FERC Policy Statement — Penalty Guidelines

Seven Factors to Consider to Determine Whether an Organization has an Effective Compliance Program

1. Established standards and procedures to prevent and detect violations.
2. Governing authority is knowledgeable about the content and operation, and it exercises reasonable oversight with respect to the implementation and effectiveness.
3. Uses reasonable efforts not to include within its substantial authority personnel any individual who has engaged in violations or other conduct inconsistent with an effective compliance and ethics program.

FERC Policy Statement — Penalty Guidelines

Seven Factors, continued …

4. Takes reasonable steps to communicate periodically and in a practical manner its standards and procedures and other aspects of the compliance and ethics program … by conducting effective training programs and otherwise disseminating information.
5. Ensures that the compliance program is followed, including auditing and monitoring, evaluates effectiveness periodically, and maintains and publicizes a system with mechanisms for anonymity or confidentiality for employees to report or seek guidance without fear of retaliation.

FERC Policy Statement — Penalty Guidelines

Seven Factors, continued …

6. Promotes and enforces the compliance program consistently throughout the organization through appropriate incentives and appropriate disciplinary measures.
7. Responds appropriately to detected violations and prevents further similar violations, including making any necessary modifications to the compliance program.

FERC Policy Statement — Enforcement

Thirteen Questions

1. Does the company have an established, formal program for internal compliance? Is it well documented and widely disseminated within the company?
2. Is the program supervised by an officer or other high-ranking official?
3. Does the compliance official report to or have independent access to the chief executive officer and/or the board of directors?
4. Is the program operated and managed to be independent?
5. Are there sufficient resources dedicated to the compliance program?
6. Is compliance fully supported by senior management? (e.g., actively involved in compliance efforts and do company policies regarding compensation, promotion, and disciplinary action take into account the relevant employee's compliance with Commission regulations and the reporting of any violations?)

FERC Policy Statement — Enforcement

Thirteen Questions

7. How frequently does the company review and modify the compliance program?
8. How frequently is training provided to all relevant employees?
9. Is the training sufficiently detailed and thorough to instill an understanding of relevant rules and the importance of compliance?
10. In addition to training, does the company have an ongoing process for auditing compliance with commission regulations?
11. How has the company responded to prior wrongdoing? Did it take disciplinary action against employees involved in violations?
12. When misconduct occurs, is it a repeat of the same offense or misconduct of a different nature?
13. Does the company adopt and ensure enforcement of new and more effective internal controls and procedures to prevent a recurrence of misconduct?

Risk Management

What risk is being managed?

- Inherent and residual risk
- Current risk
- Potential risk
- Emerging risk

Management Responsibilities (COSO)

1. **Define objectives** clearly to enable the identification of risks and **define risk tolerances**
2. **Identify, analyze, and respond to risks** related to achieving the defined objectives
3. **Consider the potential for fraud** when identifying, analyzing, and responding to risks
4. Identify, analyze, and **respond to significant changes** that could affect the internal control system

Conceptual Example

Minor Car Accident

What risks can be identified and categorized?

- Who is driving the vehicle? Are they well-trained?
- Do you have car insurance? What kind of coverage?
- What are the safety features? What condition are they in?

Program management

- When you are purchasing your vehicle, you are assessing the safety of the vehicle and the risks it poses to drive it.
  - Modern SUV vs. Motorcycle vs. Vintage sports car

Leading Indicators of Weakness

Risk Requires Continual Monitoring and Tracking

- Behavior and performance signals often precede failures.
  - Are employees acting (in good faith) in accordance with the internal compliance program?
- Recurrence is a risk signal.
  - Repeated issues indicate systemic weaknesses.
  - Shows vulnerability in:
    - Post-event evaluation
      - Data capture; record/log keeping and maintenance; analysis
    - Implementing lessons learned
      - Program execution; training; communications

Do NOT wait until something goes wrong

Risk Management Example

A battery storage facility relies upon a single vendor to perform system updates, modifications, and evaluation of their equipment. An upcoming NERC Reliability Standard mandates the design and operation of inverter-based resources to meet or exceed voltage ride-through requirements, necessitating certain components on the asset to be modified and assessed. The vendor is reporting significant backlog to meet the demand and has estimated a lead time of 8–12 months. The NERC Reliability Standard will become effective and enforceable in six months.

Do not edit
How to change the design

What are ways in which the battery storage facility can prepare for, and mitigate the risks posed by the vendor backlog?

ⓘ The Slido app must be installed on every computer you're presenting from

slido

Risk Management

Resources

- Department of Justice Evaluation of Corporate Compliance Programs (DOJ Evaluation)
- Revised Policy Statement on Penalty Guidelines (PL10-4-000) (Commission Order)
- Policy Statement on Enforcement (PL-06-1-000) (Commission Order)
- WECC Risk Register (WECC Risk Register | Western Electricity Coordinating Council)
- WECC Internal Compliance Program Self-Assessment (Internal Compliance Program Self-Assessment.pdf)
- NERC Rules of Procedure (Rules of Procedure)
- Internal Controls Guidance and Compliance Failure Points / Internal Controls Failure Points PDFs (Compliance — United States | Western Electricity Coordinating Council)

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