RELIABILITY & SECURITY

Workshop - Tempe, Arizona

March 25–26, 2025

<Public>

WECC

Strengthening Internal Control

March 26, 2025

Molly Elliott

Senior Technical Analyst, Oversight Planning

Overview

Take the next step to more effective internal control

- How Internal Control fits into the Risk-based Monitoring Framework
- Using Risks and Potential Failure Points to Identify the Need for Controls
- Selecting Controls
- Continuous Improvement

What is an Internal Control?

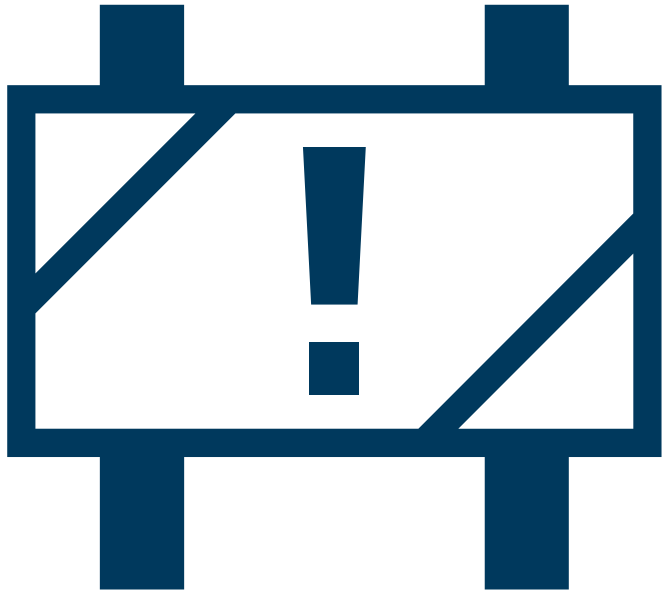
Internal controls are the . . .

- Processes
- Practices
- Policies or procedures
- System applications, technology, and tools

To address **risks** associated with the reliable operation of its business

<Public>

Start With the Risk

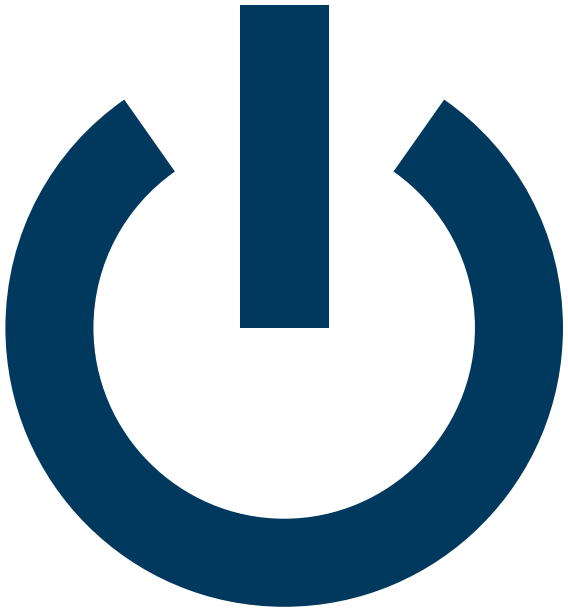


Risk(s) /risk/

noun

Anything that jeopardizes achieving defined goals.

Why are we talking about controls?



Objective: Reliability

- Protection Systems
- Preventive Maintenance

Objective: Security

- Physical barriers
- RTA and RTM Encryption

Reliability & Security
is the focus of NERC Standards

<Public>

Why Are We Talking About Controls?

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.

Why Are We Talking About Controls?

ERO Enterprise Risk-based Monitoring Framework

- When we monitor, we must consider the risk the entity poses to reliability and security
- Effective controls reduce entity risk
- Provides context for the engagement
- When noncompliance is found, controls are put in place to mitigate risk going forward

Using Risks and Potential Failure Points to Identify the Need for Controls

Reliability & Security Risks

- Enterprise Risk Management
- Compliance Monitoring and Enforcement Program Implementation Plan (CMEP IP)
- Western Interconnection Risk Register
- NERC Standards
- Industry groups

Risk Analysis

Identify the processes or activities in your organization that address those objectives

Map the current process into individual steps or tasks

- What could go wrong?
- What measures are in place to prevent or detect errors, anomalies, malice, or noncompliance?
- How could someone bypass existing controls?

Common Failure Points: Physical Access Approval

Physical Access Approval Process

Consider

- Hand-offs
- Exchanges of information/data
- Time constraints
- Tasks with no distinct owners

slido

Please download and install the Slido app on all computers you use

What can go wrong with the physical access approval process?

ⓘ Start presenting to display the poll results on this slide.

Common Failure Points: Facility Ratings

Facility Ratings Process

Consider:

- Manual processes
- External dependencies
- Changes
- Exceptions/non-routine actions

slido

Please download and install the Slido app on all computers you use

What can go wrong with the Facility Rating process?

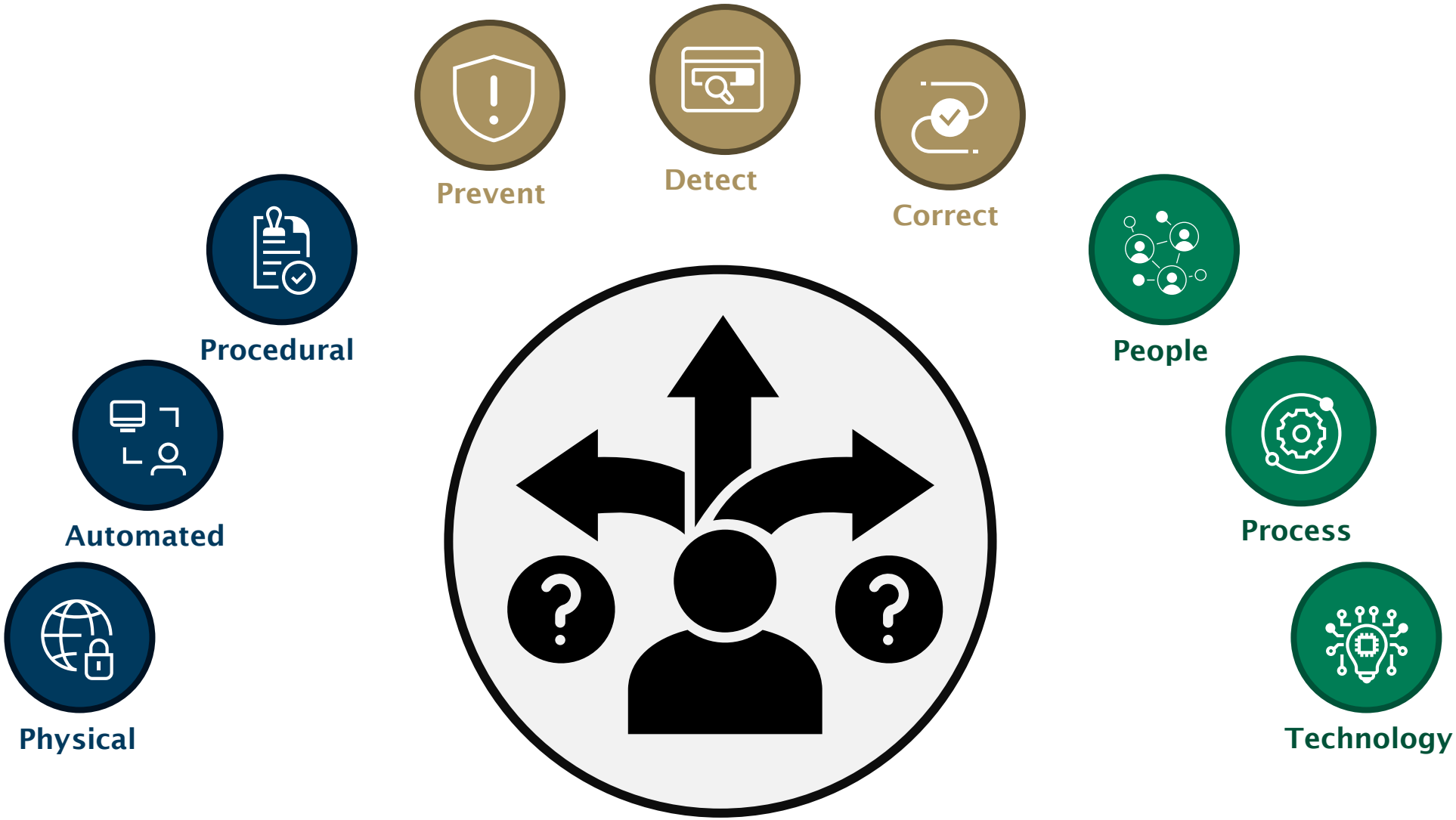
ⓘ Start presenting to display the poll results on this slide.

Common Failure Points

Information & Communication Flow

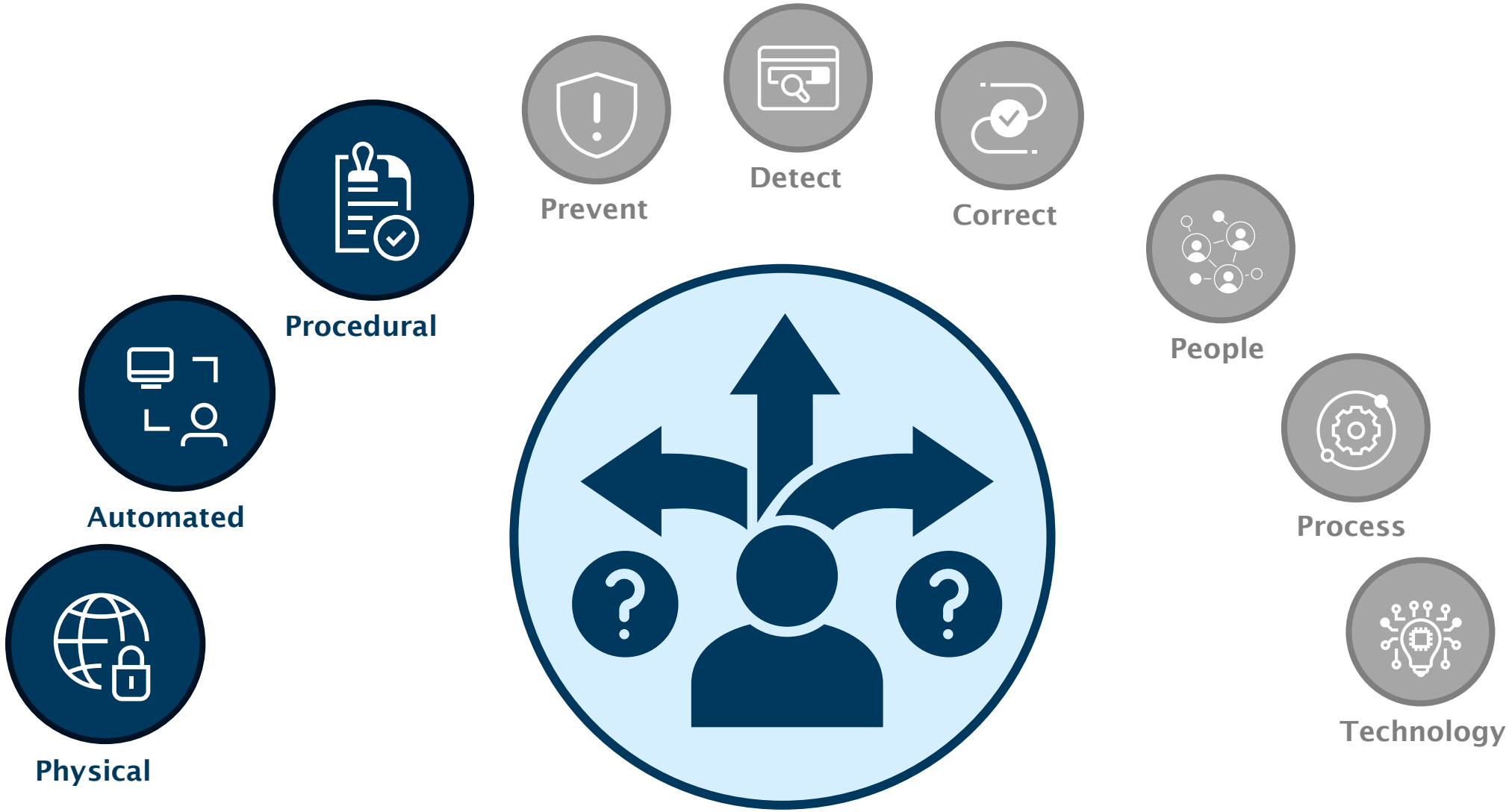
- Accuracy
- Access
- Timelines

Selecting Controls



Selecting Controls

Selecting Controls



Selecting Controls

Objective: Prevent Intrusion by Bad Actor

Fence	Security Guard	Sign-in Sheet
• Prevent • Physical • Technology	• Prevent or Detect or Correct • Procedural • People	• Prevent or Deter or Detect • Procedural • Process

Procedural Controls

Procedures mitigate a risk: Lack of Knowledge

- Inconsistency
- Absences
- Turnover

Benefits

- Inexpensive and easy to implement
- Track process changes and exceptions
- Support processes that are performed infrequently

Procedural Controls—What's Missing?

Pignoli

Ingredients

- 2 cans almond paste
- 2 egg whites
- 1 cup sugar
- powdered sugar
- egg white
- pine nuts

Directions

- Bake at 350 for 15 minutes

slido

Please download and install the Slido app on all computers you use

What is missing in this recipe?

ⓘ Start presenting to display the poll results on this slide.

Procedural Controls—What's Missing?

Purpose: How many cookies am I making?

Incomplete information/tribal knowledge:

- What size is the can of almond paste?
- Which brand?

Step-by-step instructions:

- Blend the almond paste, sugar, and egg whites in a double boiler.
- Remove from heat and cool.
- Knead on board sprinkled with powdered sugar.
- 3rd egg white is brushed on the cookie before rolling in pine nuts.
- Refrigerate before shaping.
- Bake on parchment paper.

Layering Controls

Procedural controls alone:

- Easy to circumvent
- Susceptible to human error
- May not produce enough evidence to monitor the process

Common Control Activities

	Prevent	Detect	Correct
People	Training, communication, coordination	Peer review, manager review, performance review	Disciplinary actions, remedial training
Process	Segregation of duties, action plans, checklists, triggers, identification/scoping, change authorization	Spot-checks, internal audits, inventory counts, field walkthroughs	Business continuity plans, updated policies & procedures, corrective action plans
Technology	Access controls, firewalls, fence, Locks	Alarms, alerts, reconciliations, data integrity checks, monitoring	Patching, backups

Continuous Improvement

"What is not defined cannot be measured.
What is not measured, cannot be improved. "

—Attributed to Lord Kelvin

Documentation

Set up your program to be measured and reviewed

- Current state
- Evidence of performance
- Lessons learned

Measurement

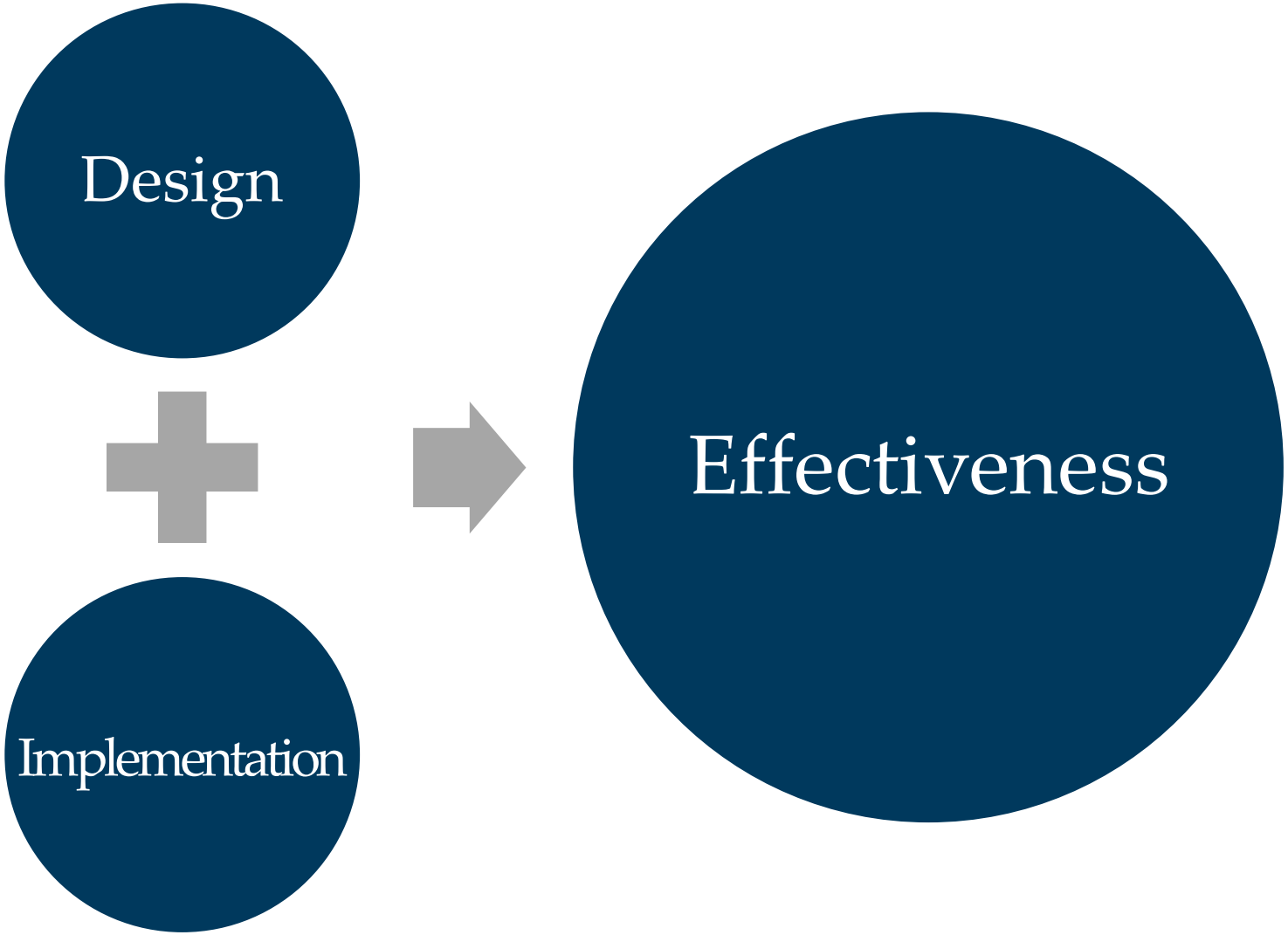
Look for Indicators

- Frequency of errors/events
- High level of rework
- Length of time it takes to find issue
- Repeated root cause
- Performance vs. others

Periodic Assessment

- Have the risks changed?
- Are the risks sufficiently mitigated?

Controls Assessment



Controls Assessment

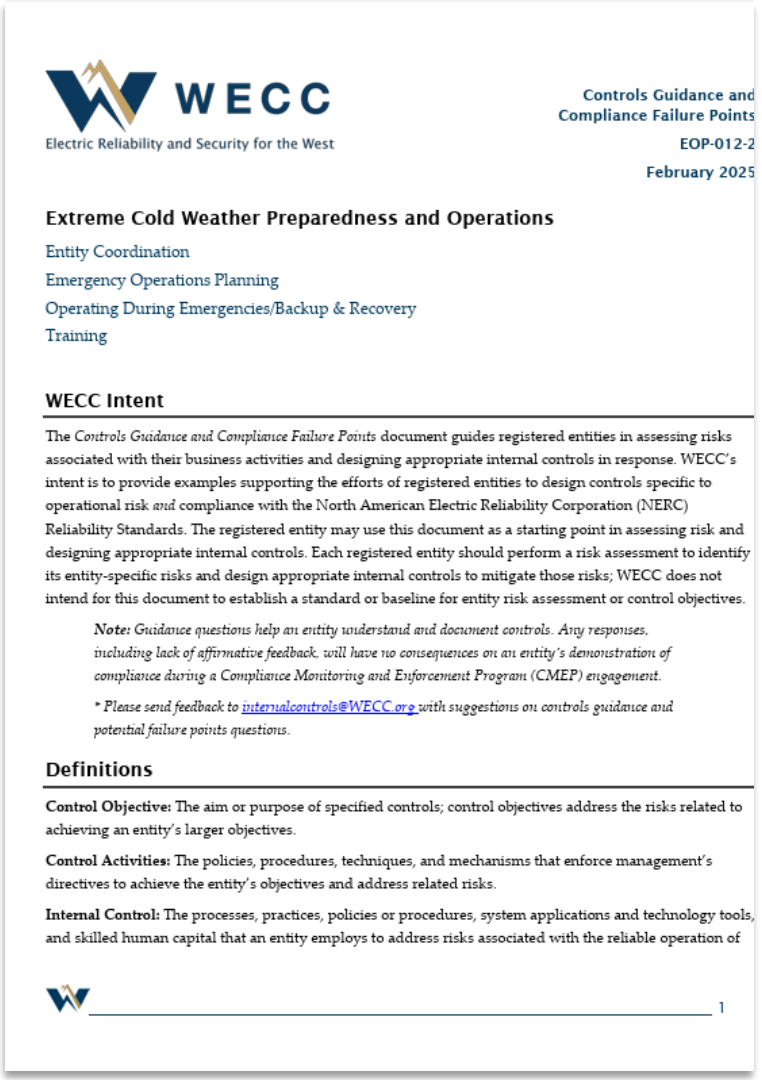
Design Assessment

- Is the control designed to mitigate the identified risk?
- Is it reliable?
- Does it allow for exceptions?
- Does it operate quickly enough?
- Does it address potential human performance issues?
- Is information flow and communication addressed?
- Is monitoring built in?

Controls Assessment Resources

Controls Guidance and Compliance Potential Failure Points

- https://www.wecc.org/program-areas/compliance/compliance-united-states >Internal Controls Guidance and Compliance Failure Points
- Currently 25 standards
- Example activities and questions



WECC
Electric Reliability and Security for the West

Controls Guidance and Compliance Failure Points
EOP-012-2
February 2025

Extreme Cold Weather Preparedness and Operations

Entity Coordination
Emergency Operations Planning
Operating During Emergencies/Backup & Recovery
Training

WECC Intent

The *Controls Guidance and Compliance Failure Points* document guides registered entities in assessing risks associated with their business activities and designing appropriate internal controls in response. WECC's intent is to provide examples supporting the efforts of registered entities to design controls specific to operational risk *and* compliance with the North American Electric Reliability Corporation (NERC) Reliability Standards. The registered entity may use this document as a starting point in assessing risk and designing appropriate internal controls. Each registered entity should perform a risk assessment to identify its entity-specific risks and design appropriate internal controls to mitigate those risks; WECC does not intend for this document to establish a standard or baseline for entity risk assessment or control objectives.

Note: *Guidance questions help an entity understand and document controls. Any responses, including lack of affirmative feedback, will have no consequences on an entity's demonstration of compliance during a Compliance Monitoring and Enforcement Program (CMEP) engagement.*

** Please send feedback to internalcontrols@WECC.org with suggestions on controls guidance and potential failure points questions.*

Definitions

Control Objective: The aim or purpose of specified controls; control objectives address the risks related to achieving an entity's larger objectives.

Control Activities: The policies, procedures, techniques, and mechanisms that enforce management's directives to achieve the entity's objectives and address related risks.

Internal Control: The processes, practices, policies or procedures, system applications and technology tools, and skilled human capital that an entity employs to address risks associated with the reliable operation of

1

Controls Assessment

Implementation Assessment

- Do you have evidence the control was performed?
  - SME interviews
  - Demonstrations
  - Examine documents and reports

Controls Assessment

Final Step: Remediate Deficiencies

- When controls do not effectively accomplish objectives, either change control design or improve implementation
- Develop Corrective Action Plan by issue type and document it, oversee its completion and re-evaluate control after completion

Program Maturity

Take One Step at a Time

Indicators of a Mature Program

- Executive support and culture of excellence
- Consistency across the organization
- Periodic Enterprise Risk Assessment
- Focus on improvement

<Public>

WECC

Electric Reliability and Security for the West

www.wecc.org