WECC

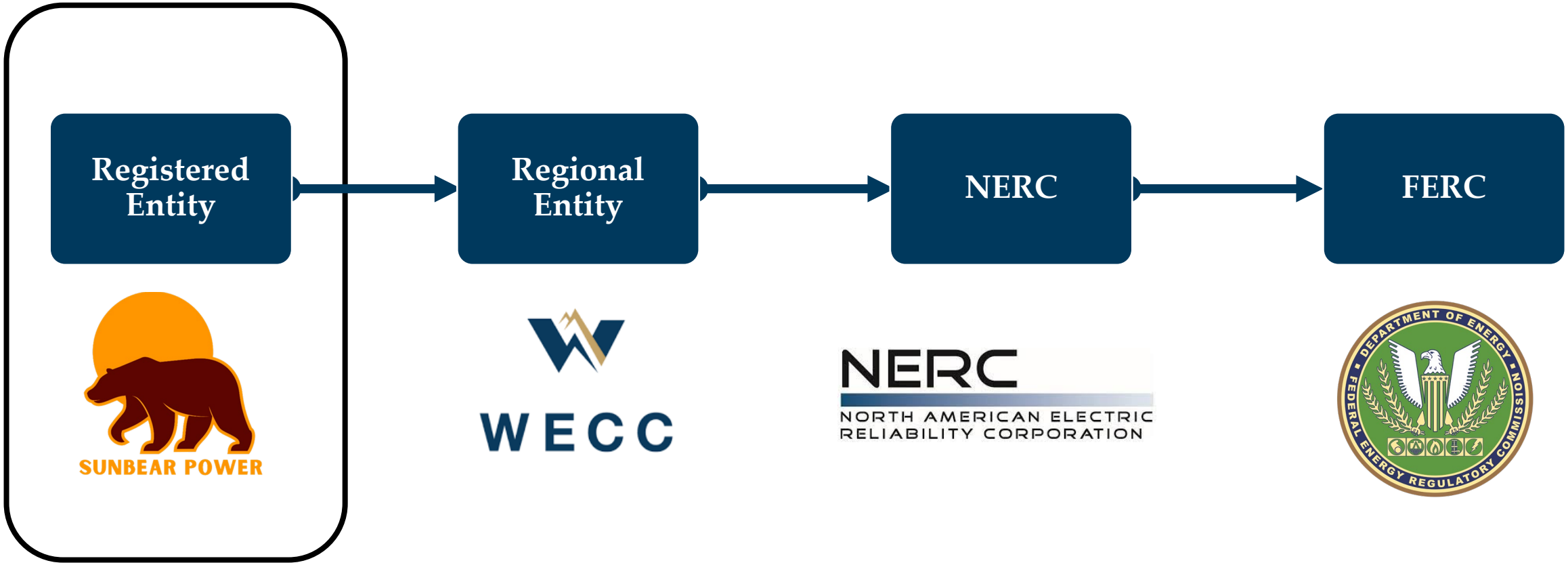
WECC Enforcement Fundamentals:

Noncompliance Reporting

March 25, 2024

WECC Enforcement Staff

Enforcement Handling



WECC Enforcement Training

Enforcement Background

- Introduction
- Enforcement Function
- Magnificent Seven
- Enforcement Processing
- Self-Logging Program

1

Noncompliance Reporting

- Building a Complete Story
- Description of Noncompliance
- Extent of Condition
- Duration
- Risk to BES
- Root Cause
- Mitigation
- Compliance History

2

Noncompliance Processing

- Enforcement Review
- Findings
- Preliminary Screen
- PNC Review
- Enforcement
- Disposition
- Closing Case

3

Practice & References

- Practice Cases
- Job Aids
- References

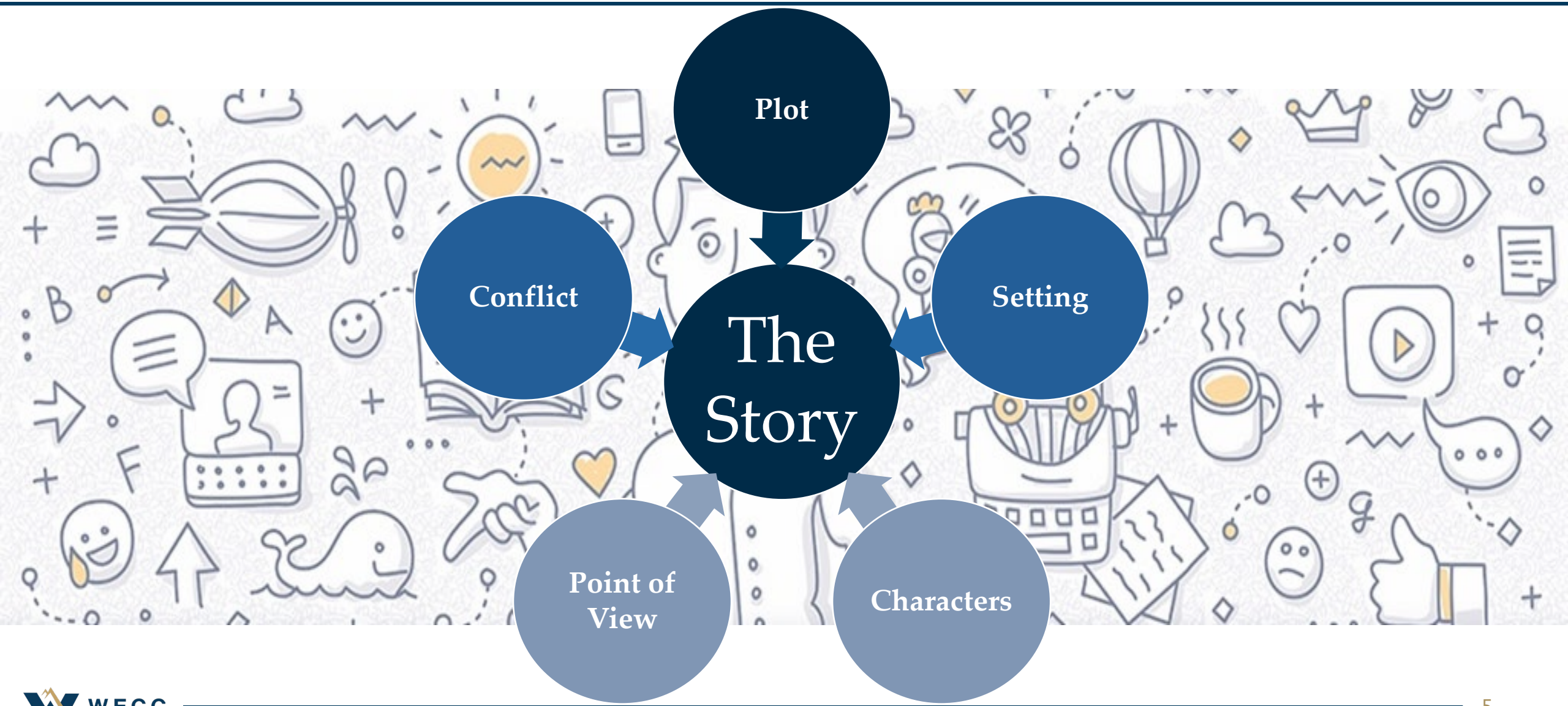
4

Building a Complete Story

"Stories create community, enable us to see through the eyes of other people, and open us to the claims of others."

– Peter Forbes

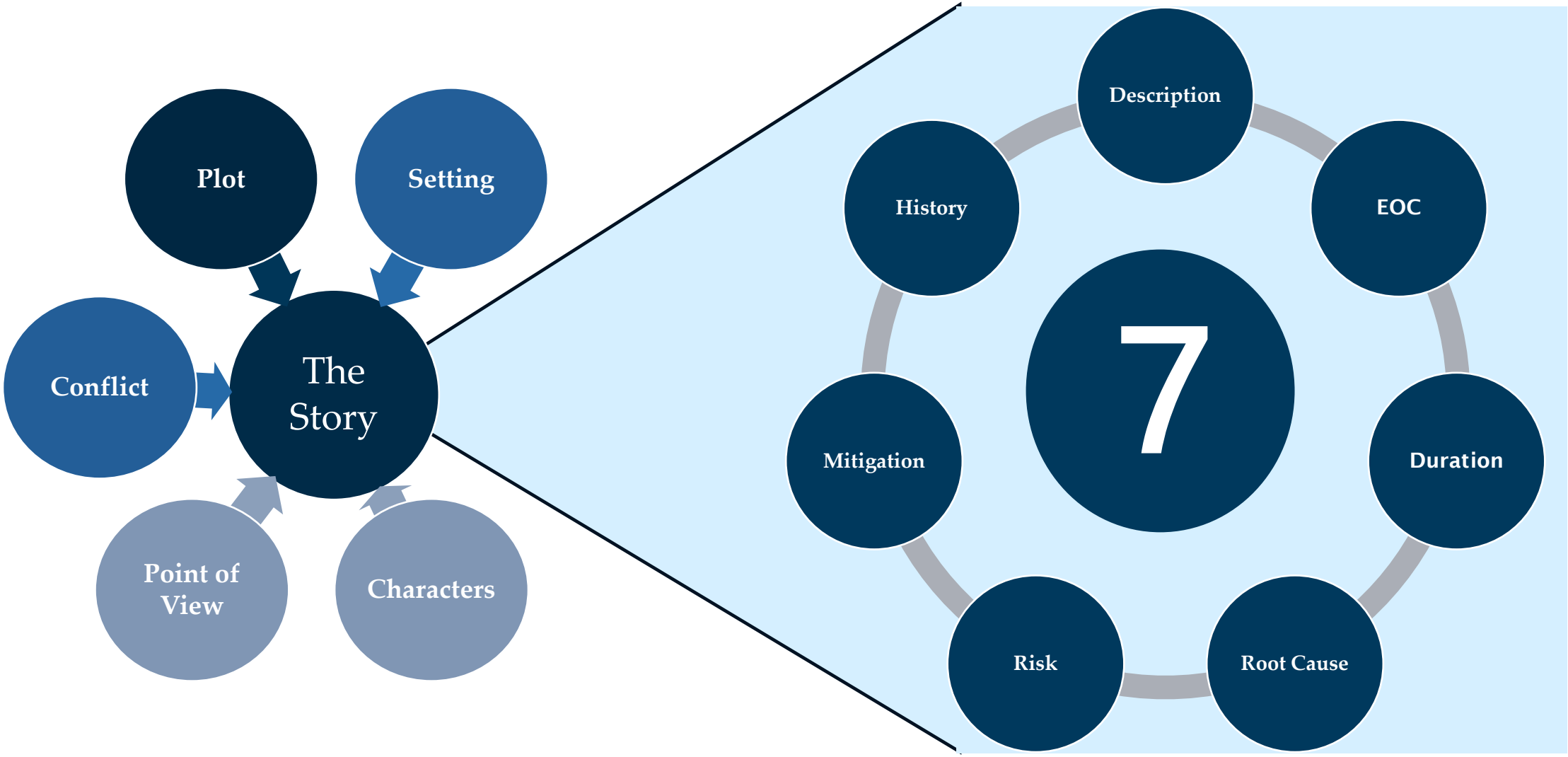
What goes into the story?



<Public>

Magnificent Seven

Traditional Story Telling



Registered Entity: Sunbear Power

SUNBEAR POWER

CIP Standards	O&P Standards
CIP-004	FAC-003
CIP-007	VAR-002

Description of Noncompliance	Extent of Condition	Duration	Risk Analysis	Root Cause	Mitigation	Compliance History

The story, registered entity, and violations portrayed in this production are fictitious. No identification with actual registered entities or reported noncompliance is intended or should be inferred.

WECC

Electric Reliability and Security for the West

www.wecc.org

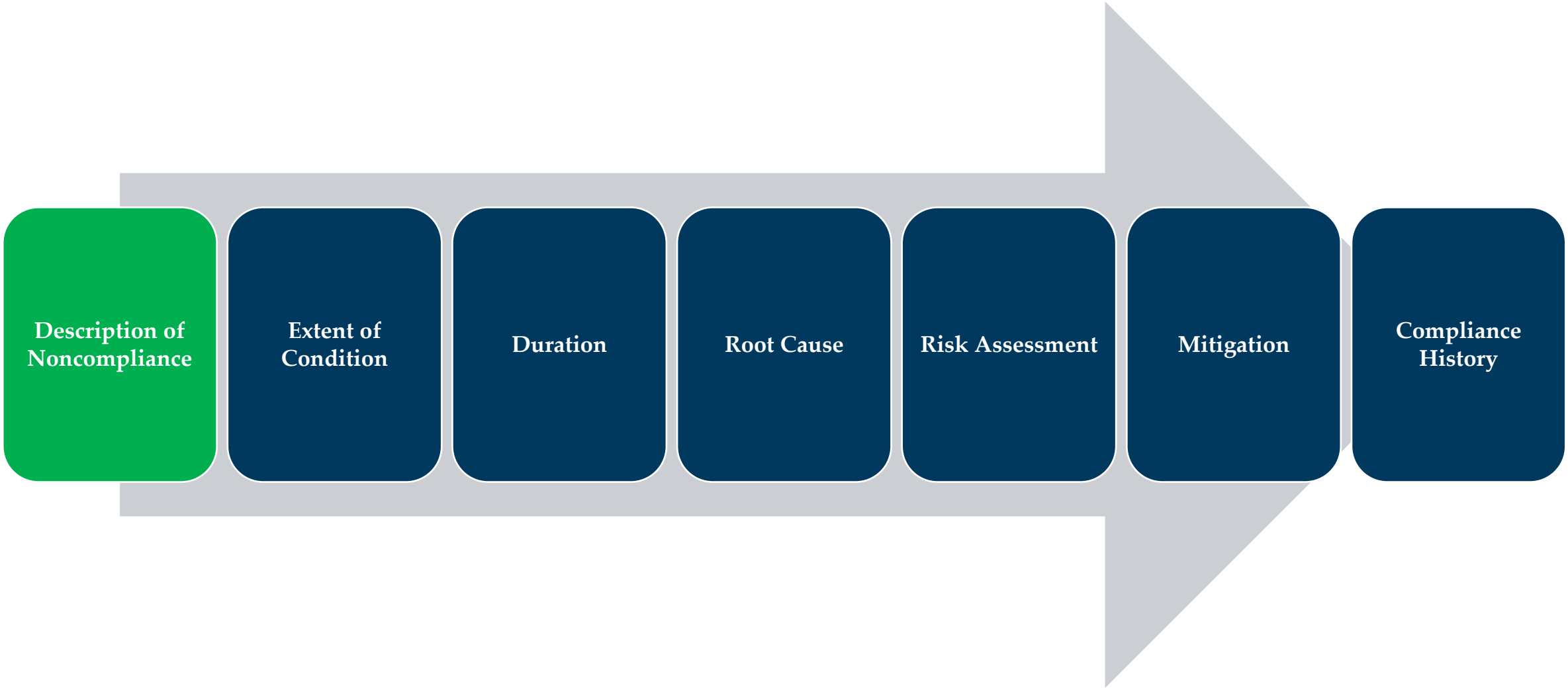
WECC

WECC Enforcement Training:

2.1 Description of Noncompliance

WECC Enforcement Staff

2.1 Description of Noncompliance



Section Learning Plan

1

Conceptual Foundation

- Application of concept to non-NERC situations

2

Teaching Exercises

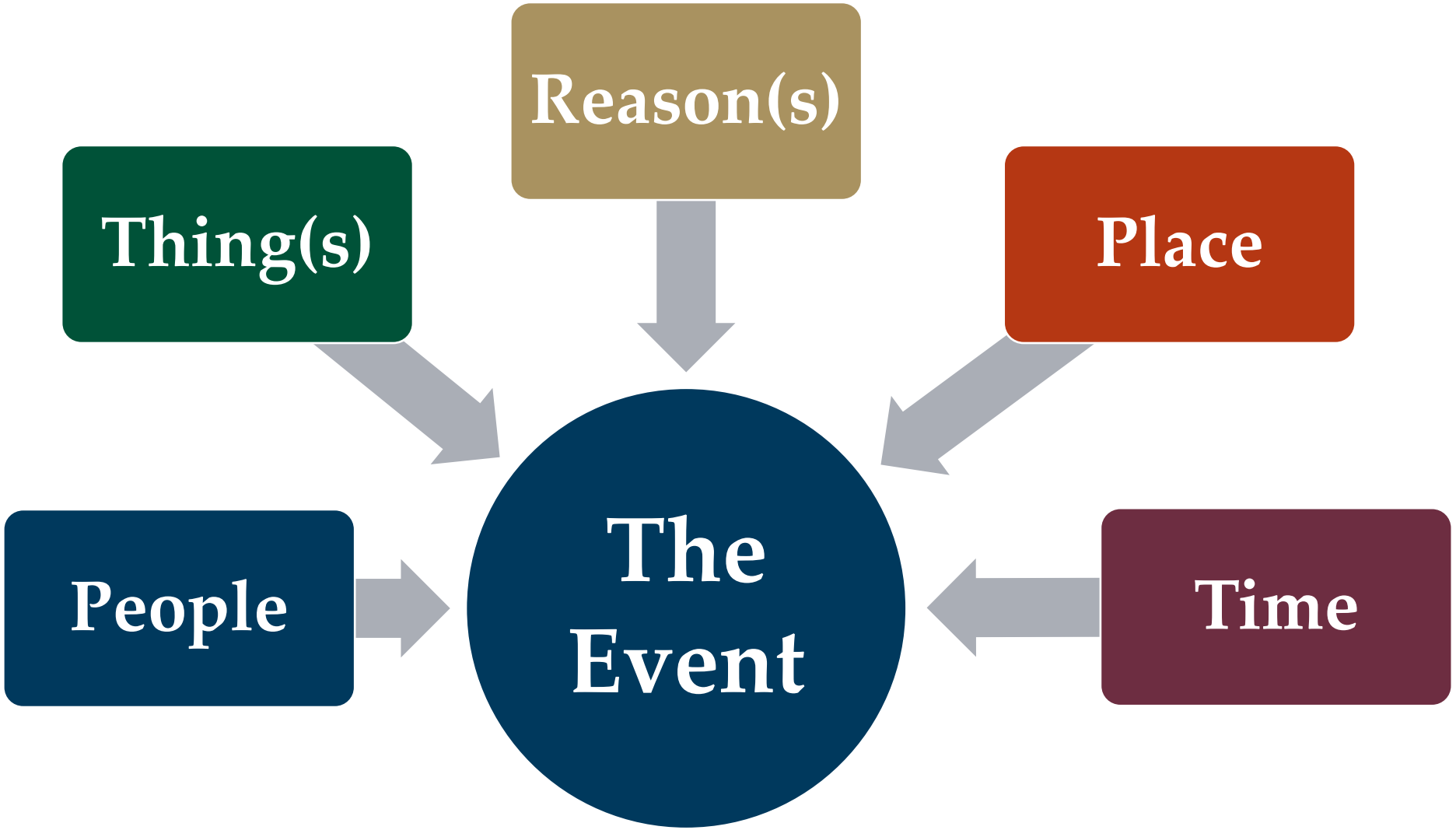
- Present incomplete examples and then demonstrate how to complete them
- FAC-003-4 & CIP-004-6

3

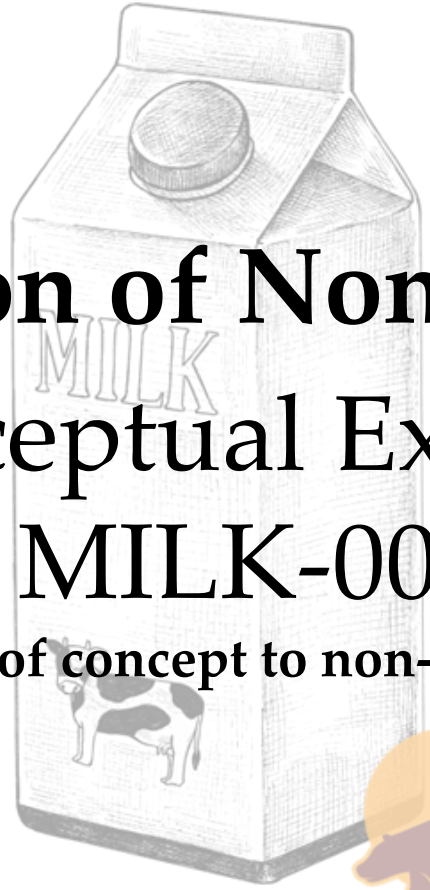
Peer Review Exercises

- Review noncompliance descriptions and participants identify deficiencies
- VAR-002-4.1 & CIP-007-6

Description of Noncompliance



Section 2.1—Concept Example



Description of Noncompliance

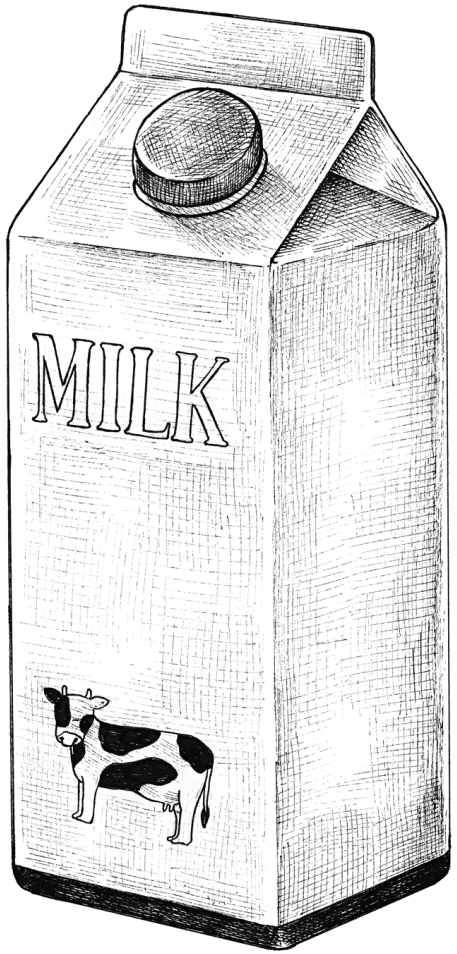
Conceptual Example

MILK-001

Application of concept to non-NERC situation

SUNBEAR POWER

2.1 Description of Noncompliance



Food Standard:

SNBR-MILK-001

Pasteurized Milk must be discarded on or before the expiration date listed on each carton.

2.1 Description of Noncompliance

- An employee recently discovered milk in the Sunbear break room that did not have the color, consistency, or smell of fresh milk. Upon further investigation, the employee determined the milk was three days past the printed food safety date.
- After determining the milk had spoiled, the employee threw out the remainder of that milk container as well as the second container in the fridge with the same food safety date.
- The employee then submitted an internal compliance report, attached a video of the spoiled milk as it was being poured out, and a provided a picture of the food safety date.

2.1 Description of Noncompliance

Original Description

Sunbear violated SNBR-MILK-001 because it found two gallons of milk not discarded prior to the food safety date.

2.1 Description of Noncompliance

SUNBEAR POWER

How much milk was discarded?

Thing(s)

Size and type of milk container?

Reason(s)

Who purchased the milk?
What was it for?

Place

Where did this happen?

People

How many people in the office?

The Event

Time

When did this happen?

2.1 Description of Noncompliance

Improved Description

While preparing coffee on Monday, July 21, 2023, an employee noticed the texture of their milk didn't look right and determined, based on the milk's color, consistency, and smell, that the milk had gone bad. The employee threw the container of bad milk and a second container of milk from the same fridge with the same food safety date into the trash. There are two refrigerators on site, so employees used milk from the cafeteria, where the milk had not spoiled, for their coffee until new milk could be brought into the small break room.

2.1 Description of Noncompliance

Description of Noncompliance

Teaching Exercise One

FAC-003-4 R2

Present incomplete examples and then demonstrate how to complete them

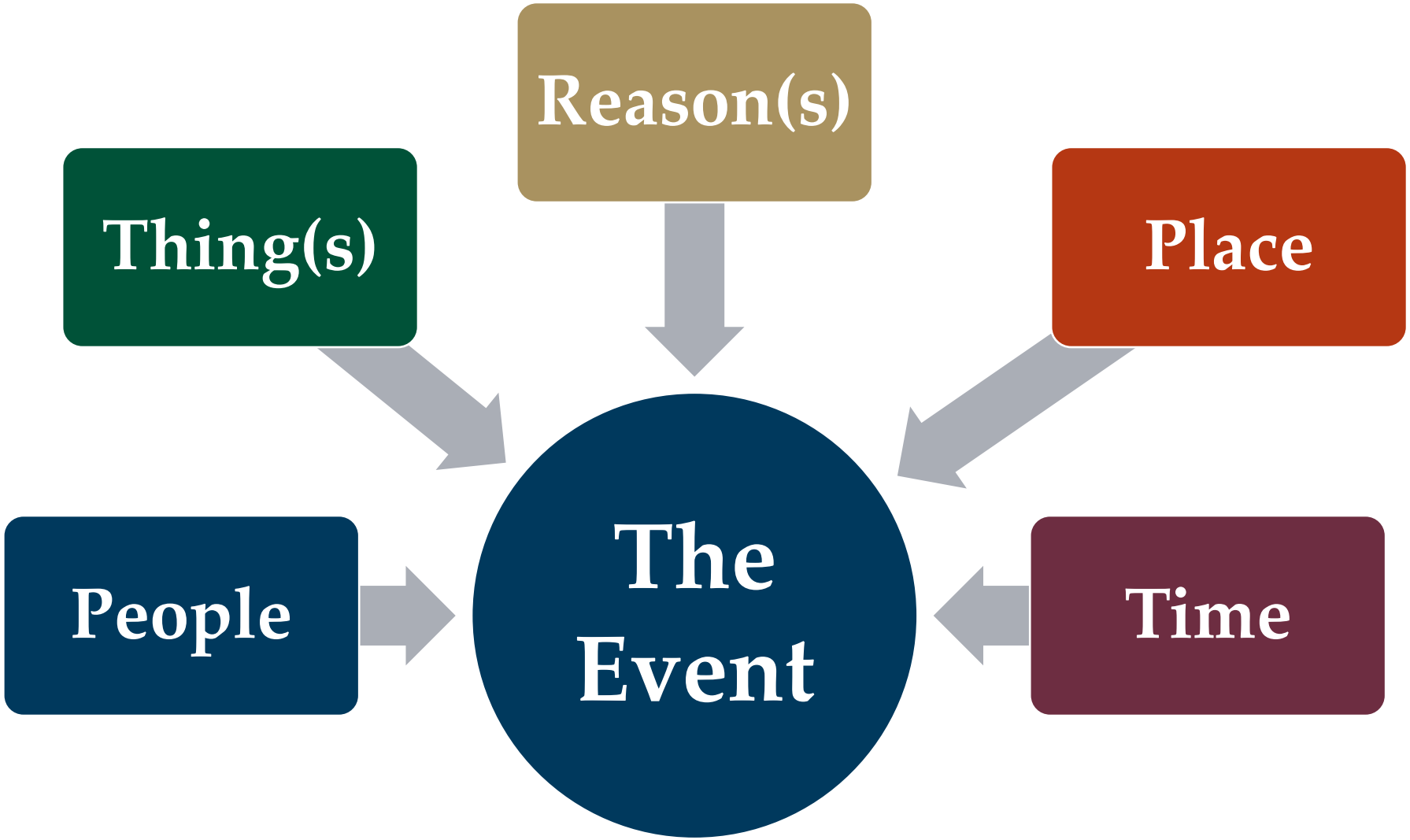
Fact Pattern

On July 20, 2017, Sunbear's line supervisor reported a line trip without a sustained outage due to a poplar tree catching fire. She thinks it could be FAC-003 R2 violation and recommends you investigate. She has sent crews to clear the tree, search for any other issues, and report back.

Example 1—FAC-003-4 R2.1

- Purpose: To maintain a reliable electric transmission system by using a defense in-depth strategy to manage vegetation located on transmission rights of way (ROW) and minimize encroachments from vegetation located adjacent to the ROW, thus preventing the risk of those vegetation-related outages that could lead to Cascading
- R2: Each applicable Transmission Owner and applicable Generator Owner shall manage vegetation to prevent encroachments into the MVCD (Minimum Vegetation Clearance Distance) of its applicable line(s) which are not either an element of an IROL, or an element of a Major WECC Transfer Path; operating within its Rating and all Rated Electrical Operating Conditions of the types shown below [Violation Risk Factor: High] [Time Horizon: Real-time]:
  - 2.1 An encroachment into the MVCD, observed in Real-time, absent a Sustained Outage

2.1 Conceptual Foundations

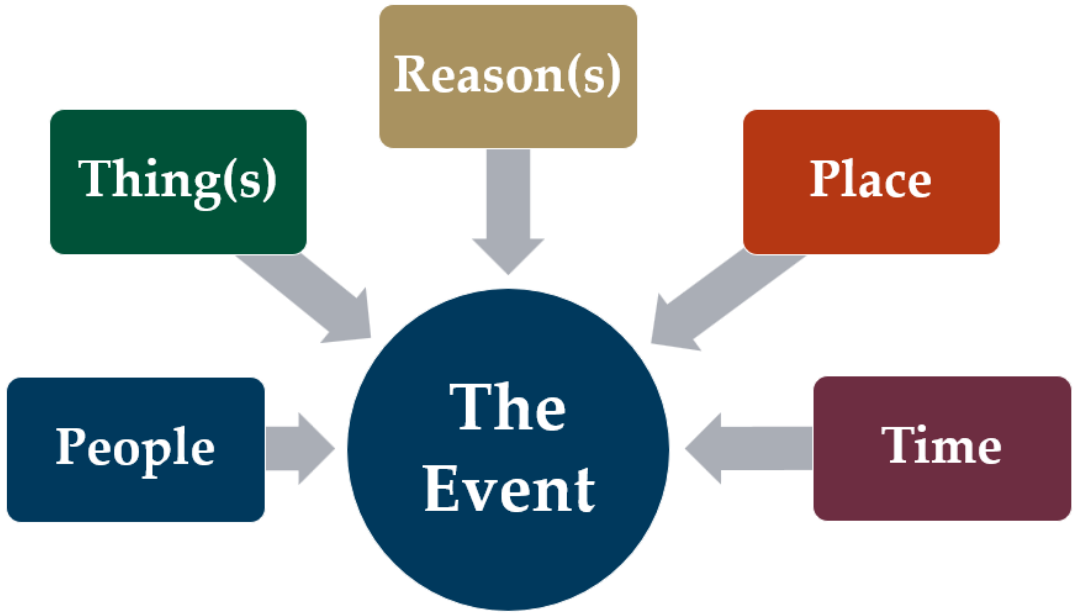


2.1 Conceptual Foundations

Original description of noncompliance

- On July 20, 2017, at 2:20 p.m., Sunbear noted that there was a phase-to-ground fault that occurred on its 230 kV Point A to Point B line.
- Prior to the supervisor being able to see the location of the fault, the ground crew needed to clear a path due to the surrounding undergrowth.
- It was determined that Sunbear, as a Transmission Owner, was in violation of FAC-003-4 R2 for having an encroachment due to vegetation growth into the line MVCD. After investigating the site, the supervisor ordered vegetation removal to take down the tree and ordered a review of all vegetation management records for the line.
- The poplar tree was entirely removed from the 230 kV Point A to Point B line easement on July 22, 2017.

2.1 Description of Noncompliance



- What has been confirmed at the time of the report?
- Describe the noncompliance with the most details possible.
- What else do we need to know to understand?
- Circumstances?
- How was it discovered? (Detective controls? Mock audit? Routine inspection? Event?)
- Roll of person that discovered the problem?
- Scope?
- What is known to be affected by this discovery/event at this time?

2.1 Conceptual Foundations

Improved description of noncompliance

- On July 20, 2017, at 2:20 p.m., Sunbear noted that there was a phase-to-ground fault that occurred on its 230 kV Point A to Point B line. The line tripped and reclosed as designed, avoiding a Sustained Outage. A transmission line supervisor was dispatched to investigate the issue.
- Prior to the supervisor being able to see the location of the fault, the ground crew needed to clear a path due to the surrounding undergrowth. When the transmission line supervisor arrived at the site, it was noted that there was some evidence of burning on a poplar tree located near the line.
- It was determined that Sunbear, as a Transmission Owner, was in violation of FAC-003-4 R2 for having an encroachment due to vegetation growth into the line MVCD. After investigating the site, the supervisor ordered vegetation removal to take down the tree and ordered a review of all vegetation management records for the line.
- The poplar tree was entirely removed from the 230 kV Point A to Point B line easement on July 22, 2017.

2.1 Description of Noncompliance

Description of Noncompliance

Teaching Exercise Two

CIP-004-6 R4

Present incomplete example and then demonstrate how to complete it.

Fact Pattern

On December 12, 2023, Sunbear discovered that it failed to document its business justification for multiple employees and contractors, some of which had electronic access to Sunbear's High Impact BES Cyber System (HIBCS) associated with its Control Center, and others who had unescorted physical access into the Physical Security Perimeter (PSP) associated with the same HIBCS.

Example 2—CIP-004-6 R4.1

- Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.
- R4: Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4—Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations]

Example 2—CIP-004-6 R4.1

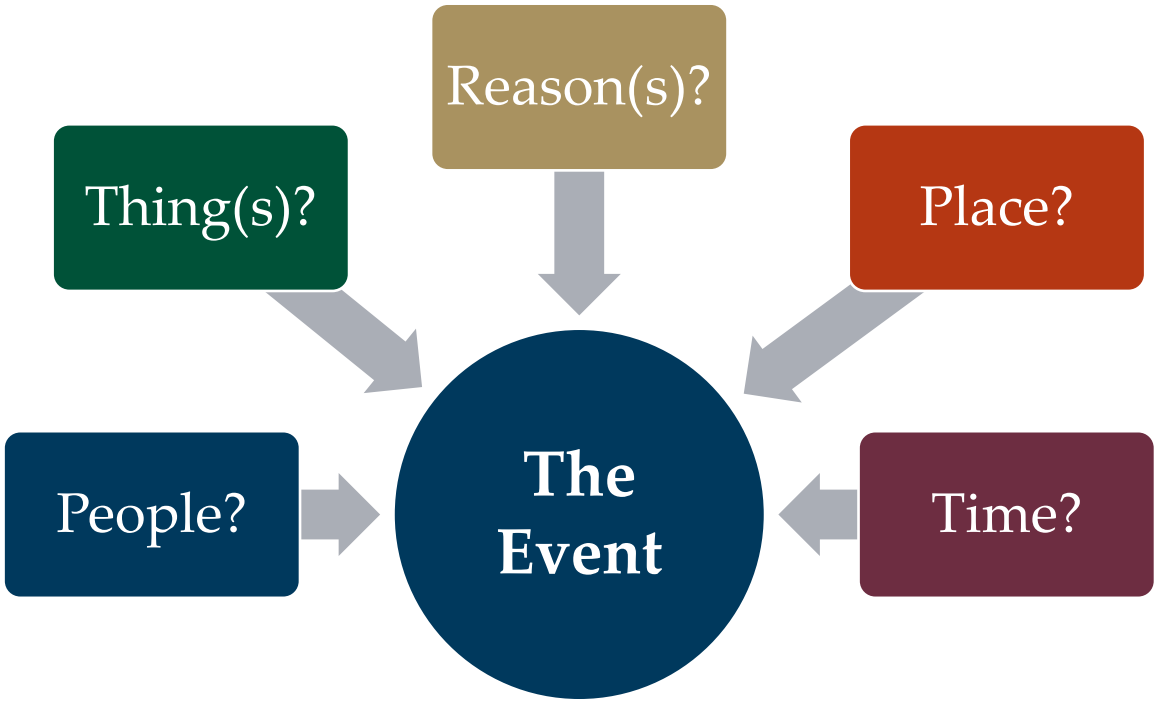
CIP-004-6 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

2.1 Description of Noncompliance

Original description of noncompliance

- Sunbear discovered on December 12, 2023, during a self-certification, that it failed to document business justifications for employees and contractors with electronic and unescorted physical access into a PSP for an HIBCS associated with its Control Center, which is required by CIP-004-6 R4 (P4.1.1 and P4.1.2). Sunbear's Control Center had 25 BES Cyber Assets (BCA), 12 Electronic Access Control or Monitoring Systems (EACMS), three Physical Access Controls Systems (PACS), and 10 Protected Cyber Assets (PCA).
- The noncompliance started on November 15, 2016, when the first unescorted physical access to a PSP was granted without a documented business justification, and ended on January 4, 2024.
- Sunbear's access control policy included its process for authorizing access for employees and contractors, which required a documented business justification and must be based on need. The process for authorizing access must be complete before electronic, unescorted physical access into a PSP, and electronic or physical BCSI access is granted. However, the workflow-managed system did not make business justification a required field and did not have other controls in place to ensure that all requests for access have a business justification.

2.1 Description of Noncompliance



- What has been confirmed at the time of the report?
- Describe the noncompliance with the most details possible.
- What else do we need to know to understand?
- Circumstances?
- How was it discovered? (Detective controls? Mock audit? Routine inspection? Event?)
- Roll of person that discovered the problem?
- Scope?
- What is known to be affected by this discovery/event at this time?

2.1 Description of Noncompliance

Improved description of noncompliance

- Sunbear discovered on December 12, 2023, during a self-certification, that it failed to document business justifications for employees and contractors with electronic and unescorted physical access into a PSP HIBCS associated with its Control Center, which is required by CIP-004-6 R4 (P4.1.1 and P4.1.2). Sunbear's Control Center had 25 BES Cyber Assets (BCA), 12 Electronic Access Control or Monitoring Systems (EACMS), three Physical Access Controls Systems (PACS), and 10 Protected Cyber Assets (PCA).
- The noncompliance started on November 15, 2016, when the first unescorted physical access to a PSP was granted without a documented business justification, and ended on January 4, 2024, when all 12 records granting access without a documented business justification were corrected to include a business justification. The other 11 instances where Sunbear granted users access without a documented business justification occurred between after November 15, 2016, and before April 4, 2023. Please see the attached spreadsheet for the specific dates, type of user, and access type for all 12 instances of noncompliance.
- Sunbear's access control policy included its process for authorizing access for employees and contractors, which required a documented business justification and must be based on need. The process for authorizing access must be complete before electronic, unescorted physical access into a PSP, and electronic or physical BCSI access is granted. However, the workflow-managed system did not make business justification a required field and did not have other controls in place to ensure that all requests for access have a business justification.

2.1 Description of Noncompliance

Description of Noncompliance

Peer Review Exercise Three

VAR-002-4.1 R3

Review a noncompliance description and participants identify deficiencies.

Fact Pattern

On February 20, 2023, the automatic voltage regulator (AVR) at one of Sunbear's generating stations unexpectedly went to manual mode from automatic mode. Sunbear failed to notify its Transmission Operator within 30 minutes of the change in AVR status as required by VAR-002-4.1 R3.

Example 3—VAR-002-4.1 R3

- Purpose: To ensure generators provide reactive support and voltage control, within generating Facility capabilities, to protect equipment and maintain reliable operation of the Interconnection.
- R3: Each Generator Operator shall notify its associated Transmission Operator of a status change on the AVR, power system stabilizer, or alternative voltage controlling device within 30 minutes of the change. If the status has been restored within 30 minutes of such change, then the Generator Operator is not required to notify the Transmission Operator of the status change. [Violation Risk Factor: Medium] [Time Horizon: Real-time Operations

2.1 Description of Noncompliance—Example 3

Original description of noncompliance

- On February 20, 2023, at 3:35 p.m., Unit 3, a 200-MW generator at the Sunbear Power Plant, received an alarm that its AVR unexpectedly shifted from automatic to manual due to an equipment malfunction within the AVR. The alarm went unnoticed by the day shift operator, who was conducting other operations. The day shift was one person short due to a sudden illness. The day shift operator did not review the alarms and indications on his screen for over 40 minutes. The night shift operator notified the Transmission Operator of the change in AVR status at 5:01 p.m.
- The night shift operator was unable to return the AVR to automatic, and plant technicians were called out to address the issue.

2.1 Description of Noncompliance

People

1. Who discovered it?
2. What staff members were involved?

Thing(s)

3. How did Sunbear resolve the AVR issue?

Reason(s)

4. Why was the AVR unable to be restored to automatic?

2.1 Description of Noncompliance

Place

Time

5. What was the timeline?
   - Date and time AVR was restored to auto,
   - Date and time the status change was noticed,
   - Any other dates and times that help tell the complete story of what happened.

2.1 Description of Noncompliance—Example 3

Improved description of noncompliance

- On February 20, 2023, at 3:35 p.m., Unit 3, a 200-MW generator at the Sunbear Power Plant, received an alarm that its AVR unexpectedly shifted from automatic to manual due to an equipment malfunction within the AVR. The alarm went unnoticed by the day shift operator, who was conducting other operations. The day shift was one person short due to a sudden illness. The day shift operator did not review the alarms and indications on his screen for over 40 minutes. The night shift operator noticed the alarm during shift change and acknowledged the alarm at 5:00 p.m. and notified the Transmission Operator of the change in AVR status at 5:01 p.m.
- The night shift operator was unable to return the AVR to automatic, and plant technicians were called out to address the issue.
- The generating unit remained online controlling voltage manually while the AVR controller was being repaired. The following morning on February 21, 2023, at 9:25 a.m., the AVR controller was repaired and placed back in automatic. At 9:30 a.m., the Sunbear day shift operator notified the Transmission Operator that the Unit 3 AVR was repaired and controlling voltage in automatic.

2.1 Description of Noncompliance—Example 3

Time?

Improved description of noncompliance

- On February 20, 2023, at 3:35 p.m., Unit 3, a 200-MW generator at the Sunbear Power Plant, received an alarm that its AVR unexpectedly shifted from automatic to manual due to an equipment malfunction within the AVR. The alarm went unnoticed by the day shift operator, who was conducting other operations. The day shift was one person short due to a sudden illness. The day shift operator did not review the alarms and indications on his screen for over 40 minutes. The night shift operator noticed the alarm during shift change, acknowledged the alarm at 5:00 p.m., and notified the Transmission Operator of the change in AVR status at 5:01 p.m.
- The night shift operator was unable to return the AVR to automatic, and plant technicians were called out to address the issue.
- The generating unit remained online controlling voltage manually while the AVR controller was being repaired. The following morning on February 21, 2023, at 9:25 a.m., the AVR controller was repaired and placed back in automatic. At 9:30 a.m., the Sunbear day shift operator notified the Transmission Operator that the Unit 3 AVR was repaired and controlling voltage in automatic.

Section 2.1—Example 4

Description of Noncompliance

Peer Review Exercise Four

CIP-007-6 R2

Review a noncompliance description and determine deficiencies.

Fact Pattern

In February 2023, Sunbear evaluated patches for BES Cyber Assets associated with its primary control center. Sunbear failed to install the patches it evaluated as required by CIP-007-6 R2 (P2.3).

Example 4—CIP-007-6 R2.3

- Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
- R2: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R2—Security Patch Management. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].

Example 4—CIP-007-6 R2.3

CIP-007-6 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

Example 4—CIP-007-6 R2 (P2.3)

- For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, do one of the following:
  - Apply the applicable patches;
  - Create a dated mitigation plan; or
  - Revise an existing mitigation plan.
- Mitigation plans must include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a time frame to complete these mitigations.

Example 4—CIP-007-6 R2 (P2.3)

- **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
- **R2:** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R2—Security Patch Management.

Section 2.1 Example 4

Original description of noncompliance

- Sunbear did not apply one security patch within 35 calendar days of the completion of the patch assessment. This noncompliance was discovered on September 15, 2023, when Sunbear was completing an internal review, which is done biannually by SMEs and managers of the patching team. This is a detective control.
- The security patch evaluation was completed on February 2, 2023, but the patches were not installed by March 7, 2023, because Sunbear's vulnerability assessment tool, which automatically applies the patches, has been intermittently up and down starting on January 6, 2023. It was down on March 1, 2023, when the patches were scheduled to be installed.
- Also, the technician responsible for applying the patches did not know that he was supposed to confirm all patches and populate the necessary security patch mitigation documentation records manually each month when the vulnerability assessment tool is down, because Sunbear's process did not include this procedural control.

2.1 Description of Noncompliance

People

1. Who took steps to resolve the noncompliance?

Thing(s)

2. How many Cyber Assets were involved in this instance?
3. What types of Cyber Assets are associated with this instance?
4. What are the functions of the Cyber Assets impacted?

Reason(s)

2.1 Description of Noncompliance

Place

5. Which facilities were involved in this instance and what Cyber Assets were associated with each facility?
6. Did the instance include Control Centers/Data Centers?
7. What was the impact level of the BES Cyber System(s) affected?

Time

8. What is the end date?
9. How was the end date determined?

Section 2.1 Example 4

Improved description of noncompliance

- Sunbear did not apply one security patch within 35 calendar days of the completion of the patch assessment for 25 BCAs. All 25 BES Cyber Assets were associated with the EMS, SCADA servers, and ICCP servers within the Primary Control Center (PCC) and associated Data Center (10 at the PCC and 15 at the Data Center). The PCC has a High Impact Rating. This noncompliance was discovered on September 15, 2023, when Sunbear was completing an internal review, which is done biannually by SMEs and managers of the patching team. This is a detective control.
- The security patch evaluation was completed on February 2, 2023, but the patches were not installed by March 7, 2023, because Sunbear's vulnerability assessment tool, which automatically applies the patches, has been intermittently up and down starting on January 6, 2023. It was down on March 1, 2023, when the patches were scheduled to be installed.
- Also, the technician responsible for applying the patches did not know that he was supposed to confirm all patches and populate the necessary security patch mitigation documentation records manually each month when the vulnerability assessment tool is down, because Sunbear's process did not include this procedural control. Sunbear SMEs applied the security patches on September 20, 2023.

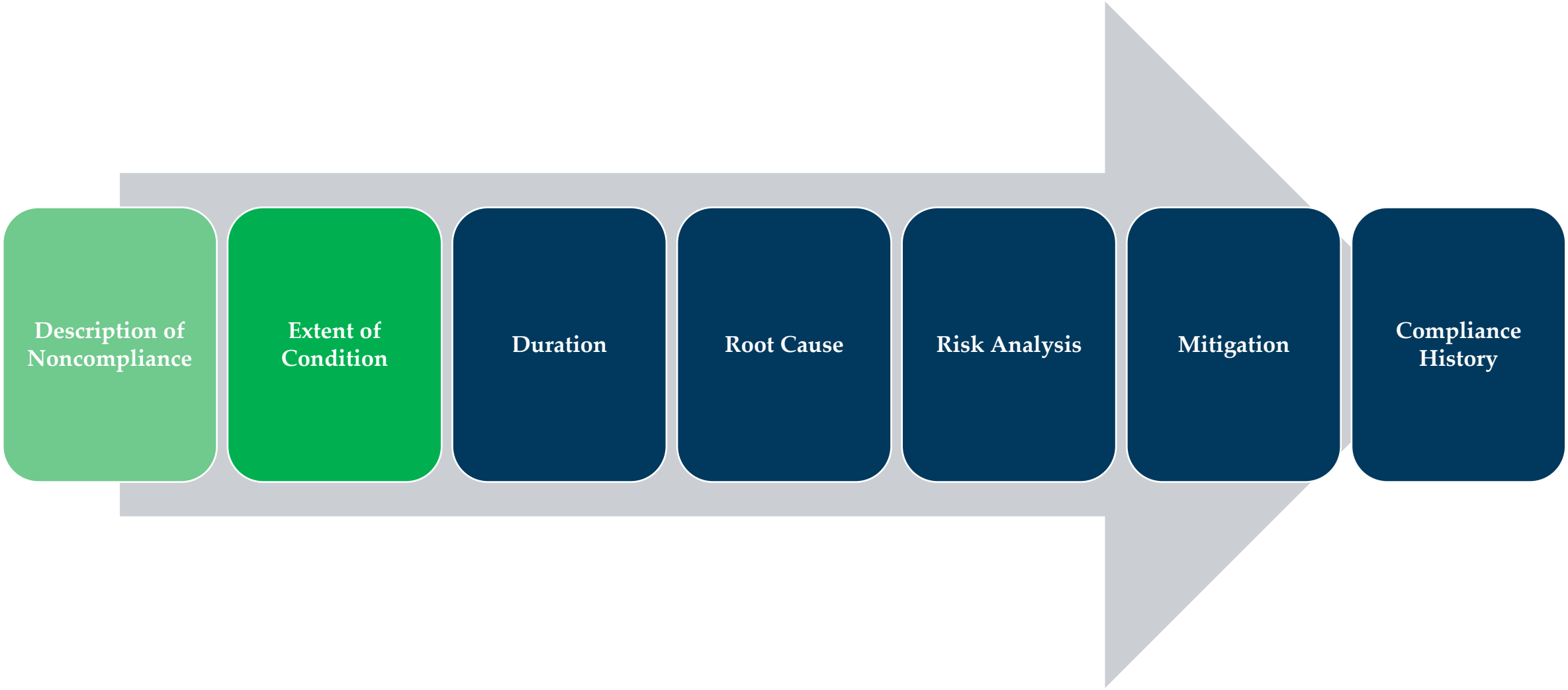
Section 2.1 Example 4

Time?

Improved description of noncompliance

- Sunbear did not apply one security patch within 35 calendar days of the completion of the patch assessment for 25 BCAs. All 25 BES Cyber Assets were associated with the EMS, SCADA servers, and ICCP servers within the Primary Control Center (PCC) and associated Data Center (10 at the PCC and 15 at the Data Center). The PCC has a High Impact Rating. This noncompliance was discovered on September 15, 2023, when Sunbear was completing an internal review, which is done biannually by SMEs and managers of the patching team. This is a detective control.
- The security patch evaluation was completed on February 2, 2023, but the patches were not installed by March 7, 2023, because Sunbear's vulnerability assessment tool, which automatically applies the patches, has been intermittently up and down starting on January 6, 2023. It was down on March 1, 2023, when the patches were scheduled to be installed.
- Also, the technician responsible for applying the patches did not know that he was supposed to confirm all patches and populate the necessary security patch mitigation documentation records manually each month when the vulnerability assessment tool is down, because Sunbear's process did not include this procedural control. Sunbear SMEs applied the security patches on September 20, 2023.

2.1 Description of Noncompliance



<Public>

WECC

Electric Reliability and Security for the West

www.wecc.org

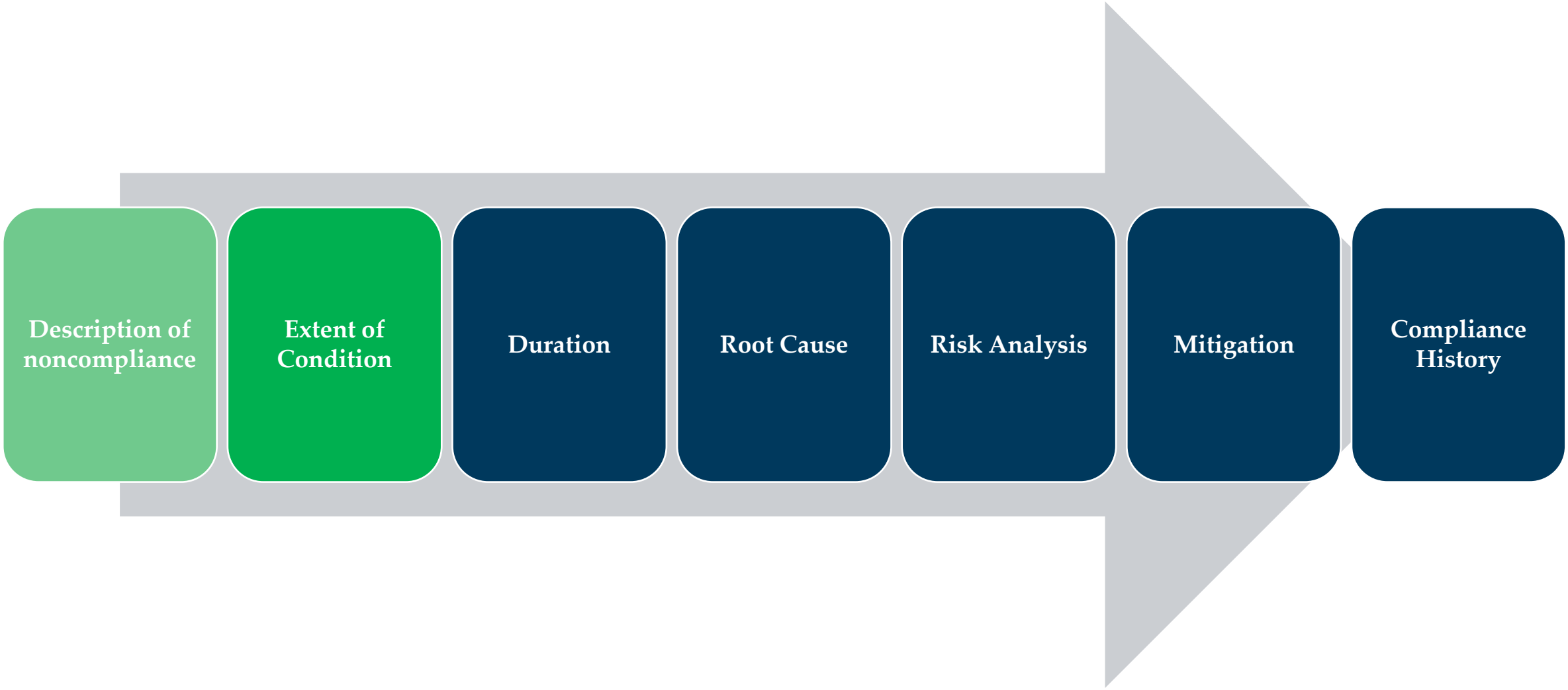
WECC

WECC Enforcement Fundamentals:

2.2 Extent of Condition Review

WECC Enforcement Staff

2.2 Extent of Condition Review



Section Learning Plan

1

Conceptual Foundation

- Application of concept to non-NERC situations

2

Teaching Exercises

- Present incomplete examples and then demonstrate how to complete them
- FAC-003-4 & CIP-004-6

3

Peer Review Exercises

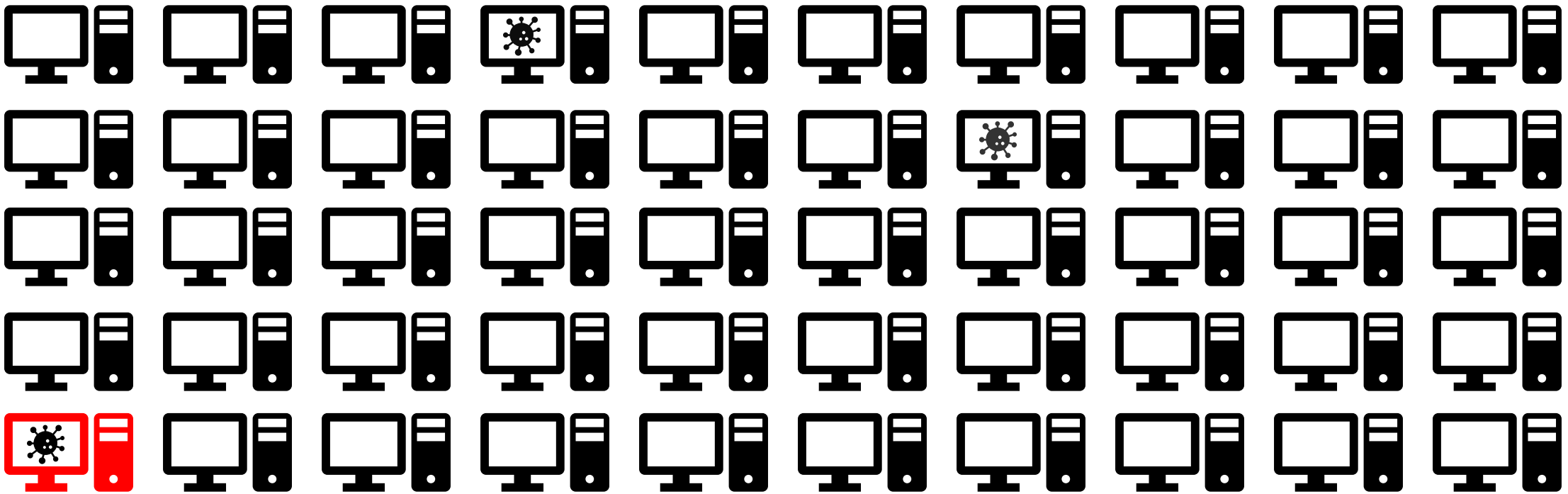
- Review noncompliance descriptions, and participants identify deficiencies
- VAR-002-4.1 & CIP-007-6

Conceptual Foundations

Extent-of-Condition Review: Strawberry Container

- If a strawberry at the top of the container has mold, how likely are you to find mold on other strawberries?
- What about the second of the two boxes you purchased?
- What about the ones you stored in the freezer?
- Going through the box to find which others have mold is performing an extent-of-condition (EOC) analysis.

Conceptual Foundations: EOC



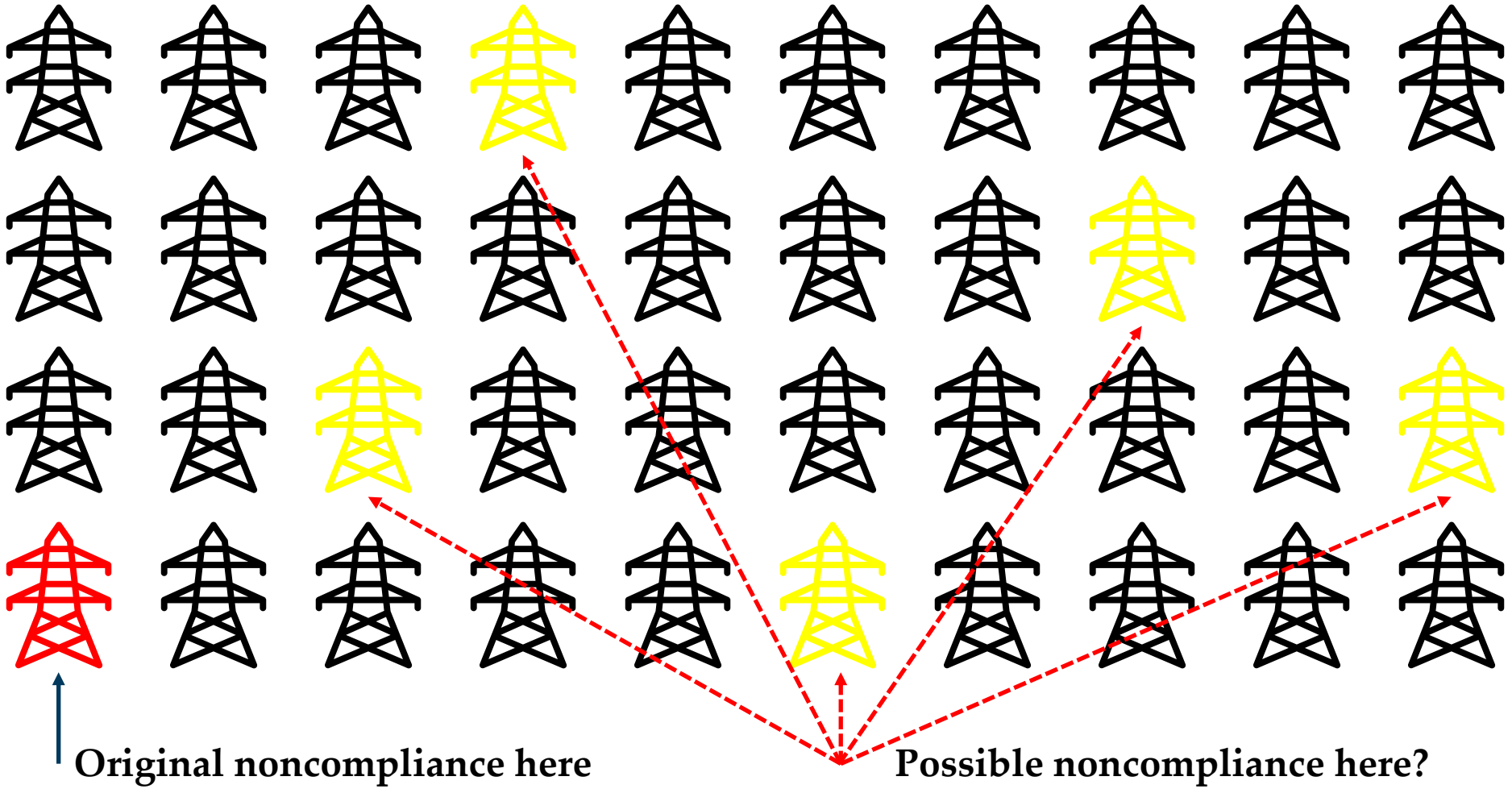
Original noncompliance here. Where else is noncompliance?

Conceptual Foundations

NERC Self-Report & Mitigation Guide

"The purpose of performing an extent-of-condition analysis is to provide **reasonable assurance that the registered entity has identified all effects from a noncompliance** so that its remediation efforts are comprehensive, thereby lessoning the risk of potential harm to the BPS."

Conceptual Foundations: EOC



Conceptual Foundations

An effective EOC assessment helps to:

- Identify all related noncompliance across the enterprise
- Identify trends, weaknesses, and strengths
  - Most effective programs use predetermined established communications plans to let everyone know how to share and document data
- Confirm the cause and inform mitigation efforts
- Ensure complete mitigation and prevent recurrence
- Identify corrective actions and internal controls

NERC Self-Report & Mitigation Guide

The CEA and NERC should be able to understand how the registered entity determined that the level of EOC assessment was appropriate, since the scope of the assessment may differ based on the facts of the noncompliance.

Conceptual Foundations

Importance to WECC

For example, if the noncompliance centers on a specific type of relay, the EOC assessment may involve all facilities that include the specified relay.

Another example: a checklist used to meet compliance was determined to be outdated. All facilities, people, and/or devices associated with that checklist may be noncompliant.

NERC Self-Report & Mitigation Guide

The CEA and NERC should be able to understand how the registered entity determined that the level of EOC assessment was appropriate, since the scope of the assessment may differ based on the facts of the noncompliance.

Conceptual Foundations

FACT

- ✓ An EOC assessment should be conducted after the immediate noncompliance has been managed.
- ✓ DO NOT HOLD the Self-Report (more than 90 days) when the EOC assessment is underway.
- ✓ If an EOC assessment has not been completed when a Self-Report is submitted, document a mitigating activity for an EOC with the planned completion by "x" date.
- ✓ Depending on where it is in the process, WECC may ask for scope expansion (i.e., Align—Finding Update).
- ✓ WECC will ask for the EOC methodology and results if not provided in Align.

WECC Review Perspective

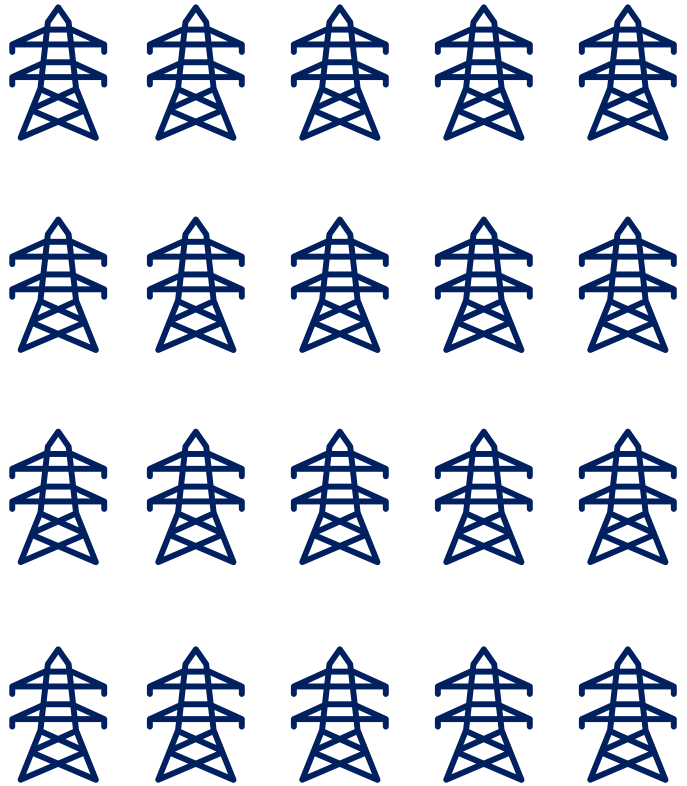
- How did you determine the complete magnitude of the noncompliance?
- Did your company assess the entire organization AND affiliates?
- Were appropriate criteria applied to the analysis?
- How was the EOC verified?

NERC Self-Report & Mitigation Guide

The CEA and NERC should be able to understand how the registered entity determined that the level of EOC assessment was appropriate, since the scope of the assessment may differ based on the facts of the noncompliance.

Determining Magnitude

- Be purposeful and thorough in planning and executing.
- Don't arbitrarily limit the scope.
- Look to assess whole entity organization and all affiliates.
- EOC depends on noncompliance.
- Know why you are excluding items and document the reason(s) in your methodology.
- Use sampling where appropriate.



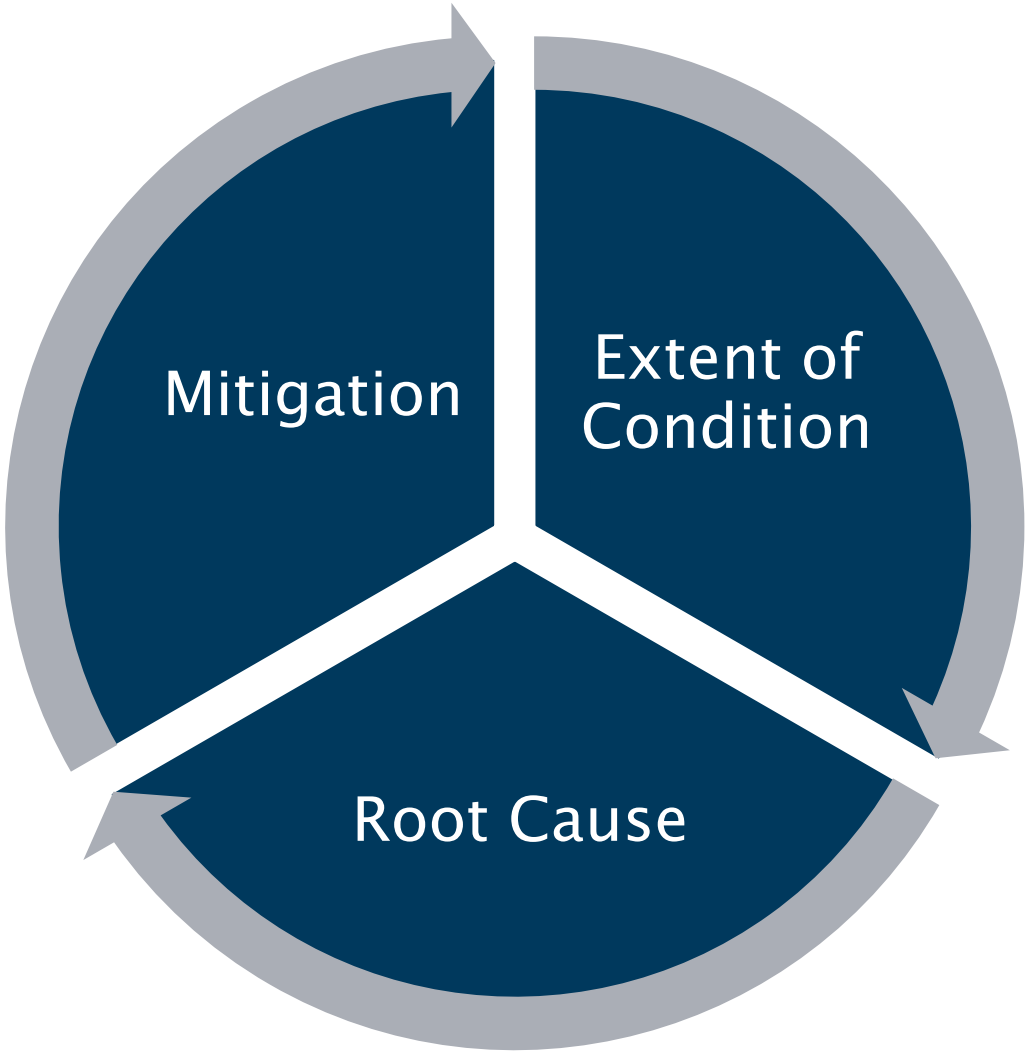
EOC Criteria Consideration

- Causal Factors
- Uniqueness
- Recurrence
- Seriousness
- Cost

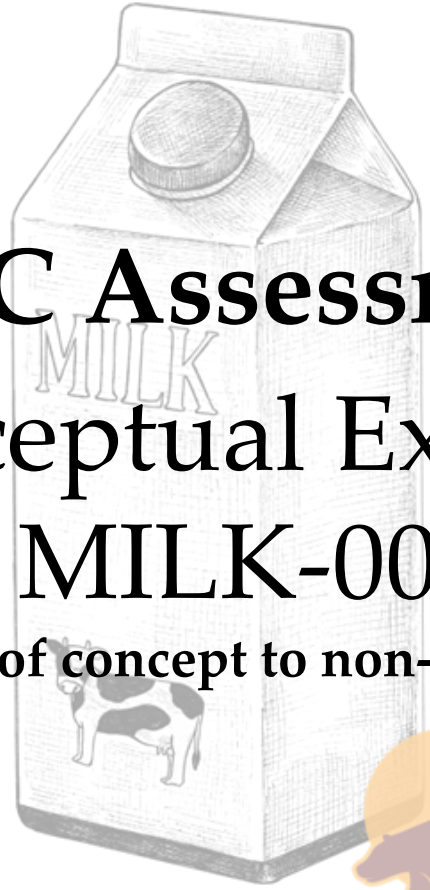
Who should perform an EOC Assessment?

- EOC assessments should be performed by:
  - Appropriate subject matter experts;
  - Staff personnel that have been trained and understand EOC assessments and the substance of the issue;
  - Individuals with appropriate expertise in the areas being evaluated and associated areas; and
  - Individuals with the problem-solving skills able to understand the corrective actions needed to resolve issues comprehensively.

Essential Interplay



Section 2.2—EOC Concept Example



EOC Assessment

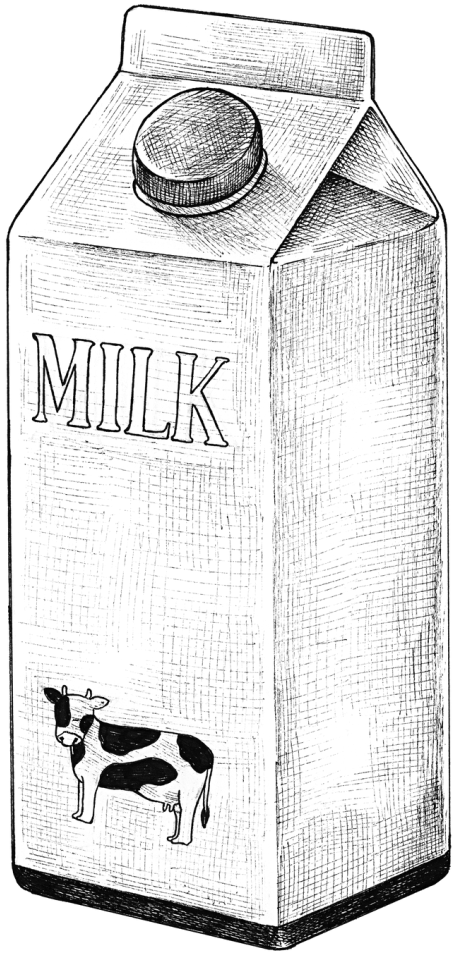
Conceptual Example

MILK-001

Application of concept to non-NERC situation

SUNBEAR POWER

2.2 EOC Assessment

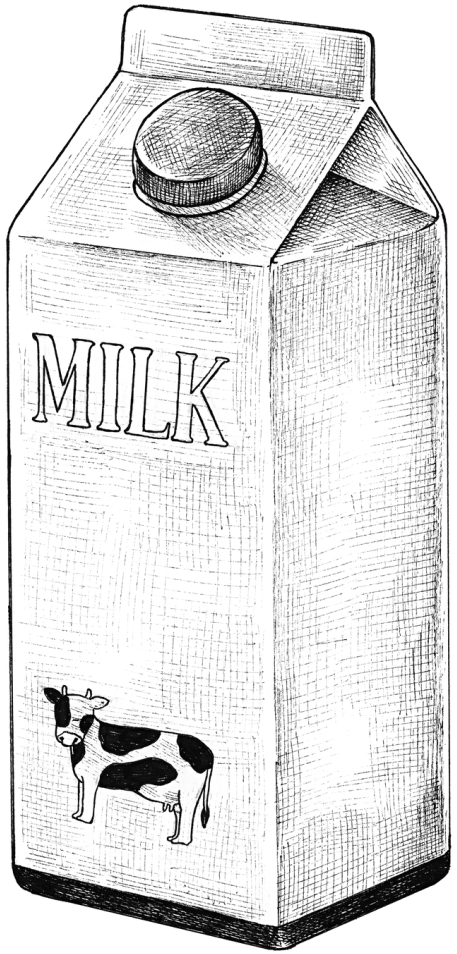


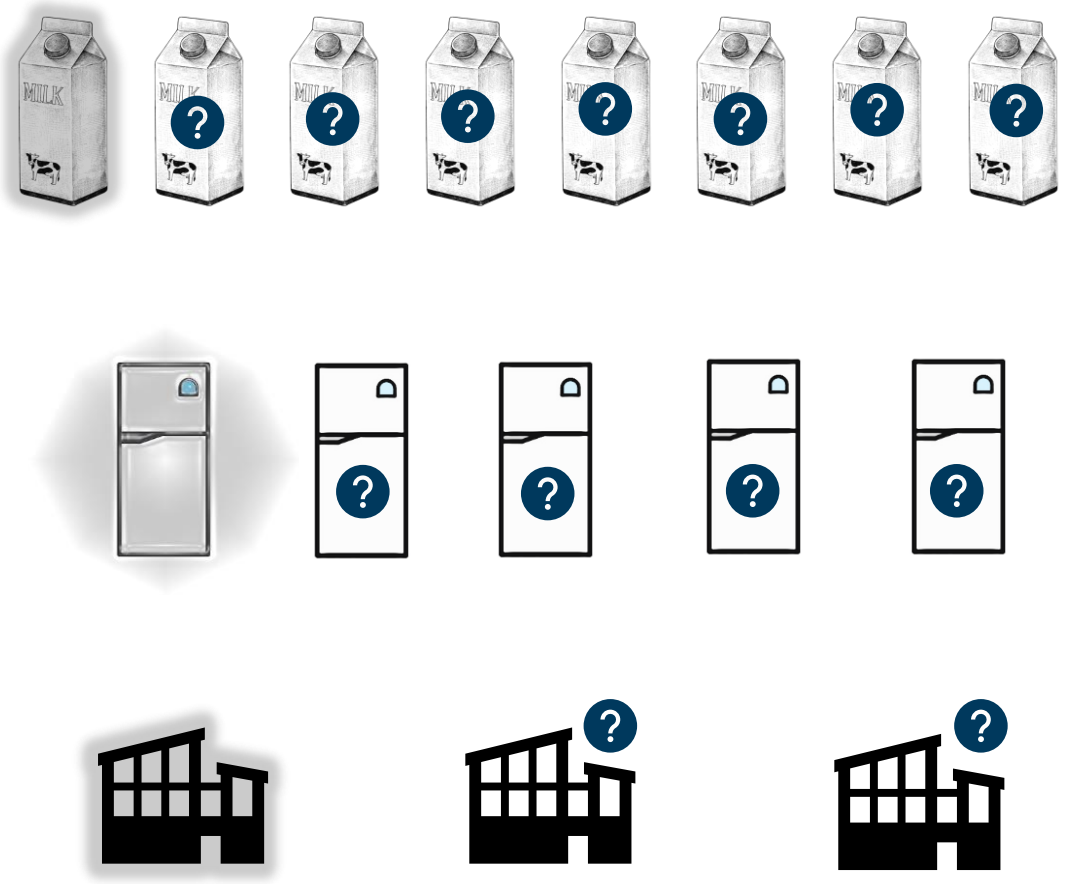
Food Standard:

SNBR-MILK-001

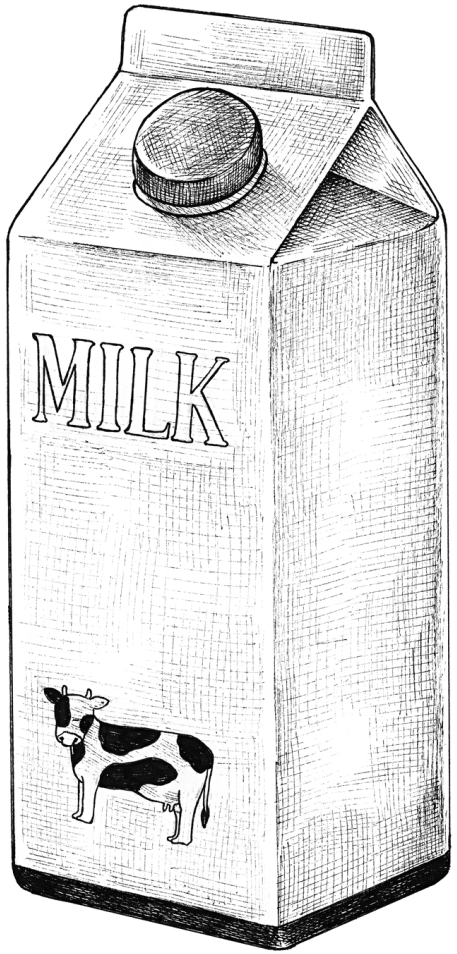
Pasteurized Milk must be discarded on or before the expiration date listed on each carton.

EOC Assessment





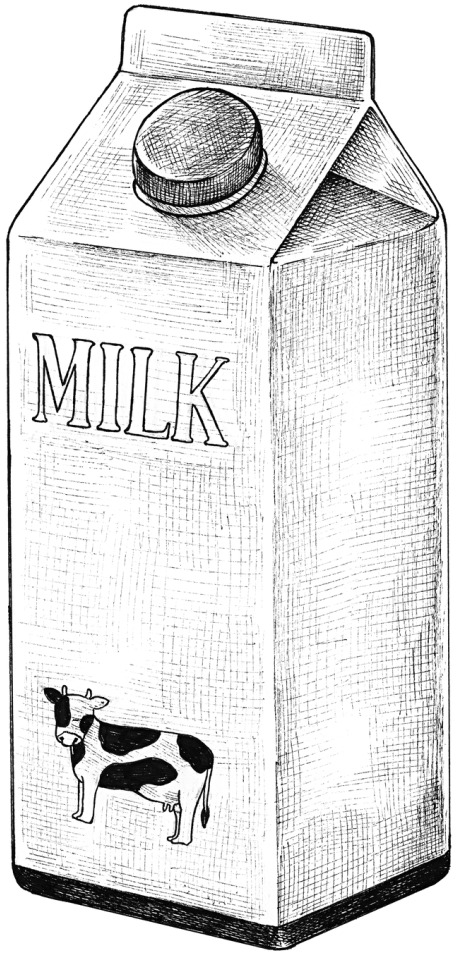
EOC Assessment



Original EOC Description

No other spoiled milk was found.

EOC Assessment



Improved EOC Description

Sunbear performed an EOC by inspecting all milk, in all refrigerators, at all locations for past expiration dates. Sunbear identified seven gallons of milk stored in five refrigerators at three locations. Three of the seven gallons of milk were determined to be five days past the food safety date but showed no signs of spoilage.

2.2 EOC Assessment—Example 1

EOC Assessment

Teaching Exercise One

FAC-003-4 R2

Present incomplete example and then demonstrate how to complete it

Section 2.2—EOC Example 1

Original EOC Assessment

- Sunbear determined the cause of the noncompliance was a documentation error in the aerial inspection log of the 230 kV Point A to Point B line that should have initiated a ground inspection of the part of this line that had the MVCD encroachment. Sunbear performed an inspection of all its lines. Sunbear found no other MVCD encroachments.
- Sunbear reviewed its aerial inspection logs to see whether there were other documentation errors. Sunbear found identical errors in its aerial inspection logs for some of its other transmission lines that were not violations of any standard requirements but were documentation errors that needed to be corrected to prevent future noncompliance.

Section 2.2—EOC Example 1

Questions to consider

- What time frame of records were reviewed?
- Why was this time frame chosen?
- What specific analysis was performed?
- Who performed the analysis?
- Were all applicable locations or facilities analyzed?
- Were there any other similar standards that could be affected?
- Does the EOC analysis make sense given all the causes?

Section 2.2—EOC Example 1

Improved EOC Assessment

- Sunbear determined the cause of the noncompliance was a documentation error in the aerial inspection log of the 230 kV Point A to Point B line that should have initiated a ground inspection of the part of this line that had the MVCD encroachment. Sunbear performed a ground inspection of all its lines to determine whether there were any other MVCD encroachments. Sunbear found no other MVCD encroachments.
- Sunbear's SMEs also reviewed 100% of its most recent aerial inspection logs to see whether there were other documentation errors that led to or could have led to other instances of noncompliance. Sunbear found identical errors in its aerial inspection logs for 3 out of 52 of its FAC-003 applicable transmission lines that were not violations of any standard requirements but were documentation errors that needed to be corrected to prevent future noncompliance.

2.2 EOC Example 2

EOC Assessment

Teaching Exercise Two

CIP-004-6 R4

Present incomplete example and then demonstrate how to complete it.

Section 2.2—EOC Example 2

Original EOC Assessment

- Sunbear's CIP-004-6 SMEs completed an EOC review by reviewing records from October 23, 2016, through January 24, 2024. Sunbear found that all employees and contractors with physical and electronic access to BES Cybersecurity Information (BCSI) had a documented business justification, and Sunbear found no more instances of missing business justifications for electronic and unescorted physical access. Sunbear also reviewed its compliance with CIP-004-6 R4 (P4.2-P4.4) and found no more instances of noncompliance.

Section 2.2—EOC Example 2

Improved EOC Assessment

- Sunbear's CIP-004-6 SMEs completed an EOC review by reviewing records from October 23, 2016, through January 24, 2024. This review period was selected because October 23, 2016, is when Sunbear implemented its new access control policy and its workflow management system; January 24, 2024, is when all mitigation was completed. Sunbear found that all employees and contractors with physical and electronic access to BES Cybersecurity Information (BCSI) had a documented business justification, and Sunbear found no more instances of missing business justifications for electronic and unescorted physical access. Sunbear also reviewed its compliance with CIP-004-6 R4 (P4.2-P4.4) and found no more instances of noncompliance.

2.2 EOC Assessment

Extent of Condition Review

Peer Review Exercise Three

VAR-002-4.1 R3

Review an Extent of Condition analysis and participants identify deficiencies

Section 2.2—Example 3

Original EOC Assessment

- Sunbear's compliance personnel and SMEs reviewed all AVR status changes from January 1, 2020, through February 28, 2023. Sunbear completed a full review of its AVR status changes before January 1, 2020, as part of a WECC Self-Certification and found no issues.
- Shift supervisor and the plant operator that discovered the issue performed the EOC. This process was completed on February 28, 2023.
- Additionally, the operator logs and alarms from January 1, 2020, through February 28, 2023, were reviewed to ensure no other standards were violated during periods when Sunbear was understaffed. No other issues were identified.

Continued…

Section 2.2—Example 3

Original EOC Assessment

- Sunbear also reviewed VAR-002-4.1 R3 to see whether this issue was potentially a violation of that requirement. Sunbear does not believe that this is a violation of R3 because Sunbear notified its TOP that it was operating temporarily in manual mode 55 minutes after the status unexpectedly changed, and Sunbear was not intentionally operating the AVR in a mode contrary to the direction of its TOP. Furthermore, Sunbear returned the AVR to automatic mode as soon as the repairs were complete that allowed the AVR to be returned to automatic mode.
- Sunbear does not have any affiliates, and this issue would not affect Sunbear's transmission compliance.
- The registered entity determined the EOC was sufficient because it reviewed all AVR status changes at all generating units since this standard became effective.

Section 2.2—Example 3

Improved EOC Assessment

- Sunbear's compliance personnel and SMEs reviewed all AVR status changes from January 1, 2020, through February 28, 2023, for all five of Sunbear's generating units. Sunbear completed a full review of its AVR status changes for all five of Sunbear's generating units before January 1, 2020, as part of a WECC Self-Certification and found no issues.
- Shift supervisor and the plant operator that discovered the issue performed the EOC. This process was completed on February 28, 2023.
- Sunbear determined that there were 36 additional AVR status changes that lasted 30 minutes or more during this review period. Sunbear compared these to the Operator logs and determined that all 36 instances were correctly reported within 30 minutes of the status change to its TOP.
- Additionally, the operator logs and alarms from January 1, 2020, through February 28, 2023, were reviewed to ensure no other standards were violated during periods when Sunbear was understaffed. No other issues were identified.

Continued…

Section 2.2—Example 3

Improved EOC Assessment

- Sunbear also reviewed VAR-002-4.1 R1 to see whether this issue was potentially a violation of that requirement. Sunbear does not believe that this is a violation of R1 because Sunbear notified its TOP that it was operating temporarily in manual mode 55 minutes after the status unexpectedly changed, and Sunbear was not intentionally operating the AVR in a mode contrary to the direction of its TOP. Furthermore, Sunbear returned the AVR to automatic mode as soon as the repairs were complete that allowed the AVR to be returned to automatic mode.
- Sunbear does not have any affiliates, and this issue would not affect Sunbear's transmission compliance.
- The registered entity determined the EOC was sufficient because it reviewed all AVR status changes at all generating units since this standard became effective.

2.2 EOC Assessment

EOC Assessment

Peer Review Exercise Four

CIP-007-6 R2

Review an Extent of Condition analysis and participants identify deficiencies.

Section 2.2—Example 4

Original EOC Analysis Statement

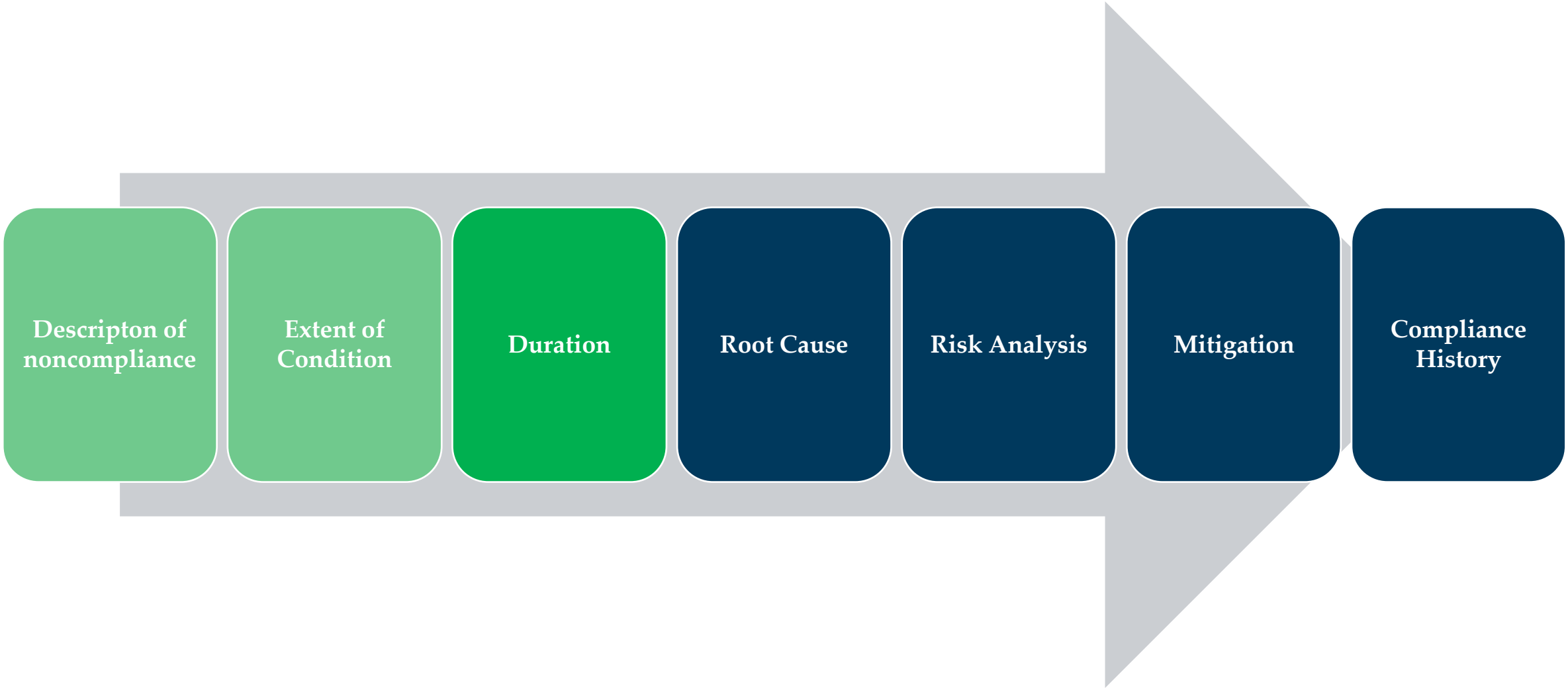
- To determine the EOC, Sunbear SMEs reviewed all other patches released during the same calendar quarter as this noncompliance start (1/1/2023–3/1/2023) to ensure no other patches failed to install on any of Sunbear's applicable Cyber Assets. Sunbear has 101 Cyber Assets (45 BCAs, 10 PCAs, 36 EACMS, and 10 PACS) associated with its one HIBCS. Sunbear has no affiliates.
- Sunbear did not identify any additional patches that failed to install on other applicable Cyber Assets. After the vulnerability assessment tool was functional again, the entity did not identify any additional issues with missed patches.
- Sunbear reviewed and did not identify any other parts of R2 that were affected and identified no other standard requirements that were violated because of this incident.

Section 2.2—Example 4

Improved EOC Analysis Statement

- To determine the EOC, Sunbear SMEs reviewed all other patches released during the same calendar quarter as this noncompliance start (1/1/2023–3/1/2023) to ensure no other patches failed to install on any of Sunbear's applicable Cyber Assets. Sunbear has 101 Cyber Assets (45 BCAs, 10 PCAs, 36 EACMS, and 10 PACS) associated with its one HIBCS. Sunbear has no other HIBCS and no MIBCS. Sunbear has no affiliates.
- Sunbear used this review period because its vulnerability assessment tool was intermittently down six times from January to March of 2023 due to issues the vulnerability assessment tool provider experienced with this application. Sunbear had experienced no other vulnerability assessment tool outages before January 2023 and has not had any vulnerability assessment tool outages since March 18, 2023. Sunbear also reviews its patching biannually and found no issues from 1/1/2023 to 6/30/2023.
- Sunbear did not identify any additional patches that failed to install on other applicable Cyber Assets. After the vulnerability assessment tool was functional again, the entity did not identify any additional issues with missed patches.
- Sunbear reviewed and did not identify any other parts of R2 that were affected and identified no other standard requirements that were violated because of this incident.

2.2 Extent of Condition Review



<Public>

WECC

Electric Reliability and Security for the West

www.wecc.org

WECC

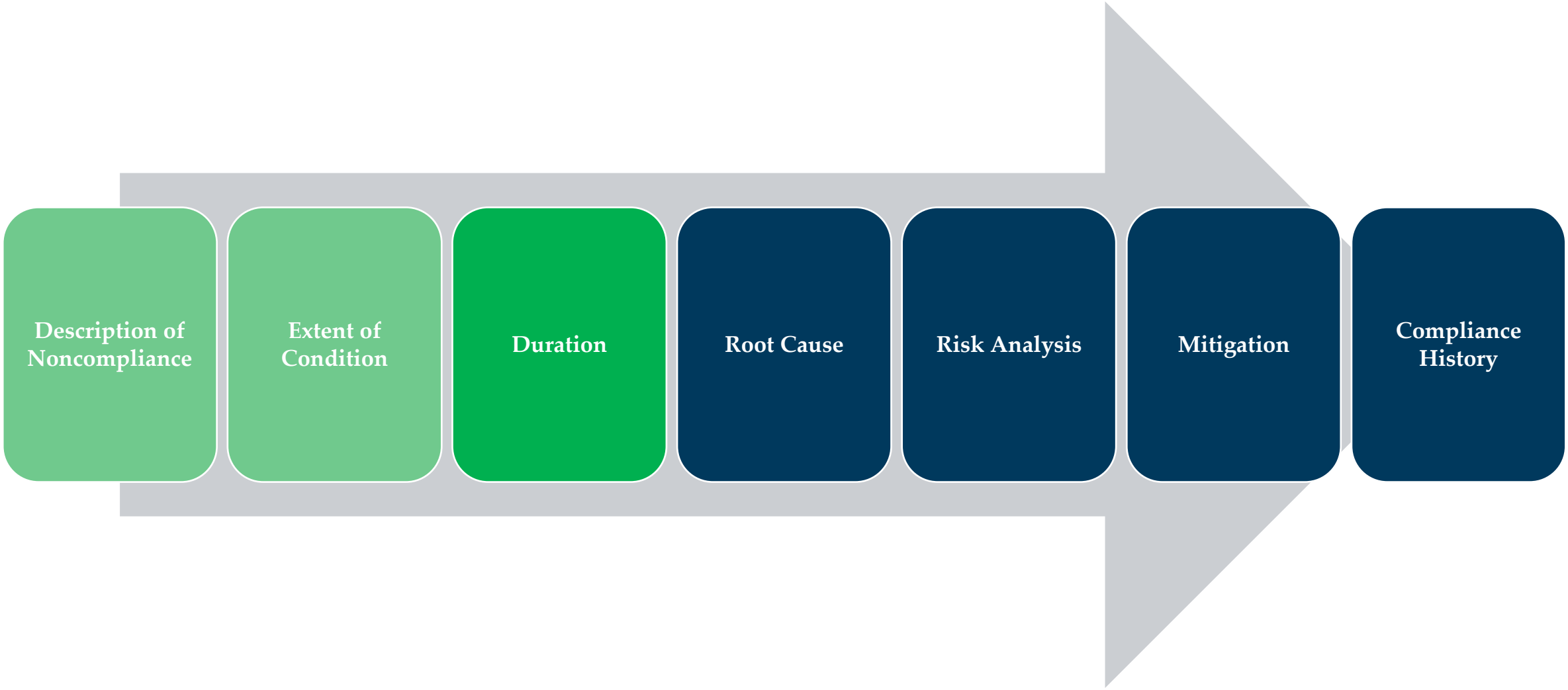
WECC Enforcement Training:

2.3 Duration

March 25, 2024

WECC Enforcement Staff

2.3 Duration


Description of Noncompliance
Extent of Condition
Duration
Root Cause
Risk Analysis
Mitigation
Compliance History

Section Learning Plan

1

Conceptual Foundation

- Application of concept to non-NERC situations

2

Teaching Exercises

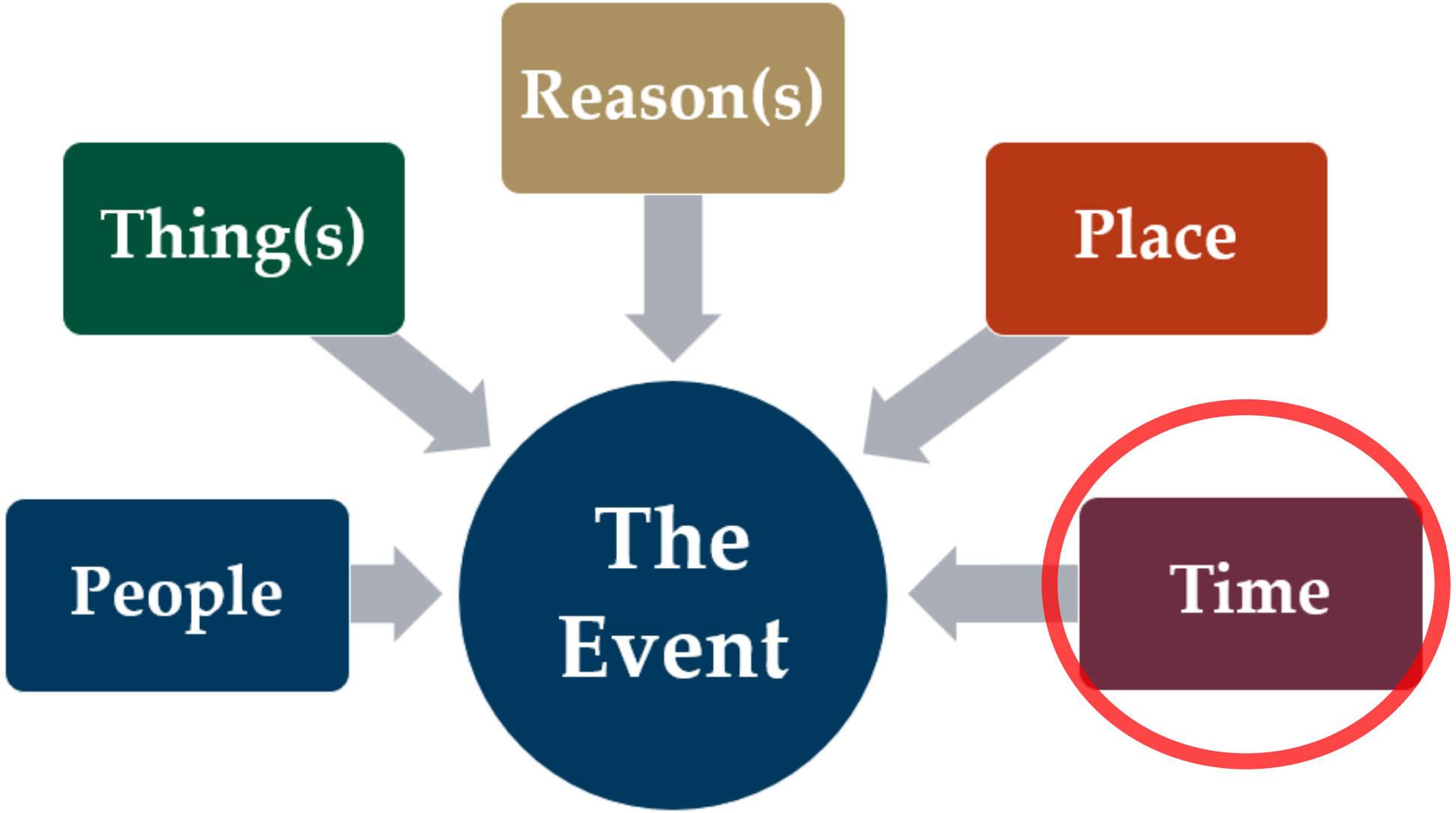
- Present incomplete examples and then demonstrate how to complete them
- FAC-003-4 & CIP-004-6

3

Peer Review Exercises

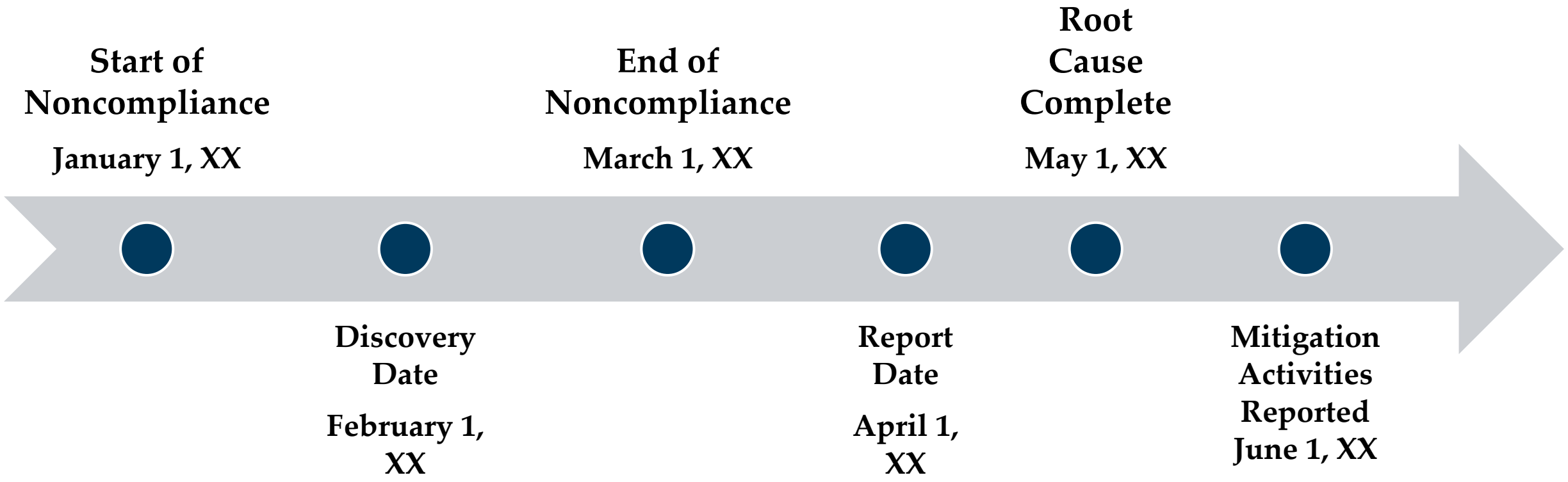
- Review noncompliance descriptions and participants identify deficiencies
- VAR-002-4.1 & CIP-007-6

2.3 Duration



2.3 Duration

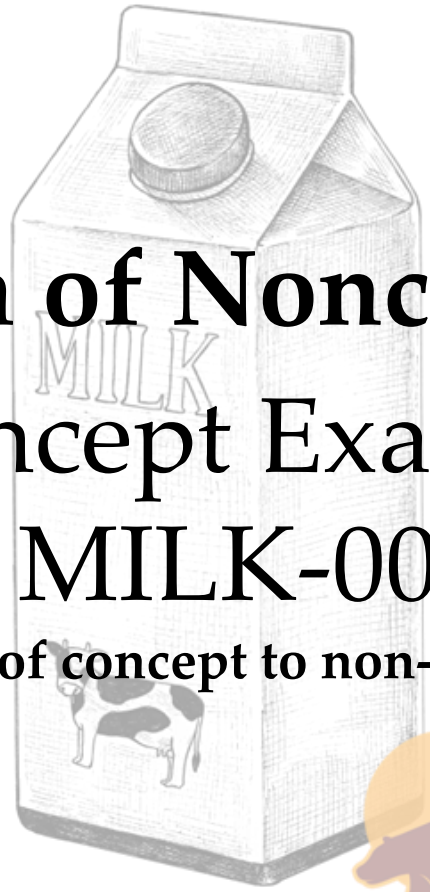
The time of each noncompliance must be understood from beginning to end.



2.3 Duration

- Identify the duration of the noncompliance, including start and end dates, and an **explanation for those dates**.
- The **start date** would be the earliest known occurrence of the noncompliance, the enforceable date of the Standard, or the prior mitigation completion date for the same Standard and Requirement.
- The **end date** would be when the entity corrected (remediated) the noncompliance, which is not necessarily the mitigation completion date.
- Consider the time horizon of the noncompliance, e.g., did the noncompliance impair or threaten real-time operations, day-ahead operations planning, or long-term planning?

Section 2.3—Concept Example



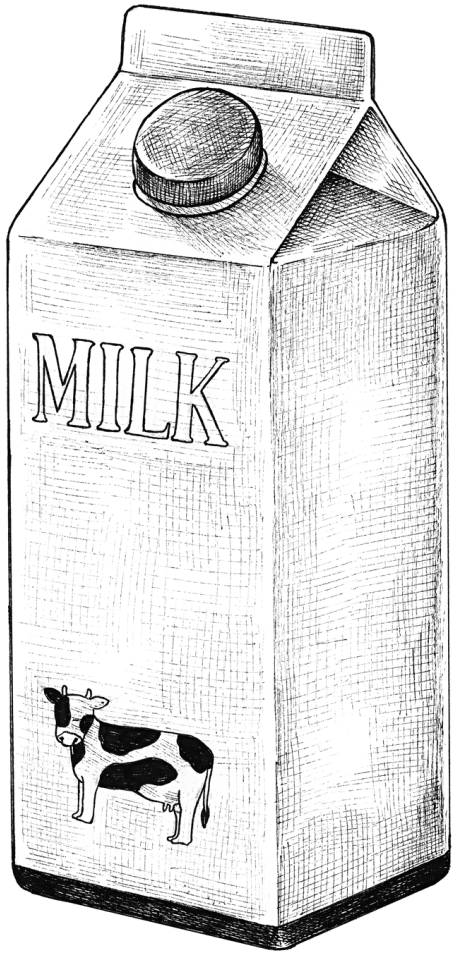
Duration of Noncompliance

Concept Example

MILK-001

Application of concept to non-NERC situation

2.3 Duration

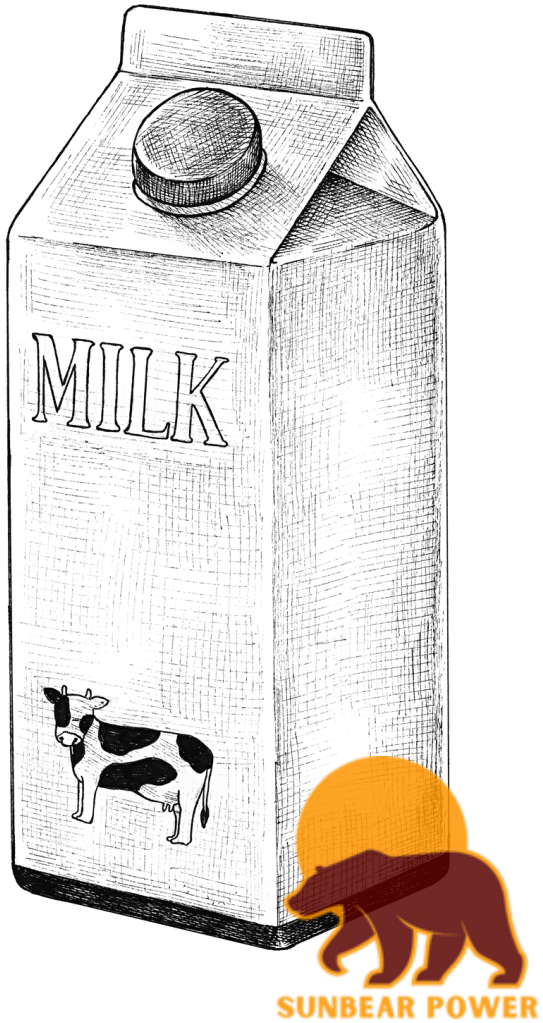


Food Standard:

SNBR-MILK-001

Pasteurized Milk must be discarded on or before the expiration date listed on each carton.

2.3 Duration of Noncompliance

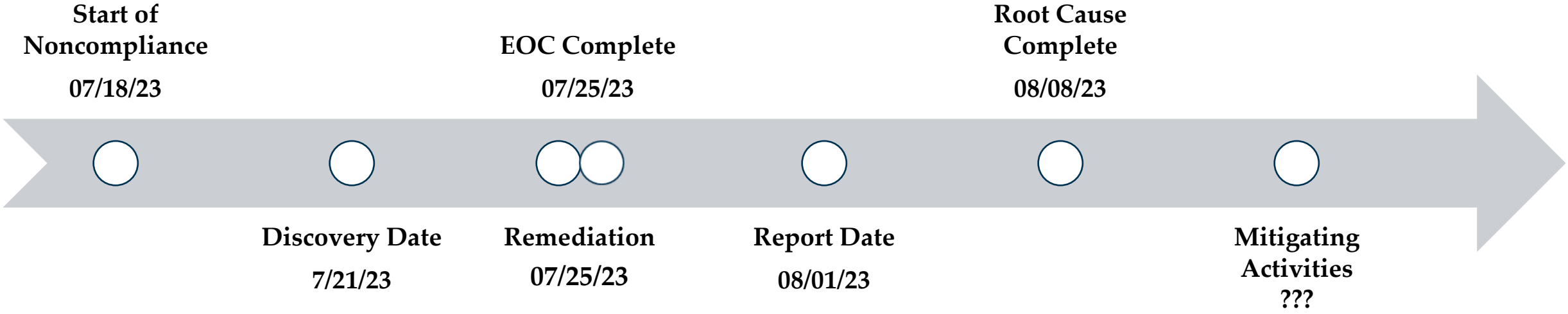


Original Duration Information

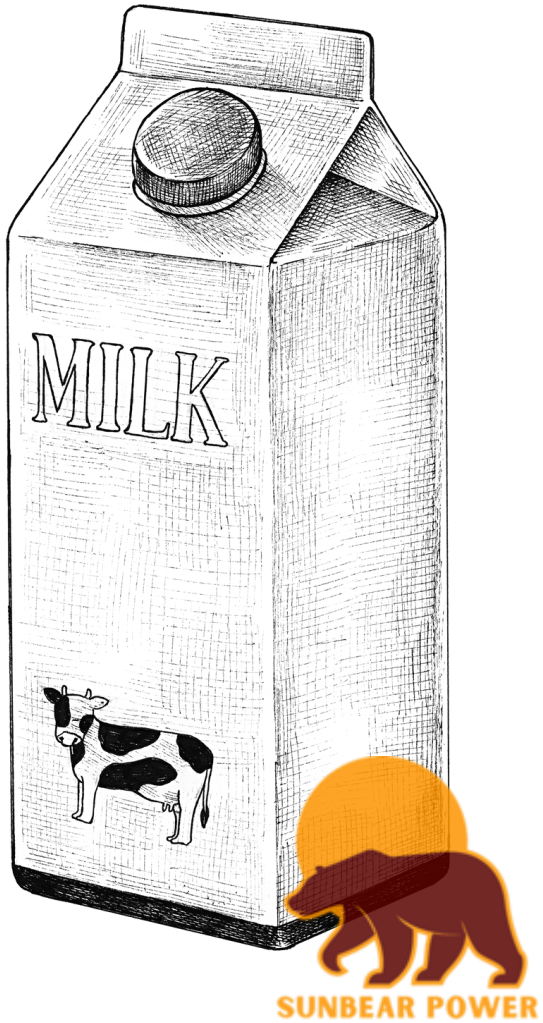
Sunbear employees discovered and discarded spoiled milk on July 21, 2023.

2.3 Duration

The time of each noncompliance must be understood from beginning to end.



2.3 Duration of Noncompliance



Improved Duration Information

Sunbear employees found spoiled milk on July 21, 2023. Two gallons had a expiration date of 7/17/23, and needed to be disposed of on or prior to this date. Based on the EOC performed, three additional gallons of noncompliant milk were identified. These had an expiration date of 7/19/23 and were discarded on July 25, 2023.

2.3 Duration

Duration of Noncompliance

Teaching Exercise One

FAC-003-4 R2

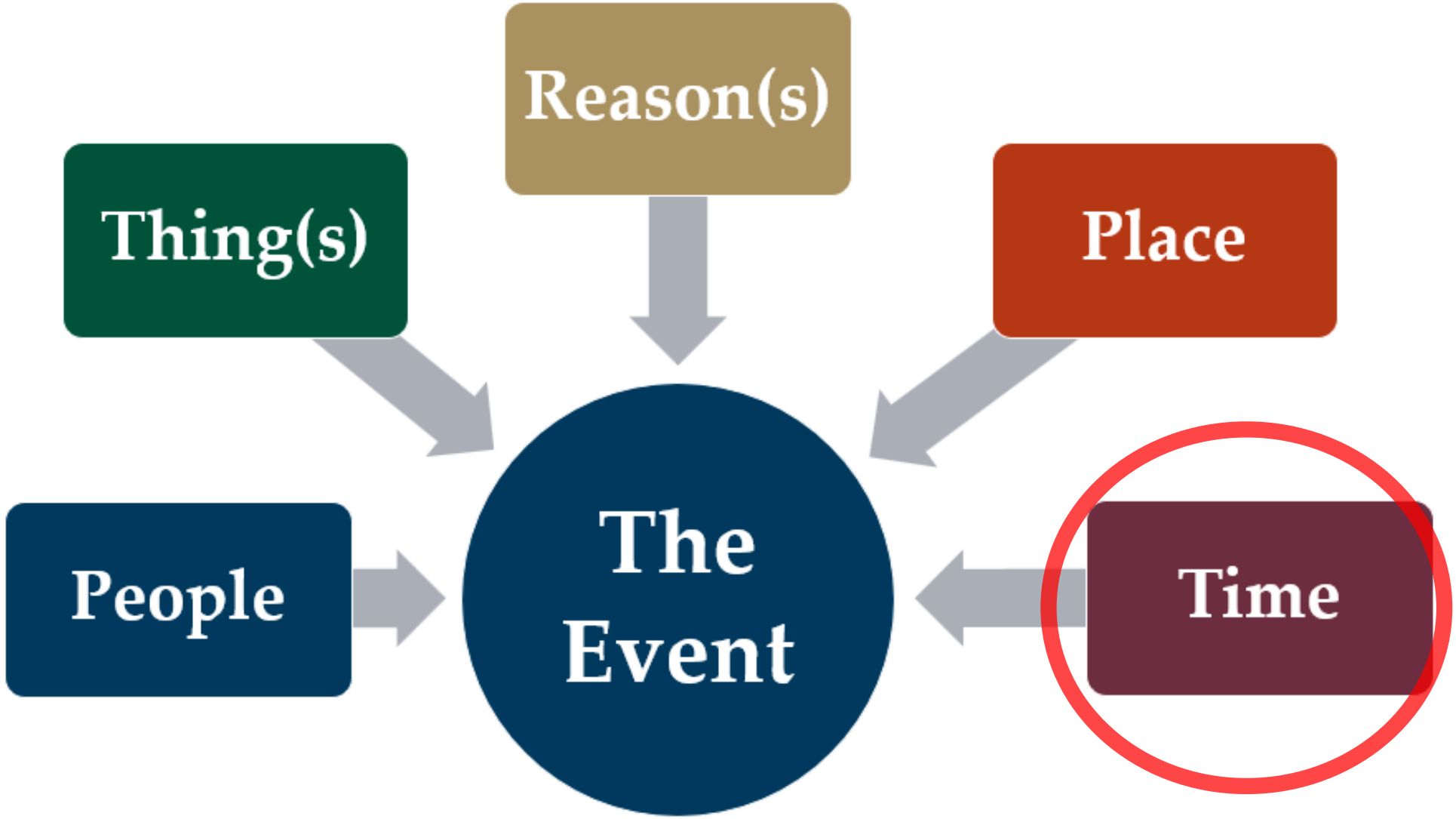
Present incomplete example and then demonstrate how to complete it

2.3 Duration

Original duration information

- A Phase to Ground fault occurred on July 20, 2017, on a 230 kV line. After a management investigation the following day, the field supervisor ordered all vegetation within the Minimum Vegetation Clearance Distance (MVCD) to be removed.

2.3 Duration



Section 2.3—Example 1

Questions to consider?

- What times did this noncompliance start and end?
- Why did it start at that date and time?
- Why did it end at that date and time?
- If there were multiple instances, when did they start and end and why?

2.3 Duration

Improved duration statement:

- On July 20, 2017, at 2:20 p.m., Sunbear noted that there was a phase to ground fault that occurred on its 230 kV Point A to Point B line when a poplar tree that was growing within the Minimum Vegetation Clearance Distance (MVCD) came in contact with the 230 kV Point A to Point B line.
- The noncompliance ended on July 22, 2017, when the poplar tree was entirely removed from the 230 kV Point A to Point B line easement.

2.3 Duration

Duration of Noncompliance

Teaching Exercise Two

CIP-004-6 R4

Present incomplete example and then demonstrate how to complete it.

2.3 Duration

Original duration information:

- The noncompliance started on November 15, 2016, when the first unescorted physical access to a PSP was granted without a documented business justification. The other 11 instances where Sunbear granted users access without a documented business justification occurred after November 15, 2016, and before April 4, 2023. Please see the attached spreadsheet for the specific dates for all 12 instances of noncompliance.

2.3 Duration

Improved duration information:

- The noncompliance started on November 15, 2016, when the first unescorted physical access to a PSP was granted without a documented business justification and ended on January 4, 2024, when all 12 records granting access without a documented business justification were corrected to include the business justification. The other 11 instances where Sunbear granted users access without a documented business justification occurred between after November 15, 2016, and before April 4, 2023. Please see the attached spreadsheet for the specific dates for all 12 instances of noncompliance.

2.3 Duration

Duration of Noncompliance

Peer Review Exercise Three

VAR-002

Review an Extent of Condition analysis and participants identify deficiencies

2.3 Duration

Original duration information:

- Sunbear's AVR changed to manual control at 3:35 pm on February 20, 2023. Sunbear was unable to change the AVR back to automatic control until February 21, 2023, at 9:25 am. The noncompliance lasted for 55 minutes.
- There were no other instances of AVR status changes without the required notification.

2.3 Duration

Improved duration information:

- Sunbear's AVR changed to manual control at 3:35 pm on February 20, 2023. Sunbear was unable to change the AVR back to automatic control until February 21, 2023, at 9:25 am. Sunbear was noncompliant from February 20, 2023, at 4:06 pm, which was 31 minutes following the AVR status change, until 5:01 pm on that same day when Sunbear's night operator informed the TOP of the AVR status change. The noncompliance lasted for 55 minutes.
- This incident started at 4:06 pm on February 20, 2023, and ended at 5:01pm on February 20, 2023.
- The noncompliance start date and time is 4:06 pm on 2/20/2023 because there is a 30-minute deadline to either restore the AVR to the correct mode or notify the affected TOP that the AVR status has changed.
- The noncompliance end date and time is 5:01 pm on 2/20/2023 because the TOP was notified of the change at this time.
- There were no other instances of AVR status changes without the required notification.

2.3 Duration

If there were multiple instances, when did they start and end and why?

Improved duration information:

- Sunbear's AVR changed to manual control at 3:35 pm on February 20, 2023. Sunbear was unable to change the AVR back to automatic control until February 21, 2023, at 9:25 am. Sunbear was noncompliant from February 20, 2023, at 4:06 pm, which was 31 minutes following the AVR status change, until 5:01 pm on that same day when Sunbear's night operator informed the TOP of the AVR status change. The noncompliance lasted for 55 minutes.
- This incident started at 4:06 pm on February 20, 2023, and ended at 5:01pm on February 20, 2023.
- The noncompliance start date and time is 4:06 pm on 2/20/2023 because there is a 30-minute deadline to either restore the AVR to the correct mode or notify the affected TOP that the AVR status has changed.
- The noncompliance end date and time is 5:01 pm on 2/20/2023 because the TOP was notified of the change at this time.
- There were no other instances of AVR status changes without the required notification.

2.3 Duration

Duration of Noncompliance

Peer Review Exercise Four

CIP-007-6 R2

Review a duration statement and determine deficiencies.

2.3 Duration of Noncompliance

Original duration information:

- The noncompliance started on March 8, 2023. Sunbear evaluated security patches for the 25 BCAs that are the subject of this noncompliance on February 2, 2023. Therefore, Sunbear should have installed the security patches by midnight on March 7, 2023, but failed to do so.
- This noncompliance was discovered on September 15, 2023, when Sunbear found it during a regular, biannual internal review which is a detective control.

2.3 Duration of Noncompliance

Improved duration information:

- There was one instance which started on March 8, 2023, and ended on September 20, 2023.
- The noncompliance started on March 8, 2023. Sunbear evaluated security patches for the 25 BCAs that are the subject of this noncompliance on February 2, 2023. Therefore, Sunbear should have installed the security patches by midnight on March 7, 2023, but failed to do so.
- The compliance ended on September 20, 2023, when Sunbear applied the patches to the 25 affected BCAs.
- This noncompliance was discovered on September 15, 2023, when Sunbear found it during a regular, biannual internal review which is a detective control.

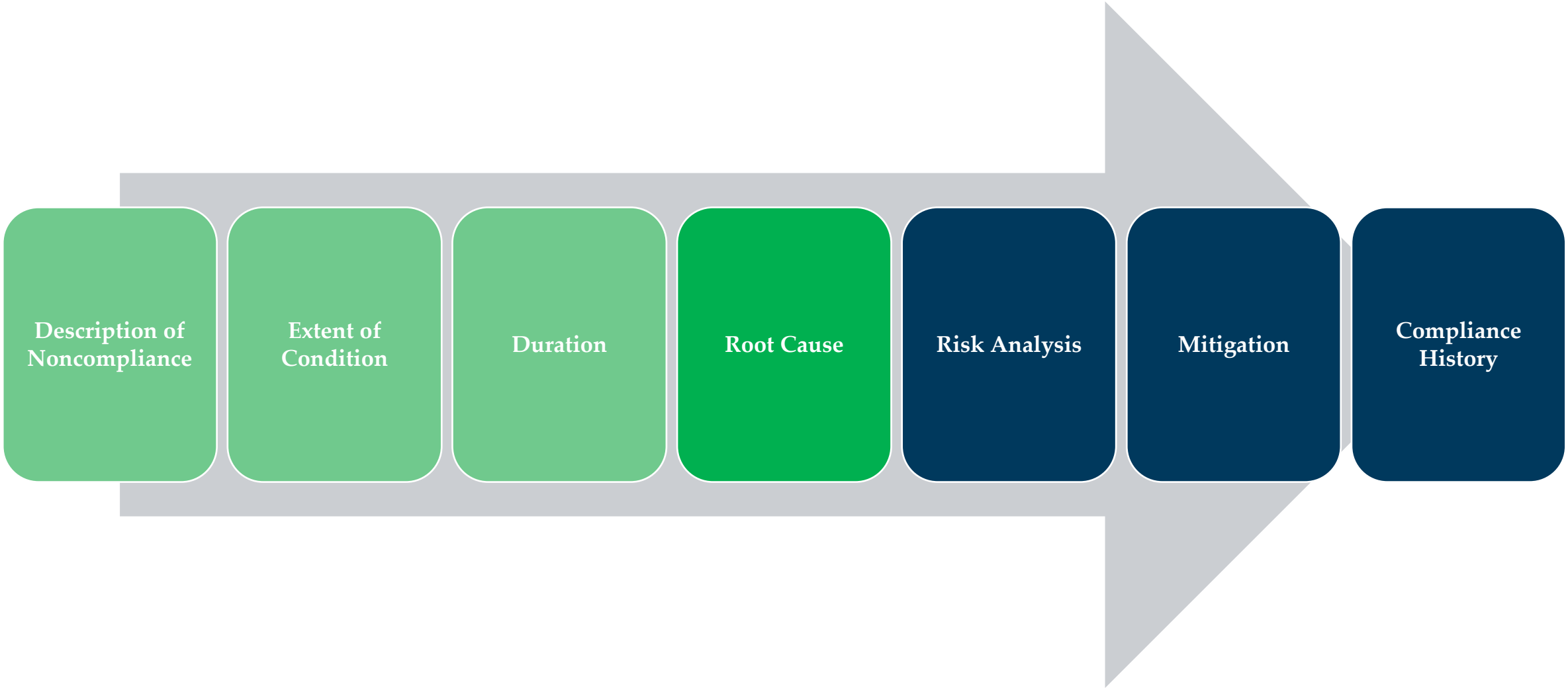
2.3 Duration of Noncompliance

Improved duration information:

- There was one instance which started on March 8, 2023, and ended on September 20, 2023.
- The noncompliance started on March 8, 2023. Sunbear evaluated security patches for the 25 BCAs that are the subject of this noncompliance on February 2, 2023. Therefore, Sunbear should have installed the security patches by midnight on March 7, 2023, but failed to do so.
- The compliance ended on September 20, 2023, when Sunbear applied the patches to the 25 affected BCAs.
- This noncompliance was discovered on September 15, 2023, when Sunbear found it during a regular, biannual internal review which is a detective control.

If there were multiple instances, when did they start and end and why?

2.3 Duration


Description of Noncompliance
Extent of Condition
Duration
Root Cause
Risk Analysis
Mitigation
Compliance History

<Public>

WECC

Electric Reliability and Security for the West

www.wecc.org

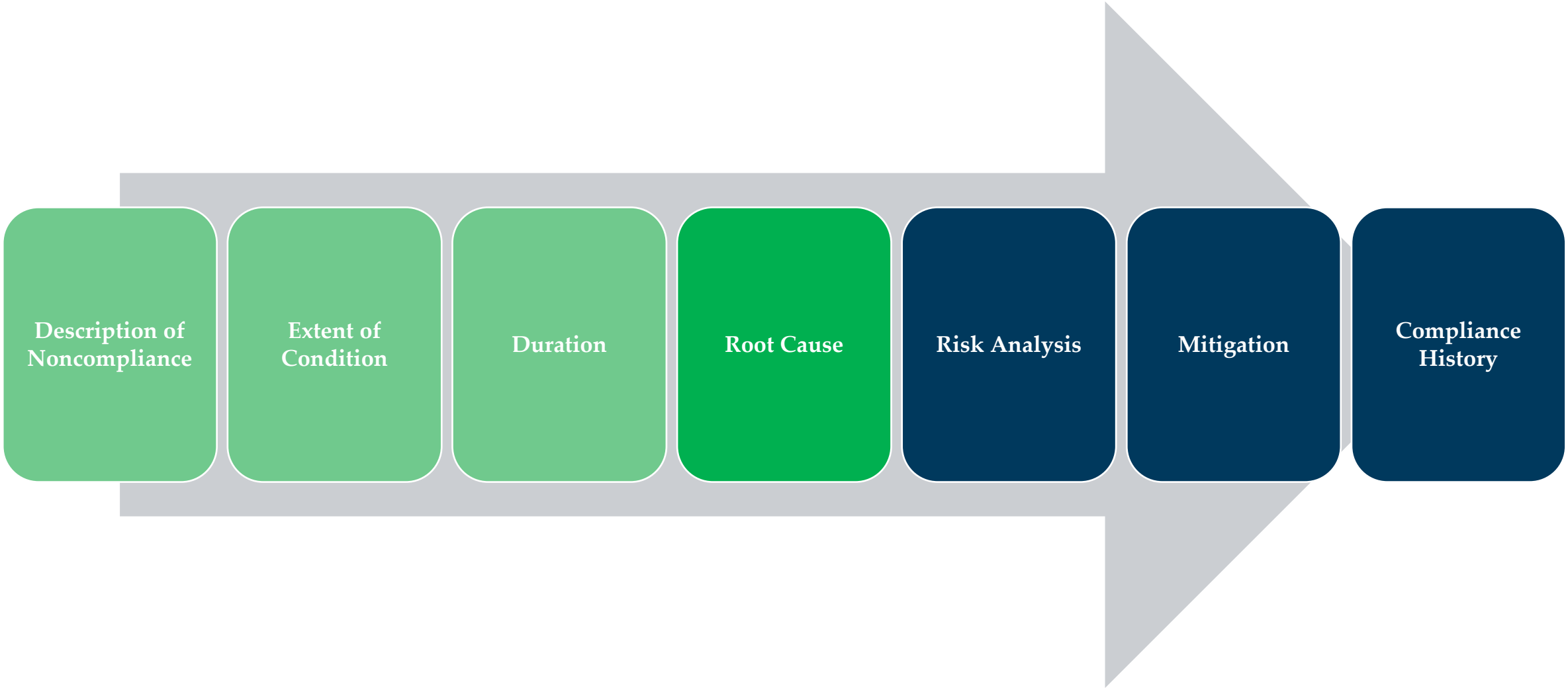
WECC

WECC Enforcement Training:

2.4 Root Cause

WECC Enforcement Staff

2.4 Root Cause



Section Learning Plan

1

Conceptual Foundation

- Application of concept to non-NERC situations

2

Teaching Exercises

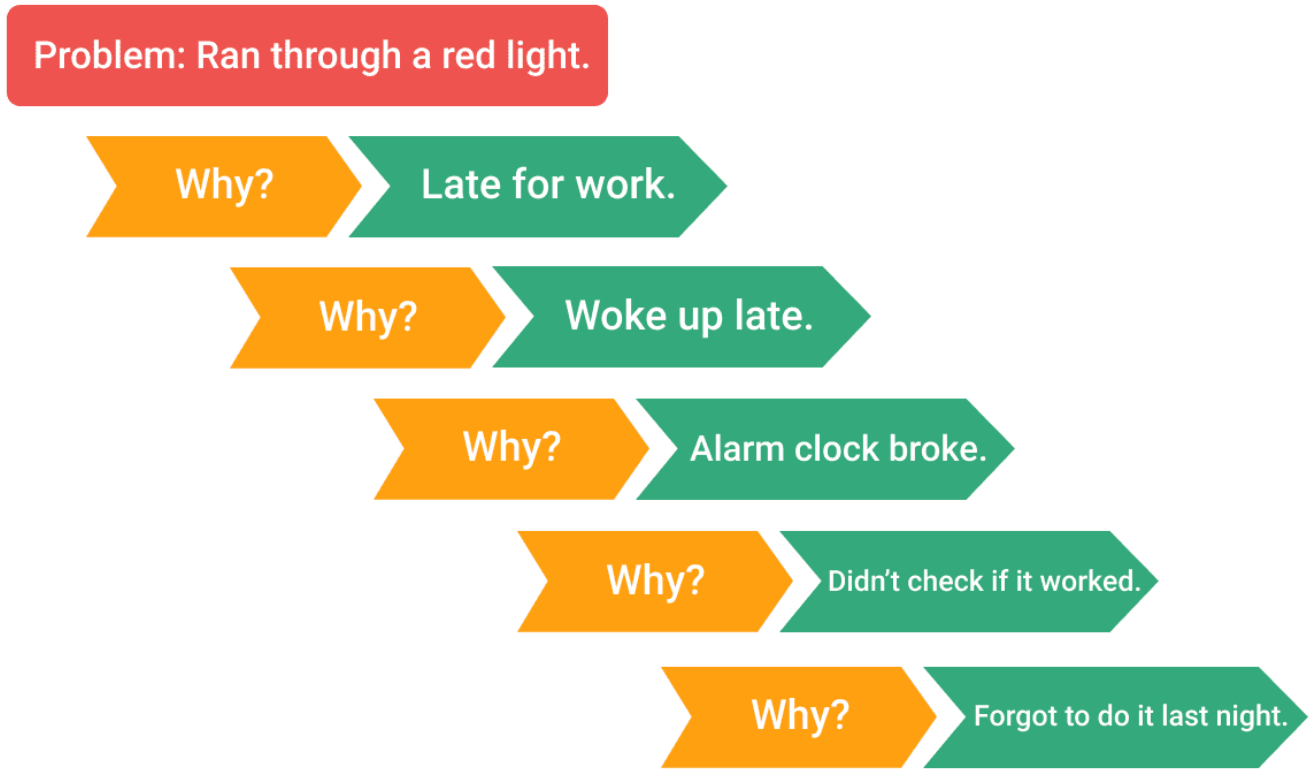
- Present incomplete examples and then demonstrate how to complete them
- FAC-003-4 & CIP-004-6

3

Peer Review Exercises

- Review noncompliance descriptions and participants identify deficiencies
- VAR-002-4.1 & CIP-007-6

Conceptual Foundations



- Root cause analysis (RCA)—a collective term that describes a wide range of approaches, tools, and techniques used to uncover causes of problems.
- The root cause —the core issue—the highest-level cause—that sets in motion the entire cause-and-effect reaction that ultimately leads to the problem(s).

Why—Root Cause

To ensure the entire problem has been identified, so remediation and mitigation activities can fully address all cause(s) and prevent reoccurrences.

2.4 Root Cause

Problem

- Breaker was not restored to the correct position after maintenance

Why?

- Worker was in a rush to complete job

Why?

- They had to do maintenance on three other breakers before they could leave, and it was already after hours

Why?

- Sudden unexpected change in schedule

Why

- Poor personnel planning by management

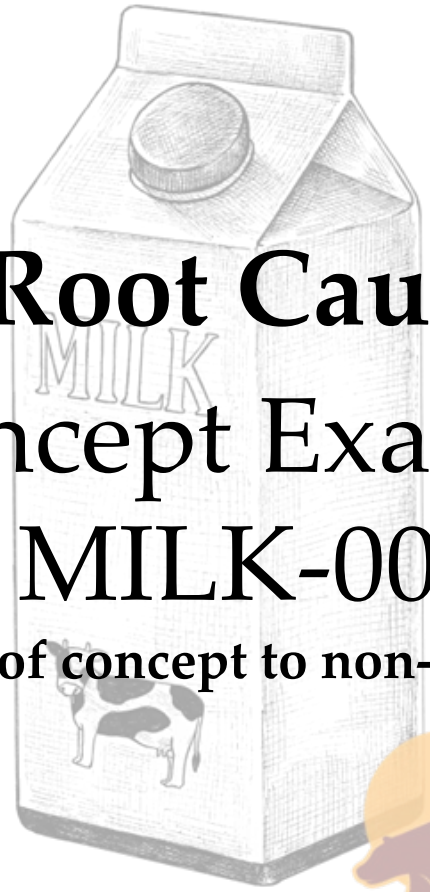
General Expectations and Guidelines

Report the noncompliance as quickly as possible and stop it from continuing or reoccurring

Perform a root cause analysis, but do not delay reporting to finish the root cause analysis

Submit additional root cause analysis details once available

Section 2.4—Concept Example



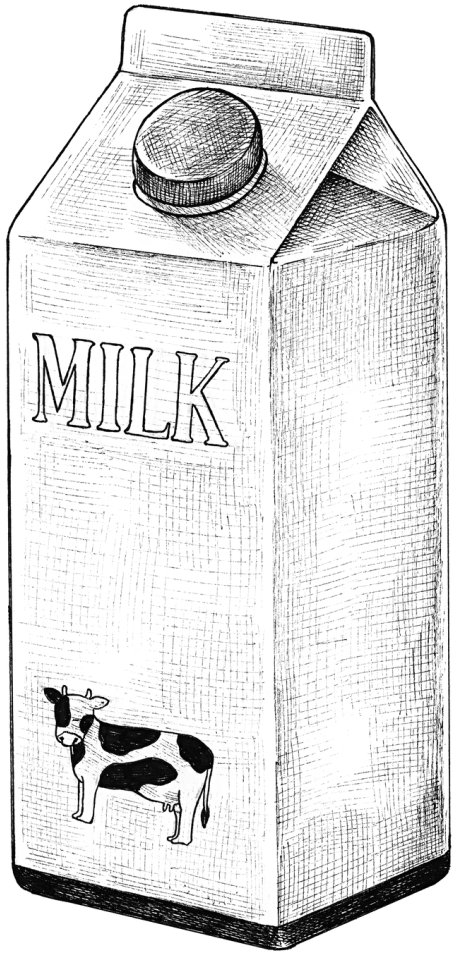
Root Cause

Concept Example

MILK-001

Application of concept to non-NERC situation

2.4 Root Cause



Food Standard:

SNBR-MILK-001

Pasteurized milk must be discarded on or before the expiration date listed on each carton.

2.4 Root Cause

Original Causal Statement

Sunbear successfully determined what caused the milk to be expired.

2.4 Root Cause Analysis

Problem: Spoiled Milk

- Bacteria developed in the milk.

Why?

- Refrigerator unplugged by janitor for extended period causing unsafe temperatures.

Why?

- Refrigerator unplugged so it could be moved to clean floor.

Why?

- The refrigerators electric cord wasn't long enough.

2.4 Root Cause

Improved Causal Statement

- Sunbear determined the spoiled milk discovered on July 21, 2023, was the result of milk being stored at an unsafe temperature. An investigation determined its janitorial staff periodically unplugs this refrigerator to perform floor maintenance. An extended period without power coupled with high ambient temperatures in July caused the milk to spoil.
- The root cause of the violation was determined to be too short of an electrical cord.
- Sunbear also discovered three gallons of milk that had not spoiled at two other locations. Although the food safety date had passed, Sunbear verified janitorial staff did not unplug the other refrigerators because their cord was long enough.
- The root cause of this violation was the employee in charge of Milk Monitoring was on sick leave and back up Milk Monitor was not informed of their absence.

2.4 Root Cause

Root Cause

Teaching Exercise One

FAC-003-4 R2.1

Present incomplete examples and demonstrate how to complete them

2.4 Root Cause

Original root cause

Sunbear determined the cause of the noncompliance related to an error in documentation of the aerial inspection log. The contractor performed an aerial inspection of the 230 kV Point A to Point B line but failed to note that part of the line needed a ground inspection to determine the vegetation distance from the line due to other undergrowth vegetation making the distance difficult to determine.

2.4 Root Cause

Questions to consider

How did the root cause connect to the noncompliance?

What is the chain of facts?

What analysis was done to determine the root cause?

Are there any other causes?

What internal controls were missing that would have detected, prevented, or corrected this encroachment?

2.4 Root Cause

Improved root cause

Sunbear determined the cause of the noncompliance related to an error in documentation of the aerial inspection log. The contractor performed an aerial inspection of the 230 kV Point A to Point B line but failed to note that part of the line needed a ground inspection to determine the vegetation distance from the line due to other undergrowth vegetation making the distance difficult to determine.

A review of current procedures for aerial inspection logs showed that there was an inadequate process to distinguish between the logs for elements inspected from the air that had no issues and those that require follow up. Normal procedure was to just include a comment if follow up was needed. This process was inadequate and contributed to the contractors failure to document the needed follow up. The procedure and forms need to include clear options for “inspected and complete” and “inspected but follow up needed.”

2.4 Root Cause

Root Cause

Teaching Exercise Two
CIP-004-6 R4

Present incomplete examples and demonstrate how to complete them

2.4 Root Cause

Original Root Cause

The cause of the noncompliance was a lack of internal controls and insufficient training. Sunbear failed to review access requests to verify that required business justifications were included. Furthermore, awareness training for those responsible for requesting or processing access requests did not contain business justification requirements.

2.4 Root Cause

Improved Root Cause

The cause of the noncompliance was a lack of internal controls and insufficient training. Sunbear failed to review access requests to verify that required business justifications were included. Although the process requires managers to ensure business justifications for all user access provisions, the workflow managed system used to process requests did not contain indicators and a required field that a business justification was required. Furthermore, awareness training for those responsible for requesting or processing access requests did not contain business justification requirements.

2.4 Root Cause—Example 3

Root Cause

Peer Review Exercise Three

VAR-002-4.1 R3

Review root cause analysis and participants identify deficiencies

2.4 Root Cause—Example 3

Original Causal Statement

- Sunbear's compliance group and SMEs performed a root cause analysis and determined that the day-shift operator did not notice the AVR alarm, even though the alarm activated and was displayed as designed on the operations screen. At the time of the alarm, the day shift operator was on the phone with Sunbear's TOP receiving an operating instruction. Sunbear determined that reduced staffing contributed to the issue, because they had only one day-shift operator, instead of two, monitoring the operations screens when this occurred.
- Sunbear is reviewing its operations procedures and will adjust operational priorities to ensure two day-shift operators are available to monitor the operations screens.
- The extenuating circumstances involved an Operating Instruction coming from the TOP at the same time the AVR unexpectedly changed status, and Sunbear was short one operator because a day-shift operator got ill on watch and their replacement had not yet arrived.

2.4 Root Cause—Example 3

Improved Causal Statement

- Sunbear's compliance group and SMEs performed a root cause analysis and determined that the day-shift operator did not notice the AVR alarm, even though the alarm activated and was displayed as designed on the operations screen. At the time of the alarm, the day-shift operator was on the phone with Sunbear's TOP receiving an operating instruction. The alarm was indexed off the screen by other alarms by the time the day-shift operator returned to his operating screen. Additionally, there was no audible component to the AVR alarm, and the alarm did not re-alarm after the day-shift operator failed to acknowledge it. Therefore, the root cause was determined to be incorrect alarm configuration. Sunbear also determined that reduced staffing contributed to the issue, because they had only one day-shift operator, instead of two, monitoring the operations screens when this occurred.
- Because of this noncompliance, Sunbear realized that other critical alarms, not necessarily related to NERC standards, may not be correctly configured. Sunbear is going to do a full review of all its operational and compliance-related critical alarms.
- Sunbear had an alarm in place, but it lacked the needed configuration to make it an effective internal control. Sunbear needs to configure the alarm to stay on the alarm screen until it is acknowledged, add an audible component to the alarm, and configure automatic, external notification capabilities to make sure the alarm is effective at ensuring reliability and compliance. Sunbear is also reviewing its operations procedures and will adjust operational priorities to ensure two day-shift operators are available to monitor the operations screens.
- The extenuating circumstances involved an Operating Instruction coming from the TOP at the same time the AVR unexpectedly changed status, and Sunbear was short one operator because a day-shift operator got ill on watch and their replacement had not yet arrived.

2.4 Root Cause—Example 4

Root Cause Review

Peer Review Exercise Four

CIP-007-6 R2

Review a root cause analysis and participants identify deficiencies.

Section 2.4—Example 4

Original Causal Statement

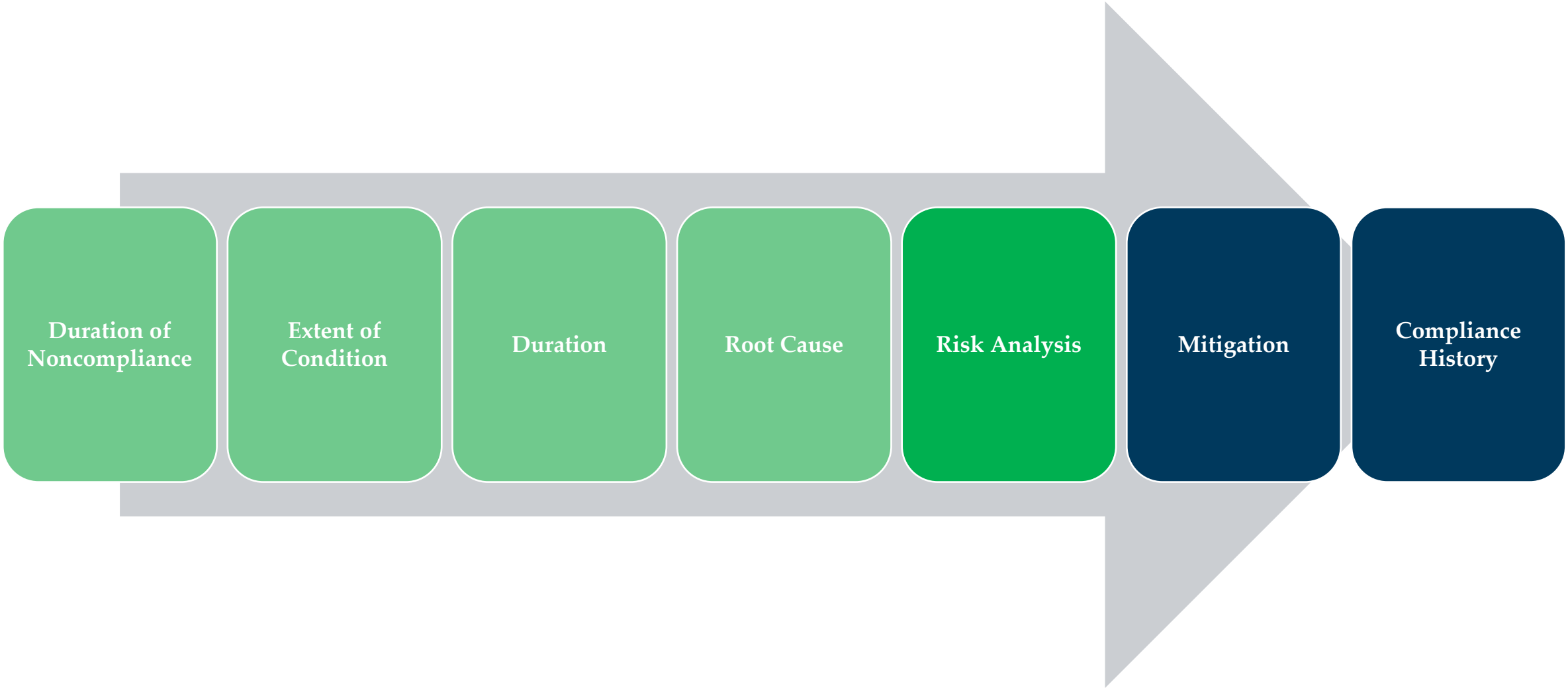
- The root cause of the noncompliance was Sunbear's deficient process. Sunbear's process did not require the technician responsible for patching to check and populate the necessary security patch mitigation documentation records when Sunbear's vulnerability assessment tool was down.
- Another contributing cause was Sunbear's vulnerability assessment tool outages. Sunbear's vulnerability assessment tool was down six times in the first calendar quarter of 2023 due to intermittent outages caused by issues associated with the maintenance activities of the provider of the vulnerability assessment tool.

Section 2.4—Example 4

Improved Causal Statement

- The root cause of the noncompliance was Sunbear's deficient process. Sunbear's process did not require the technician responsible for patching to check and populate the necessary security patch mitigation documentation records when Sunbear's vulnerability assessment tool was down.
- Sunbear indicated that not considering a vulnerability assessment tool outage was an oversight when it created its patching process, so it had not built in a step for this contingency in its process, nor had it built in any preventive/detective controls to ensure patches were installed once they were evaluated. The lack of internal controls is a contributing cause.
- Another contributing cause was Sunbear's vulnerability assessment tool outages. Sunbear's vulnerability assessment tool was down six times in the first calendar quarter of 2023 due to intermittent outages caused by issues associated with the maintenance activities of the provider of the vulnerability assessment tool.
- Sunbear's vulnerability assessment tool provider would not provide specifics on the causes of the outages, but the provider stated that it has both created redundancy and resolved the issues causing the outages. There have been no further outages since the first quarter of 2023.

2.4 Root Cause



WECC

Electric Reliability and Security for the West

www.wecc.org

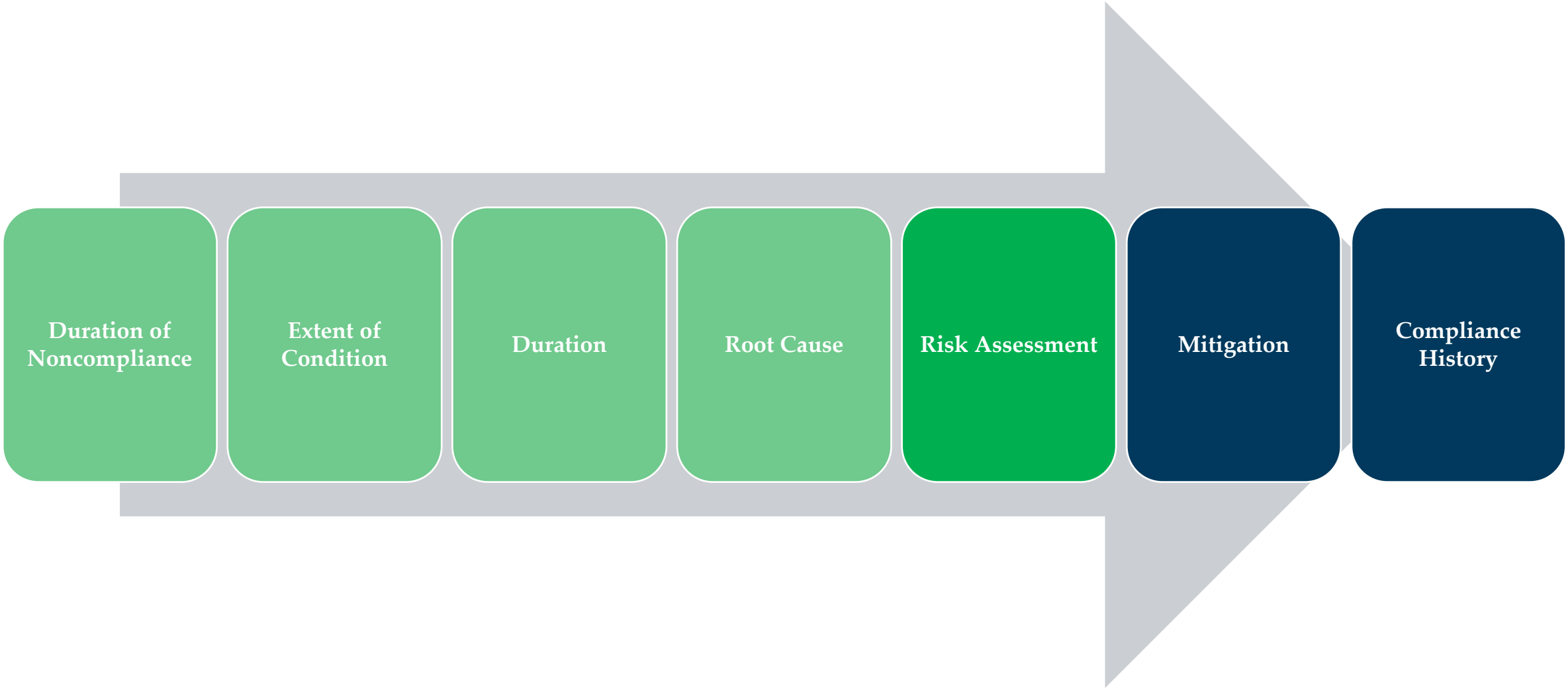
WECC

WECC Enforcement Training:

2.5 Risk Assessment

WECC Enforcement Staff

2.5 Risk Assessment



Section Learning Plan

1

Conceptual Foundation

- Application of concept to non-NERC situations

2

Teaching Exercises

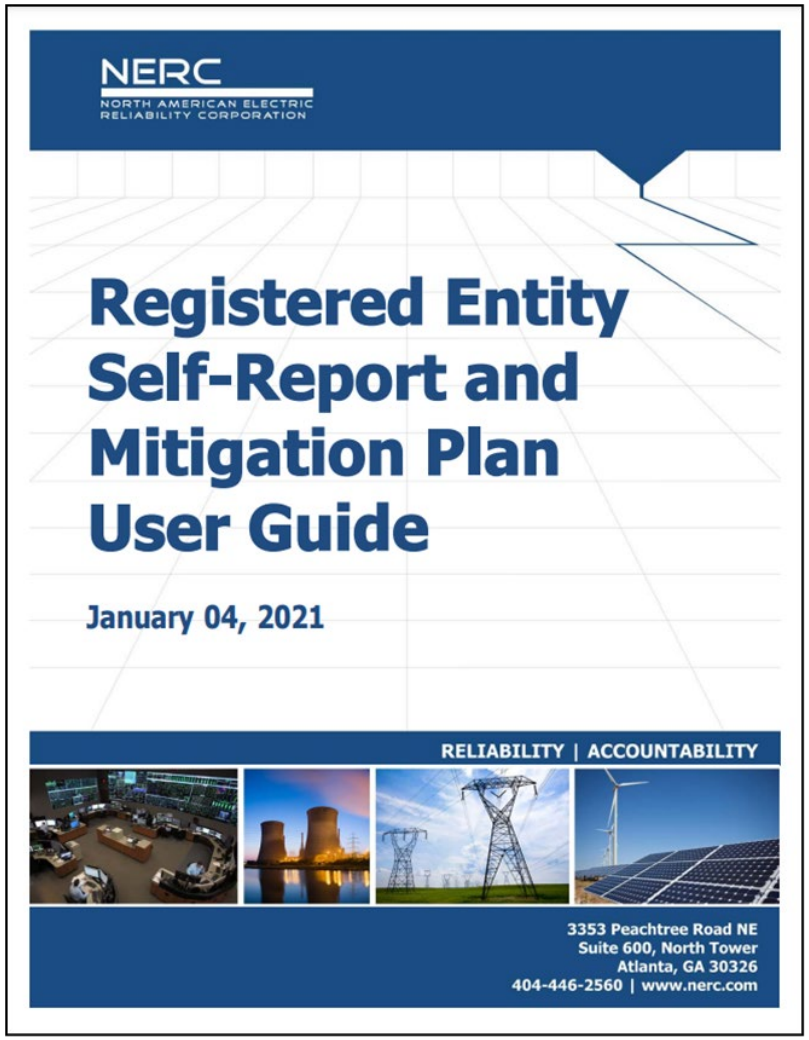
- Present incomplete examples and then demonstrate how to complete them
- FAC-003-4 & CIP-004-6

3

Peer Review Exercises

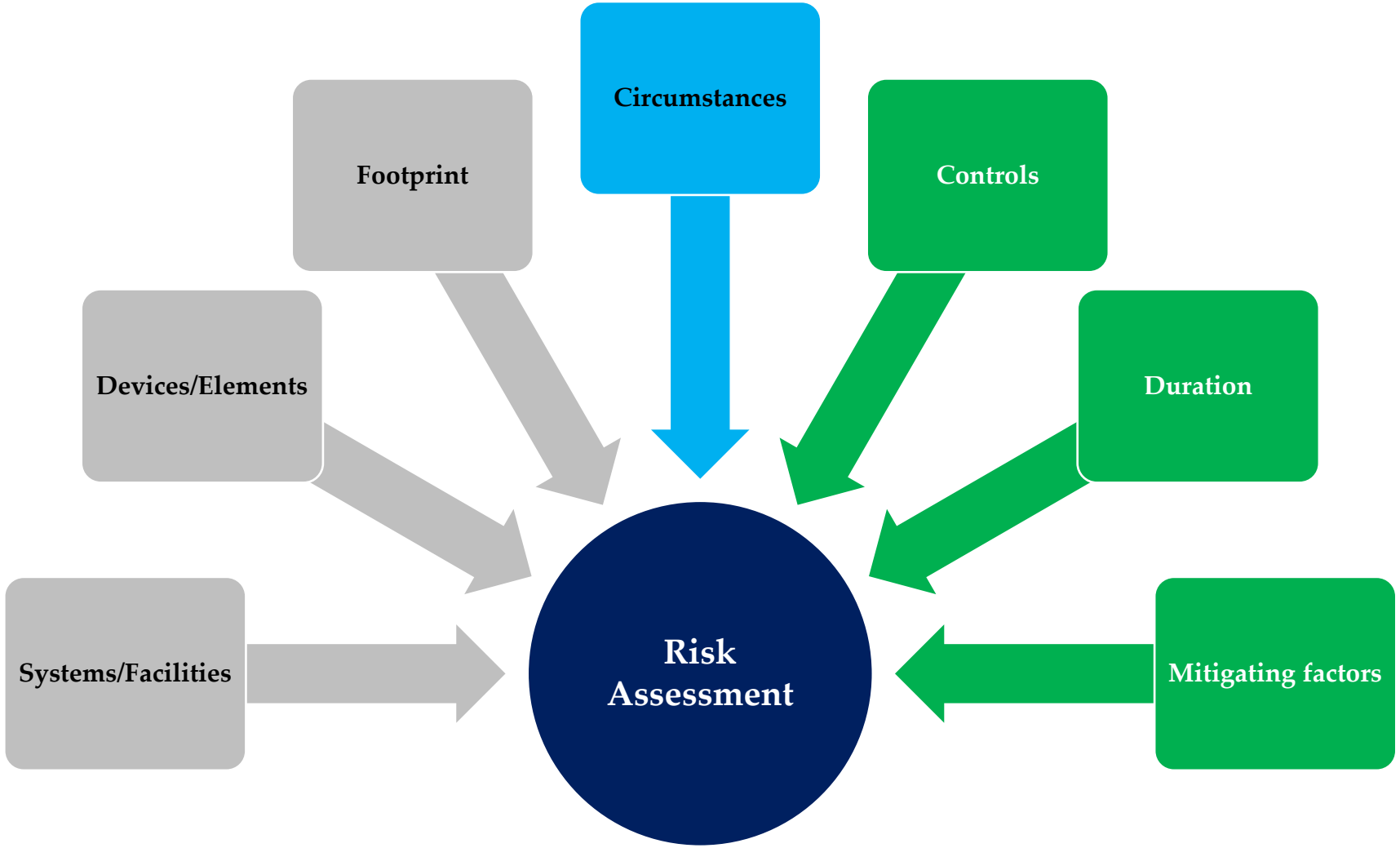
- Review noncompliance descriptions and participants identify deficiencies
- VAR-002-4.1 & CIP-007-6

2.5 Risk Assessment



"Risk is the potential impact to reliability or security multiplied by the likelihood of that impact occurring. Risk assessment involves reviewing the negative consequence or the potential impact of the event and the likelihood that the event will occur, based on the internal controls in place at the time the noncompliance occurred as well as the inherent risk of the registered entity."

2.5 Risk Assessment



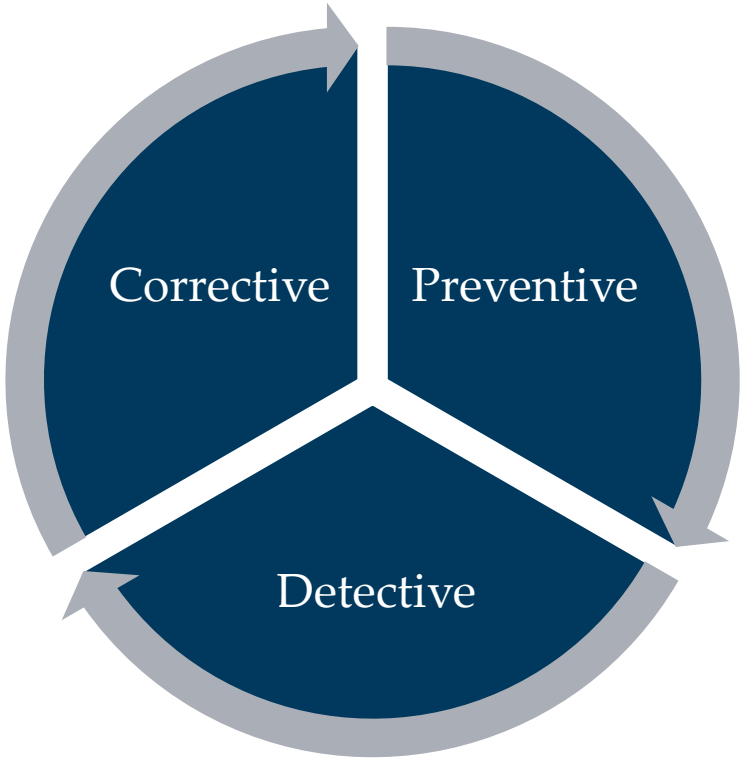
Risk Determination

- Evaluate potential impact or harm that could have occurred
- Determine the likelihood that the potential impact could occur
- Consider mitigating factors that would have reduced the likelihood of the potential impact
- Consider any internal controls that were in place at the time that expedited the discovery, shortened the duration, or reduced the severity of the impact of the noncompliance

2.5 Risk Assessment

- If the risk is moderate or serious, Registered Entities should include information to explain why the risk was not:
  - Elevated in the case of moderate
  - Lower in the case of serious
- Entities should base risk assessments on facts existing at the time of the noncompliance, not on assumptions or facts that develop later.
- Nevertheless, if an entity identifies relevant information during its extent of condition review or mitigation, it should include that information in its risk assessment.

Factors Reducing the Risk



If there were internal controls in place, the registered entity should describe how effective the entity's policies, procedures, etc. were at preventing, detecting, and correcting the noncompliance before the harm manifested.

A control could be a process, procedure, system, or a tool implemented automatically or manually. Controls will vary from entity to entity because no two entities are alike in system design, configuration, program, business plans, and functions performed.

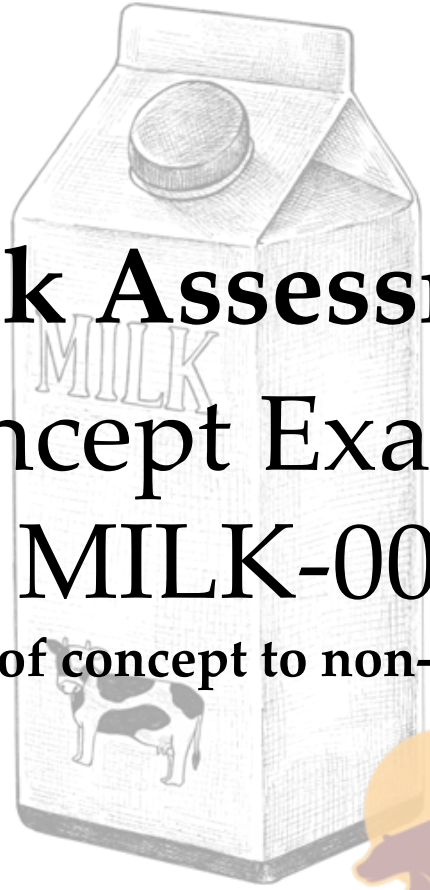
Some examples of controls are:

- A peer review process
- An automatic notification
- Frequency and voltage alerts
- A generation startup checklist
- Internal audit programs

Risk of Possible Recurrence

- Is the cause of the noncompliance the same as or similar to prior instances of noncompliance?
- Are the circumstances surrounding the noncompliance rare or common?
- What remediation steps are already in place to address the issue?
- What controls will the entity put into place to reasonably prevent recurrence?

Section 2.5—Concept Example



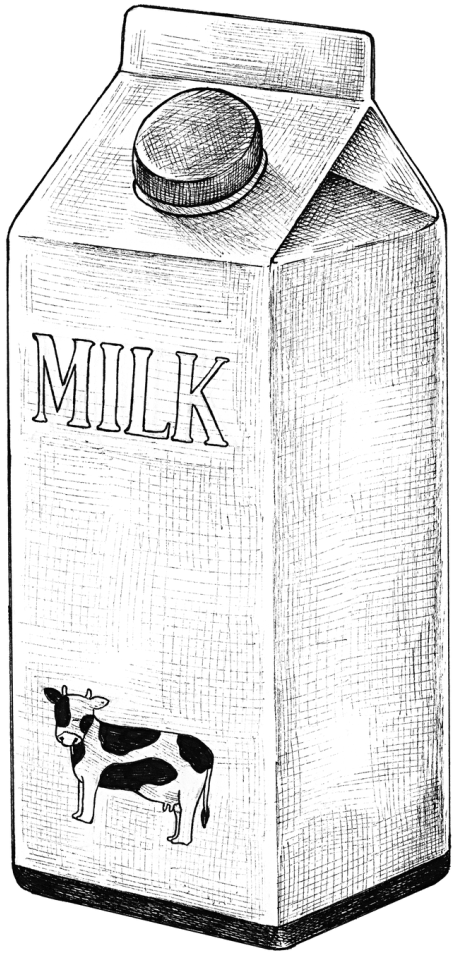
Risk Assessment

Concept Example

MILK-001

Application of concept to non-NERC situation

2.5 Risk Assessment

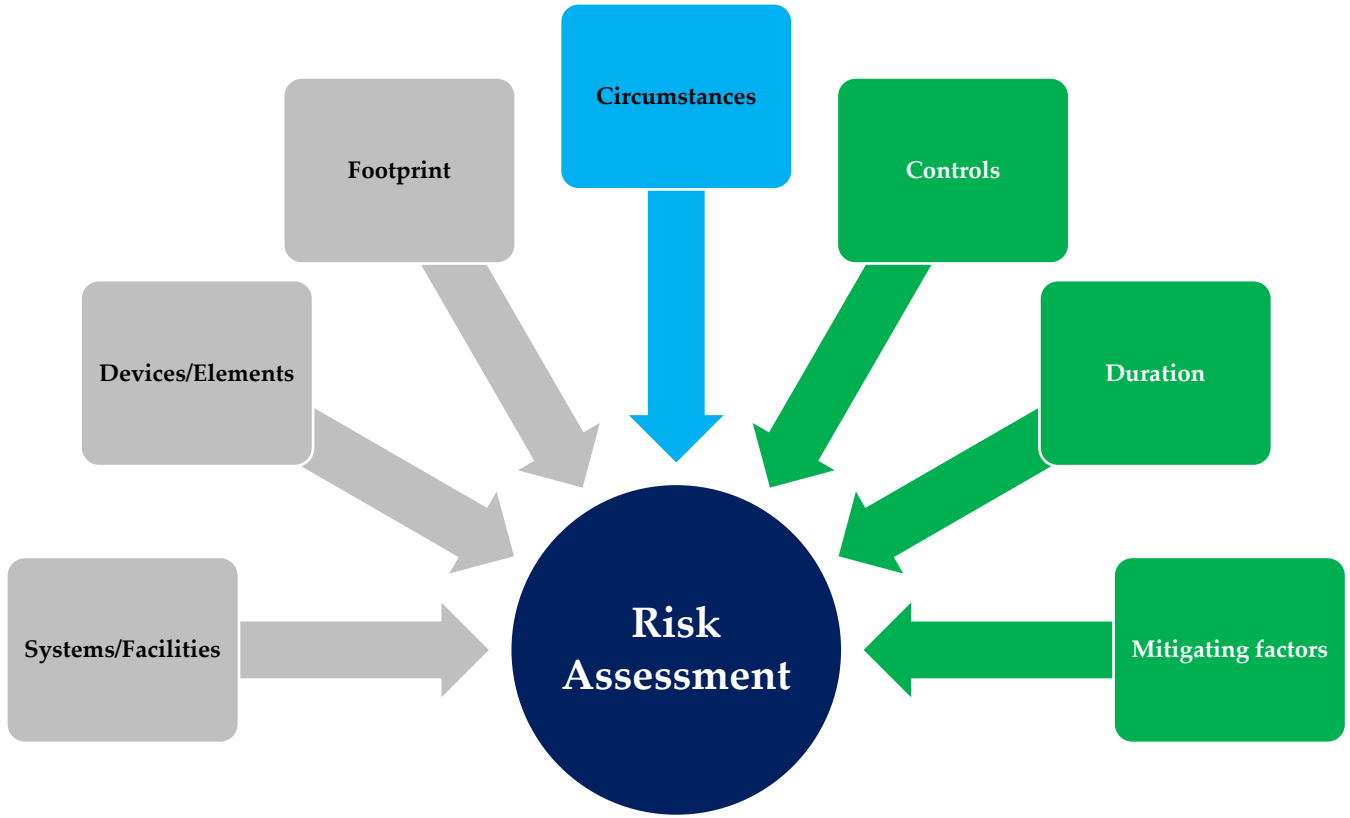


Food Standard:

SNBR-MILK-001

Pasteurized milk must be discarded on or before the expiration date listed on each carton.

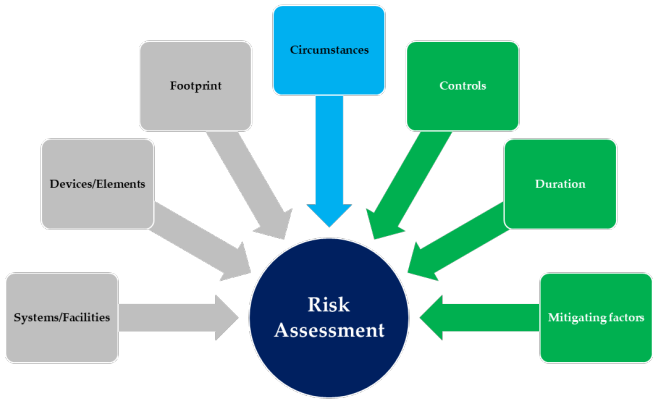
Risk Assessment



Original Risk Assessment

The risk is determined to be minimal because the milk in the small break room refrigerator is seldomly used by Sunbear employees.

Risk Assessment



Improved Risk Assessment

The risk is determined to be minimal.

Spoiled milk could potentially result in employees getting sick and an impact in operation resources. The resulting absences may cause fatigue for remaining staff, increasing the likelihood of human errors. Extended or wide-spread absences could also result in a failure to meet critical compliance filing deadlines.

However, the inherent risk of the violation was reduced due to the following factors:

1) Only 7% of employees use the refrigerator that was unplugged. Only 40% of all employees consume milk. No Sunbear employees were affected by this violation.
2) Employees have human detective controls to identify spoiled milk based on its odor, consistency, and color before consumption. Spoiled milk was discovered early Monday morning after the refrigerator had been unplugged over the weekend.
3) Food safety standards allow up to two weeks of safe consumption past the “sell by” date when stored at safe temperatures.

2.5 Risk Assessment

Risk Assessment

Teaching Exercise One

FAC-003-4 R2

Present an incomplete example and then demonstrate how to complete it

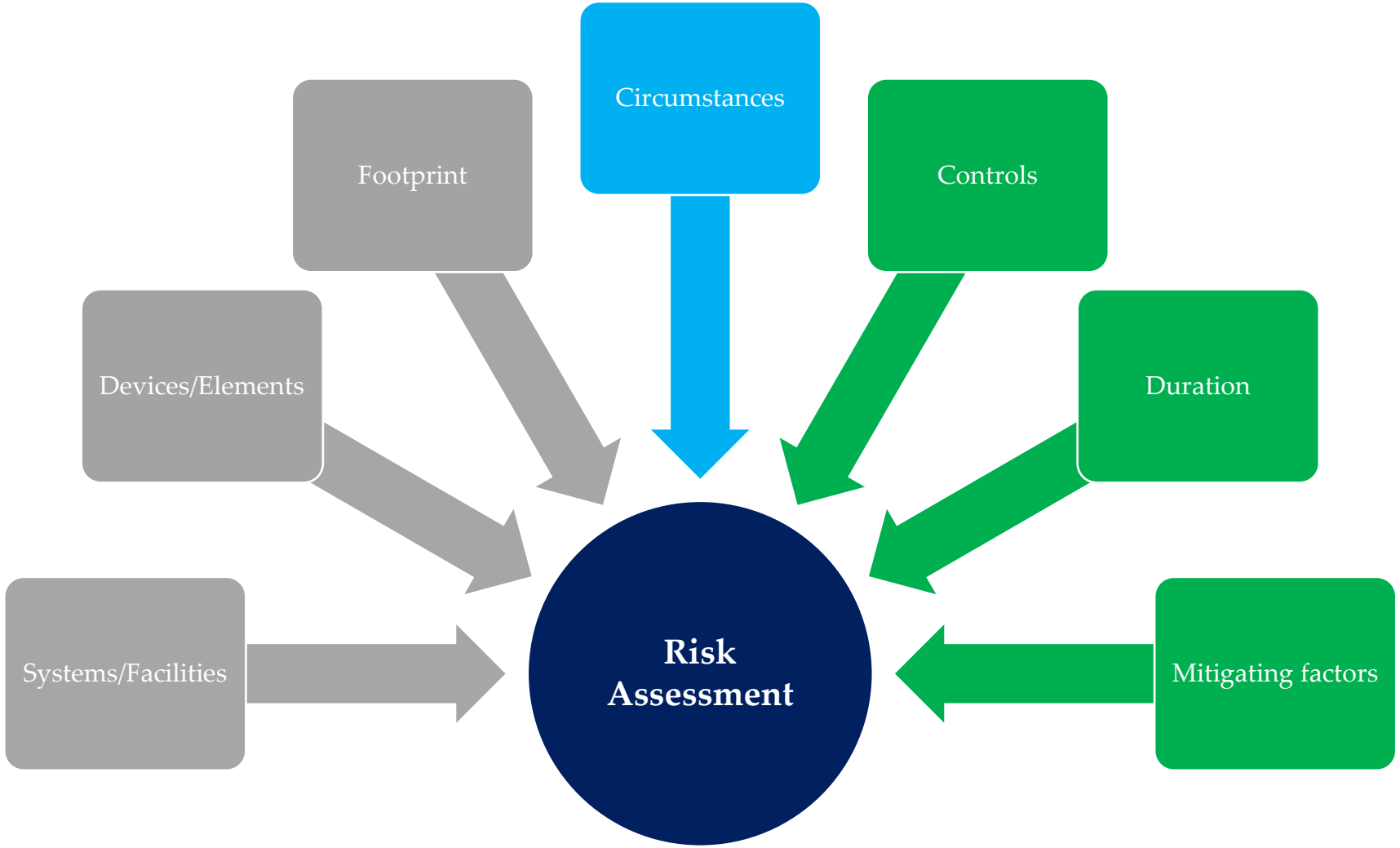
Risk Assessment

Original Risk Assessment

The violation posed a moderate risk to the reliability of the bulk power system. Improper vegetation management that causes an unplanned Sustained Outage could result in higher risk to system conditions or loss of load. The likelihood of the impact was reduced because the line tripped and reclosed as designed, which resulted in a momentary outage.

In the event of a Sustained Outage, the entity was able to demonstrate Operating Plans that would have mitigated operating above the normal ratings of their facilities. Due to the identified gap in controls, it is possible that there are other instances where a line was inspected, additional ground inspection was required, but the additional inspection was not completed. Prior documentation showed this gap only existed in inspection logs beginning in 2017; thereby limiting the scope of the identified gap.

2.5 Risk Assessment



Risk Assessment

Improved Risk Assessment

The violation posed a moderate risk to the reliability of the bulk power system. Improper vegetation management that causes an unplanned Sustained Outage could result in higher risk to system conditions or loss of load. The likelihood of the impact was reduced because the line tripped and reclosed as designed, which resulted in a momentary outage. Automatic reclosing operated as designed, restoring the line to service in five seconds, limiting any impact to the 230 kV system. This line was neither an element of an IROL nor an element of a Major WECC Transfer Path.

In addition, the momentary loss of the line did not result in an exceedance of any SOLs. The line was loaded at 20% at the time of the fault and nearby facilities operated within normal ratings. Further, in the event of a Sustained Outage, the entity was able to demonstrate Operating Plans that would have mitigated operating above the normal ratings of their facilities. Due to the identified gap in controls, it is possible that there are other instances where a line was inspected, additional ground inspection was required, but the additional inspection was not completed. Prior documentation showed this gap only to exist in inspection logs beginning in 2017; thereby limiting the scope of the identified gap.

2.5 Risk Assessment

Risk Assessment

Teaching Exercise Two

CIP-004-6 R4

Present an incomplete example and then demonstrate how to complete it

Risk Assessment

Original Risk Assessment

This noncompliance posed a minimal risk to the reliability of the Bulk Power System. A failure to fully implement one or more documented access management programs could have resulted in unauthorized access and changes to Sunbear's Control Center's HIBCS, leading to a misoperation or intentional tampering with critical parts of the BPS. Sunbear is a large TOP with approximately 2,300 miles of 500 kV and 1,500 miles of 350 kV transmission lines.

However, no actual impact occurred because all original access requests were authorized before access was granted. Those authorizing access were aware of job functions and associated business needs. Thus, the lack of documented business justification was a documentation oversight. No harm is known to have occurred.

Risk Assessment

Improved Risk Assessment

This noncompliance posed a minimal risk to the reliability of the Bulk Power System. A failure to fully implement one or more documented access management programs could have resulted in unauthorized access and changes to Sunbear's Control Center's HIBCS, leading to a misoperation or intentional tampering with critical parts of the BPS. Sunbear is a large TOP with approximately 2,300 miles of 500 kV and 1,500 miles of 350 kV transmission lines.

However, in all instances, the access was determined to be necessary and authorized, and there were no instances that were inappropriate or unauthorized identified during the extent of condition review. No actual impact occurred because all original access requests were authorized before access was granted. All access was subject to periodic reviews to ensure individuals retained only the minimum access necessary to perform their job functions. Those authorizing access were aware of job functions and associated business needs, which resulted in proper authorization in all instances. Thus, the lack of documented business justification was a documentation oversight. No harm is known to have occurred.

2.5 Risk Assessment—Example 3

Risk Assessment

Peer Review Exercise Three

VAR-002-4.1 R3

Review a Risk Assessment and participants identify deficiencies

Section 2.5—Example 3

Original Risk Assessment

- The potential harm is assessed as minor. Failure to inform the TOP of changes in AVR status could have resulted in Sunbear's TOP being unaware of Sunbear's inability to provide the expected voltage control.
- However, the likelihood of the impact occurring was minimal due to the following factors:
  - Sunbear stayed within the voltage schedule requirements of its TOP during the 55 minutes of noncompliance, so no harm is known to have occurred.
  - The unit 3 AVR was still in service in manual mode, which would have allowed Sunbear to manually change the voltage output of unit 3 if needed.
  - The duration of this noncompliance was short, less than one hour.

Section 2.5—Example 3

Improved Risk Assessment

- The potential harm is assessed as minor. Failure to inform the TOP of changes in AVR status could have resulted in Sunbear's TOP being unaware of Sunbear's inability to provide the expected voltage control.
- Sunbear's total generation footprint is 5 generating units totaling 1000MW.
- However, the likelihood of the impact occurring was minimal due to the following factors:
- Unit 3 has a generating capacity of 200 MW and represents 5% of the generating capacity attached to Sunbear's TOP's transmission system. At the time of the noncompliance unit 3 was producing 120MW. The other four units were online with AVR in automatic mode and producing 800 MW.
- Sunbear stayed within the voltage schedule requirements of its TOP during the 55 minutes of noncompliance, so no harm is known to have occurred.
- Sunbear has audible alarms for voltage limits in the control room for Low Warning, Low Alert, High Warning and High Alert.
- The unit 3 AVR was still in service in manual mode, which would have allowed Sunbear to manually change the voltage output of unit 3 if needed.
- The duration of this noncompliance was short, less than 1 hour.

Section 2.5—Example 3

Improved Risk Assessment

- The potential harm is assessed as minor. Failure to inform the TOP of changes in AVR status could have resulted in Sunbear's TOP being unaware of Sunbear's inability to provide the expected voltage control.
- Sunbear's generation footprint is small with 5 generating units totaling 1000MW.
- However, the likelihood of the impact occurring was minimal due to the following factors:
- Unit 3 has a generating capacity of 200 MW and represents 5% of the generating capacity attached to Sunbear's TOP's transmission system. At the time of the noncompliance unit 3 was producing 120MW. The other four units were online with AVR in automatic mode and producing 800 MW.
- Sunbear stayed within the voltage schedule requirements of its TOP during the 55 minutes of noncompliance, so no harm is known to have occurred.
- Sunbear has audible alarms for voltage limits in the control room for Low Warning, Low Alert, High Warning and High Alert.
- The unit 3 AVR was still in service in manual mode, which would have allowed Sunbear to manually change the voltage output of unit 3 if needed.
- The duration of this noncompliance was short, less than 1 hour

Mitigating Factors

2.5 Risk Assessment—Example 4

Risk Assessment

Peer Review Exercise Four

CIP-007-6 R2

Review a Risk Assessment and determine deficiencies.

Section 2.5—Example 4

Original Risk Assessment

The potential risk to the BPS was substantial because the security patch was associated with 25 BES Cyber Assets (BCA), including EMS, SCADA, and ICCP servers associated with HIBCS within the primary Control Center and associated Data Center.

Failure to maintain patches could have resulted in security vulnerabilities which could be used to compromise BCSs. However, the likelihood of the impact occurring was low due to the following:

- All BCAs are located within a defined Electronic Security Perimeter (ESP) behind an Electronic Access Point that controls inbound and outbound communication.
- Sunbear implements Interactive Remote Access using an Intermediate System with dual-factor authentication and encryption.
- All BES Cyber Assets at issue were located within a Physical Security Perimeter with access controlled by a card reader.
- The BCAs also require dual-factor authentication.
- The duration was approximately six months.
- No harm is known to have occurred.

Section 2.5—Example 4

Improved Risk Assessment

The potential risk to the BPS was substantial because the security patch was associated with 25 BES Cyber Assets (BCA), including EMS, SCADA, and ICCP servers associated with HIBCS within the primary Control Center and associated Data Center, and the security patches were addressing high risk vulnerabilities. Sunbear has 45 BCAs, 10 PCAs, 36 EACMS and 10 PACS associated with Sunbear's HIBCS.

Failure to maintain patches could have resulted in security vulnerabilities which could be used to compromise BCSs. However, the likelihood of the impact occurring was low due to the following:

- All BCAs at issue were compliant with other applicable CIP requirements
- All BCAs are located within a defined Electronic Security Perimeter (ESP) behind an Electronic Access Point that controls inbound and outbound communication.
- Sunbear implements Interactive Remote Access using an Intermediate System with dual-factor authentication and encryption.
- Vendor remote access requires assistance from an Entity authorized user that has the capability to disconnect the vendor at any time.
- All BES Cyber Assets at issue were located within a Physical Security Perimeter with access controlled by a card reader.
- The BCAs also require dual-factor authentication.
- No harm is known to have occurred.
- The duration was approximately six months.

Section 2.5—Example 4

Improved Risk Assessment

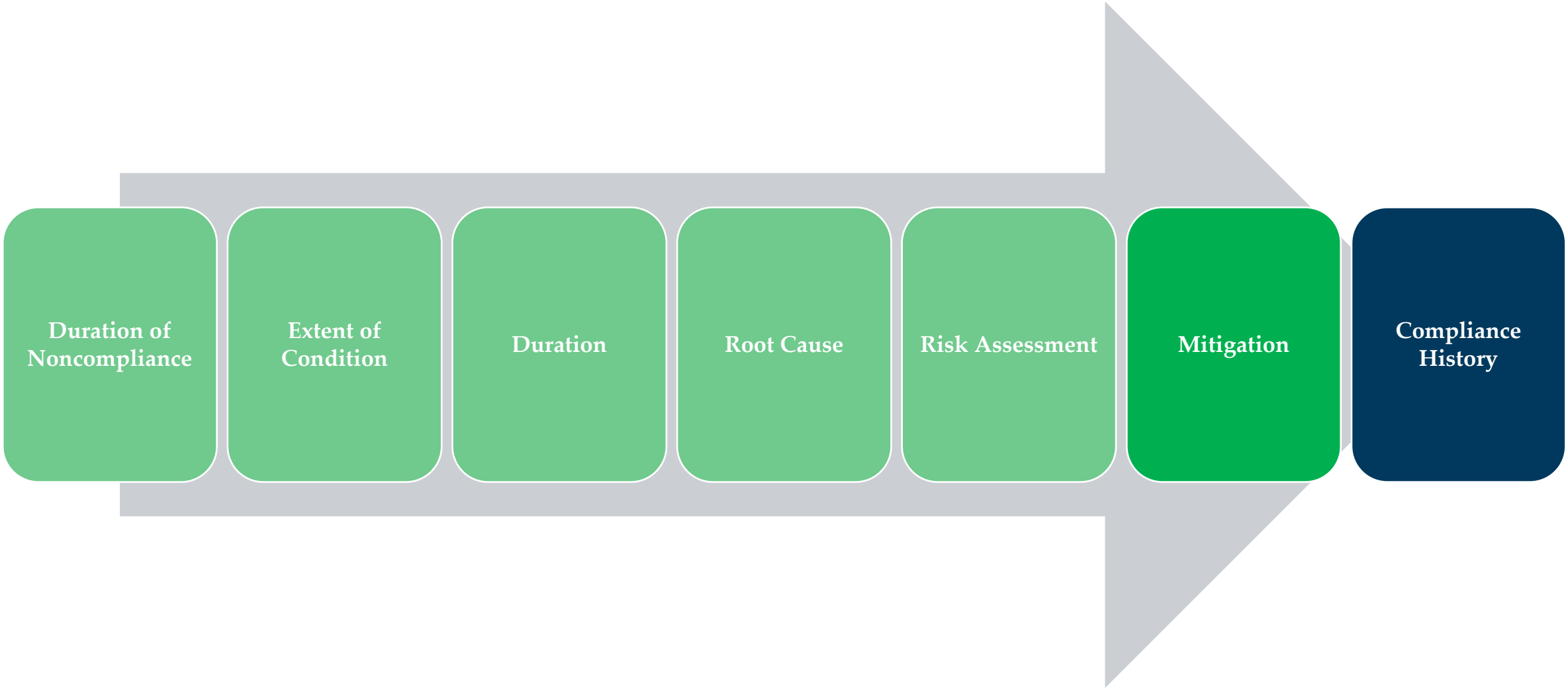
The potential risk to the BPS was substantial because the security patch was associated with 25 BES Cyber Assets (BCA), including EMS, SCADA, and ICCP servers associated with HIBCS within the primary Control Center and associated Data Center, and the security patches were addressing high risk vulnerabilities. Sunbear has 45 BCAs, 10 PCAs, 36 EACMS and 10 PACS associated with Sunbear's HIBCS.

Failure to maintain patches could have resulted in security vulnerabilities which could be used to compromise BCSs. However, the likelihood of the impact occurring was low due to the following:

- All BCAs at issue were compliant with other applicable CIP requirements
- All BCAs are located within a defined Electronic Security Perimeter (ESP) behind an Electronic Access Point that controls inbound and outbound communication.
- Sunbear implements Interactive Remote Access using an Intermediate System with dual factor authentication and encryption.
- Vendor remote access requires assistance from an Entity authorized user that has the capability to disconnect the vendor at any time.
- All BES Cyber Assets at issue were located within a Physical Security Perimeter with access controlled by a card reader.
- The BCAs also require dual-factor authentication.
- No harm is known to have occurred.
- The duration was approximately six months.

Mitigating Factors

2.5 Risk Assessment



WECC

Electric Reliability and Security for the West

www.wecc.org

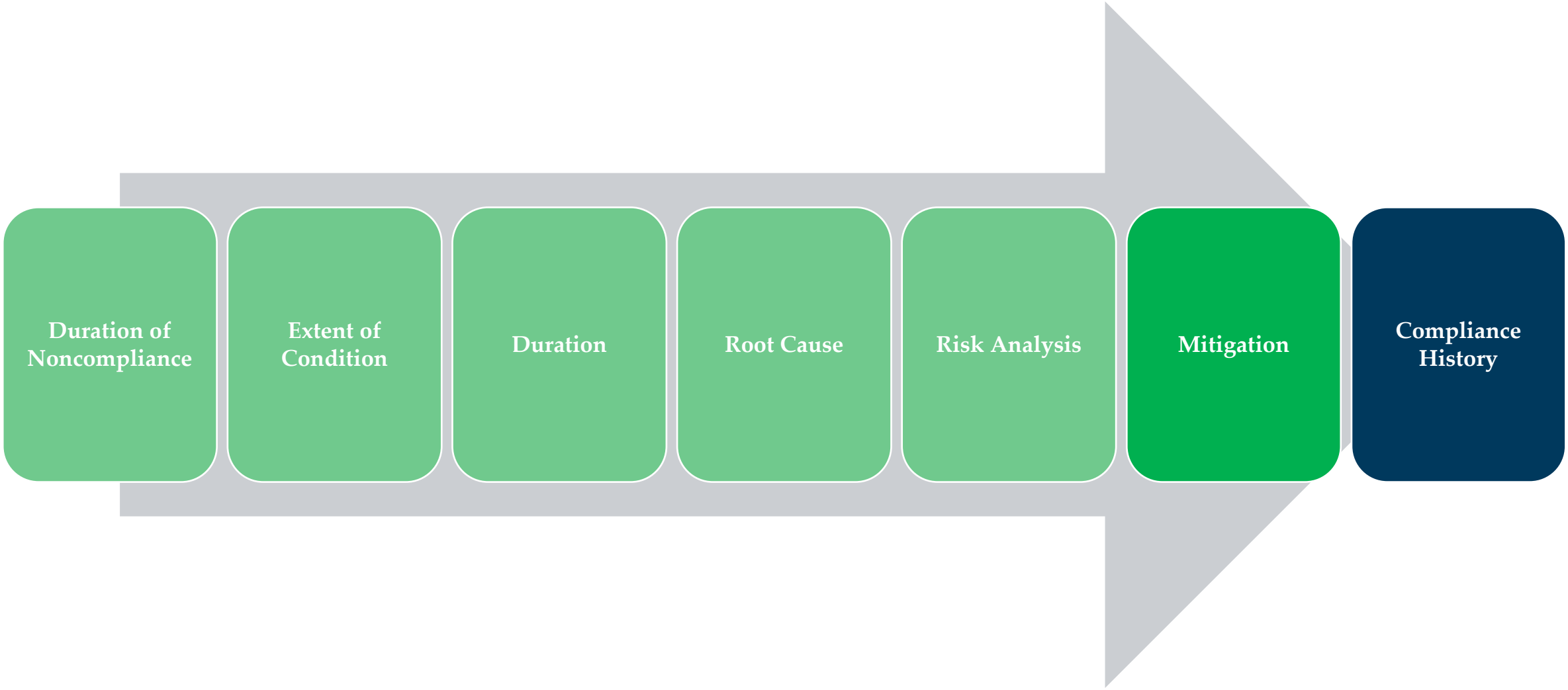
WECC

WECC Enforcement Training:

2.6 Mitigation

WECC Enforcement Staff

2.6 Mitigation



Section Learning Plan

1

Conceptual Foundation

- Application of concept to non-NERC situations

2

Teaching Exercises

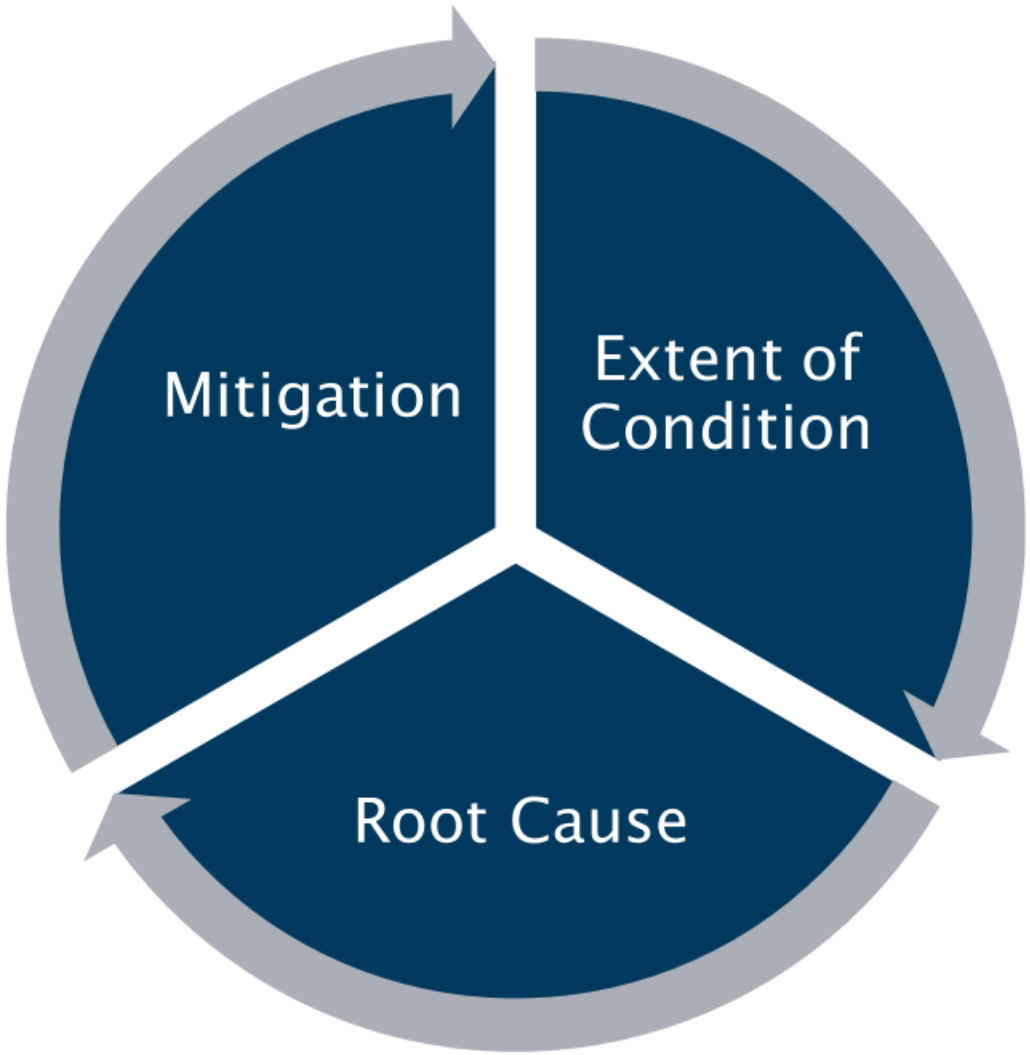
- Present incomplete examples and then demonstrate how to complete them
- FAC-003-4 & CIP-004-6

3

Peer Review Exercises

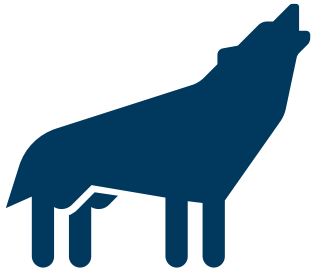
- Review noncompliance descriptions and participants identify deficiencies
- VAR-002-4.1 & CIP-007-6

Essential Interplay



2.6 Mitigation

Conceptual Foundation: Mitigation of K9 Coworkers


2.6 Mitigation—Conceptual Foundation

WECC Enforcement's K9 Investigation Team

2.6 Mitigation—Conceptual Foundation

K9 Coworker Internal Controls

Prevent

- Establish Physical Security Perimeter
- Exercise routine
- Mute button

Detect

- Audio headsets
- Video cameras
- Black light inspections

Correct

- Spray bottle to interrupt barking
- Angry voice
- Carpet cleaner

2.6 Mitigation

Internal Controls that are designed or enhanced during mitigation can:

- Increase reliability and security by improving processes and procedures;
- Identify emerging or potential risks in other areas;
- Identify gaps in related processes that can be improved to increase reliability and security;
- Inform the Compliance Enforcement Authority's development of the Registered Entity's Compliance Oversight Plan; and
- Reduce audit burden by providing justification for a continuous monitoring process rather than an audit or other periodic event-monitoring activities.

Types of Mitigating Activities

- Remediating Action: An action taken to return to compliance for this PNC.
- Corrective Control: a mechanism to mitigate damage once an operational risk event has occurred.
- Preventative Control: a mechanism to keep errors or irregularities from occurring in the first place. At least one preventative control should address each cause identified.
- Detective Control: an internal control designed to identify errors or deviations from the norm.
- Other: Use this category if a milestone does not meet the criteria of any of the other types

Mitigation Minimums Requirement

- Remediating action- Must address the specific instances in the PNC
- Preventative action: What prevents reoccurance based on the root cause. Each identified root cause must be addressed. One action can address multiple root causes

Mitigating Plans vs Mitigating Activities

Plans

- Serious risk
- Long completion time (12+ months)
- Complex
- Verified complete
- Milestones <3 months apart
- Will be requested by WECC

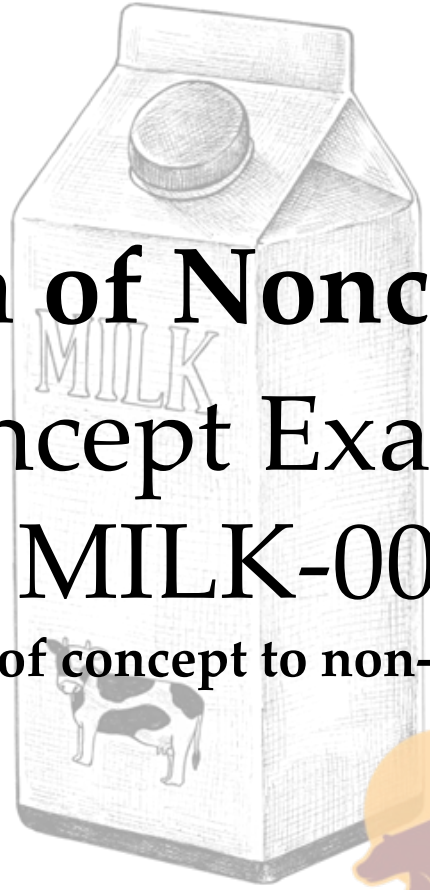
Activities

- Minimal & Moderate Risk
- Shorter (<12 months from filing)
- Sampled for completion
- Default in Align

When to Perform Mitigation

- An entity should begin performing mitigation after a potential noncompliance is identified.
- An entity must submit Mitigating Activities or a Mitigation Plan to ensure the noncompliance is fully remediated and mitigated.

Section 2.3—Concept Example



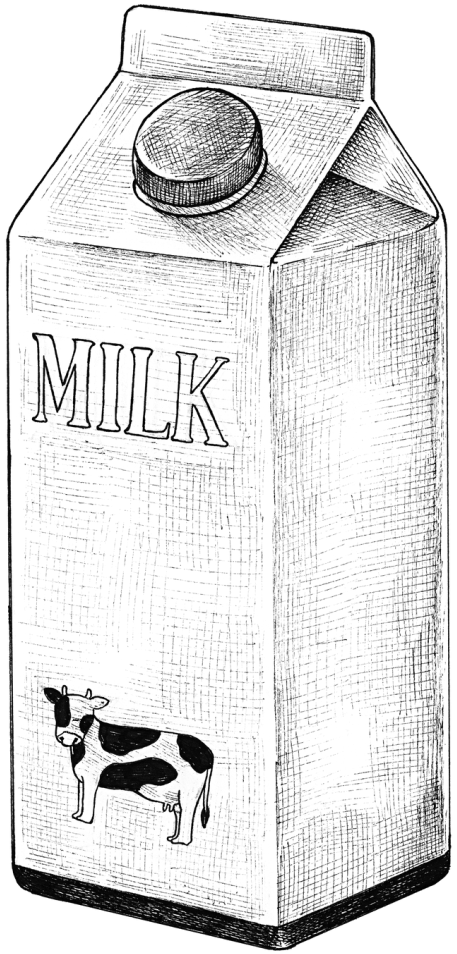
Duration of Noncompliance

Concept Example

MILK-001

Application of concept to non-NERC situation

2.6 Mitigation

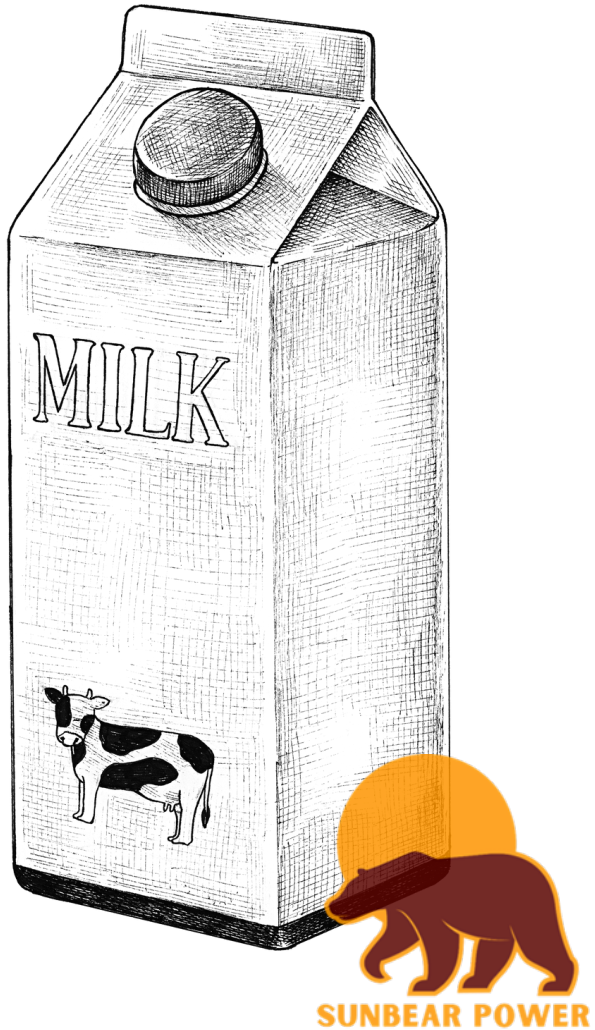


Food Standard:

SNBR-MILK-001

Pasteurized milk must be discarded on or before the expiration date listed on each carton.

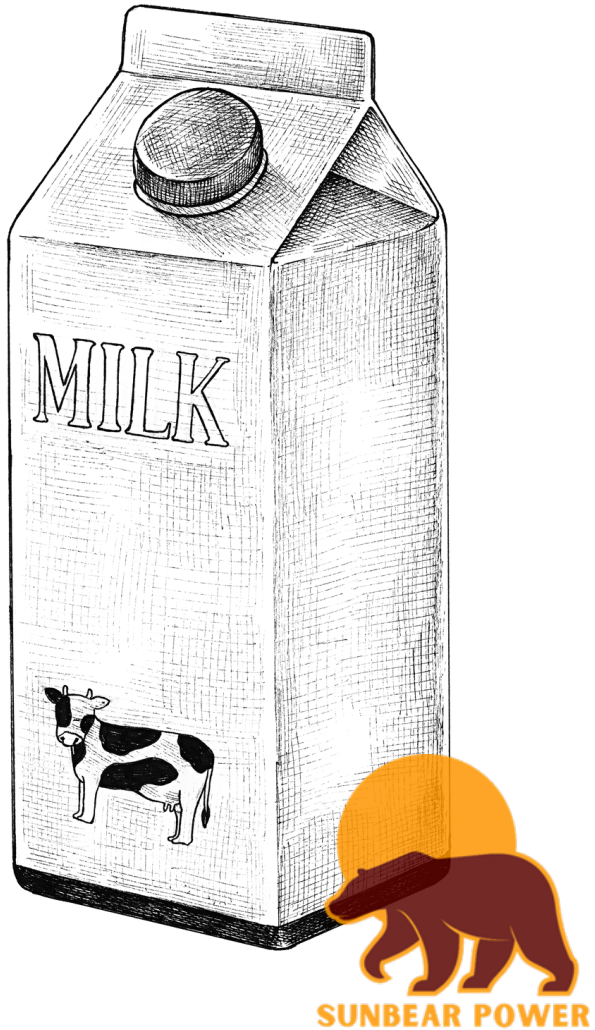
2.6 Mitigation



Original Mitigation Activities

Remediating Activity: Sunbear's dispatch center manager will talk to the janitor who cleans the small break room at its dispatch center and tell him not to unplug the refrigerator anymore.

2.6 Mitigation



Improved Mitigation Activities (minus dates)

- **Remediating Activity:** Sunbear disposed of all expired milk.
- **Preventative Control:** Sunbear will attach signs to the right corner of every refrigerator reminding everyone not to unplug the refrigerators unless they move the milk to another refrigerator.
- **Preventative Control:** Sunbear electricians installed a longer electrical cord on the refrigerator, so the janitor could move the refrigerator to clean without unplugging it.
- **Preventative Control:** Sunbear's dispatch center manager will talk to the janitor who cleans the small break room at its dispatch center and tell him not to unplug the refrigerator and let him know that a longer cord was installed.
- **Preventative Control:** the Milk Monitors manager will notify the alternate Milk Monitor if the primary Milk Monitor is unable to perform their responsibilities

2.6 Mitigation

Mitigation

Teaching Exercise One

FAC-003-4 R2

Present incomplete example and then demonstrate how to complete it

2.6 Mitigation

Original Mitigation Activities Description (minus dates)

- **Remediating Activity**: Sunbear removed the poplar tree.
- **Detective Activity**: Sunbear conducted a foot patrol inspection of the remainder of the line to see whether there were any other concerns.
- **Preventive Control**: Sunbear added an annual training requirement for a review of the FAC-003 procedures for all applicable internal staff and contractors.

2.6 Mitigation

Questions to consider

What action(s) remediated the noncompliance?

What action(s) addresses the root cause(s)?

What action(s) addresses the other cause(s)?

What other controls are being implemented to detect, prevent, or correct similar non-compliances in the future?

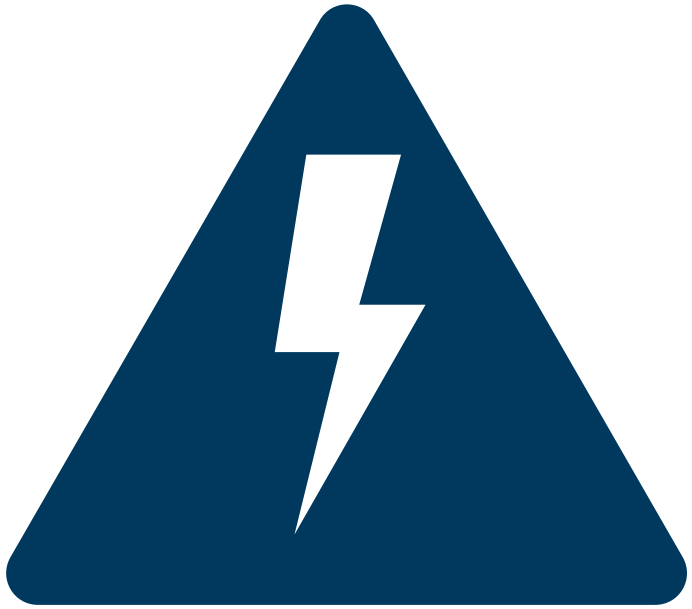
2.6 Mitigation

Improved Mitigation Activities Description (minus dates)

- **Remediating Activity:** Sunbear removed the poplar tree.
- **Detective Activity (Completing the EOC):** Sunbear conducted a review of all vegetation management records of the line.
- **Detective Activity (Completing the EOC):** After identifying the error related to aerial records, Sunbear conducted a review of all the aerial contractor's work to see if there were any other concerns that needed to have ground inspections.
- **Detective Activity (Completing the EOC):** Sunbear conducted a foot patrol inspection of the remainder of the line to see whether there were any other concerns.
- **Preventive Control:** Sunbear confirmed that the line would have the aerial as well as ground inspection for both spring and fall inspections.
- **Preventive Control:** Sunbear updated procedures to require ground inspection for all lines and to require the contractor to note all vegetation conditions. Sunbear trained its contractors and affected staff on the procedural updates.

(continued)

2.6 Mitigation



Improved Mitigation Activities Description Continued (minus dates)

- **Preventive Control:** Updated its technical specifications concerning reporting of vegetation conditions and its inspection practices. This includes the addition of a documented sign-off process.
- **Preventive and Detective Control:** Installed software that accommodates planning and implementation of annual work performance, schedules, work orders, work in progress, and reporting capabilities.
- **Preventive Control:** Sunbear added an annual training requirement for a review of the FAC-003 procedures for all applicable internal staff and contractors.

2.6 Mitigation

Mitigation

Teaching Exercise Two

CIP-004-6 R4

Present incomplete example and then demonstrate how to complete it

2.6 Mitigation

Original Mitigation Activities Description (minus dates)

- **Remediating Activity**: Provided business justifications for the 12 users that did not have a documented business justification;
- **Preventive Control**: Added an approval step where managers had to review the request and approve the content and substance of all access requests;
- **Preventive Control**: Trained all applicable employees regarding the process changes and the business justification documentation requirement; and
- **Detective Controls**: Created a quarterly task to sample and review 3% of all access requests to ensure they meet all NERC requirements.

2.6 Mitigation

Improved Mitigation Activities Description (minus dates)

- **Remediating Activity**: Provided business justifications for the 12 users that did not have a documented business justification;
- **Preventive Control**: Implemented a system enhancement to the access request system, adding a mandatory text field for business justification on all service requests;
- **Preventive Control**: Added an approval step where managers had to review the request and approve the content and substance of all access requests;
- **Preventive Control:** established an approval attestation which was added to the manager's console, which reminded managers of their responsibilities;
- **Preventive Control**: Trained all applicable employees regarding the process changes and the business justification documentation requirement and added this training to the annual training for all applicable employees; and
- **Detective Controls**: Created a quarterly task to sample and review 3% of all access requests to ensure they meet all NERC requirements.

2.6 Mitigation—Example 3

Mitigation

Peer Review Exercise Three

VAR-002

Review mitigation and participants identify deficiencies

2.6 Mitigation—Example 3

Original Mitigation Activities Description (minus dates)

- **Remediating Activity**: Sunbear's night shift operator reported the status change to Sunbear's TOP.
- **Corrective Activity**: Sunbear repaired the AVR, allowing automatic operation.
- **Preventive Activity**: Sunbear provided training to all plant operator personnel regarding VAR-002 reporting requirements and the associated changes in alarm notifications. This training also included a lesson learned with a focus on calling for additional assistance when needed.
- **Preventive Control**: Sunbear developed a new policy regarding staffing issues. Shift supervisors must inform management of staffing issues immediately and the shift supervisor must formally assign the responsibilities of unfilled roles among the other operators. Shift supervisors received additional training on how to redistribute responsibilities and what to prioritize when understaffed.

2.6 Mitigation—Example 3

Improved Mitigation Activities Description (minus dates)

- **Remediating Activity**: Sunbear's night shift operator reported the status change to Sunbear's TOP.
- **Corrective Activity**: Sunbear repaired the AVR, allowing automatic operation.
- **Preventive Activity**: Sunbear provided training to all plant operator personnel regarding VAR-002 reporting requirements and the associated changes in alarm notifications. This training also included a lesson learned with a focus on calling for additional assistance when needed.
- **Preventive Control**: Sunbear developed a new policy regarding manning issues. Shift supervisors must inform management of staffing issues immediately And the shift supervisor must formally assign the responsibilities of unfilled roles among the other operators. Shift supervisors received additional training on how to redistribute responsibilities and what to prioritize when understaffed.
- **Preventive Control**: Sunbear modified AVR status change alarms to add an audible alarm notification and to change the alarm priority to require acknowledgement of an AVR status alarm by the operator before the alarm will index off the operator's active alarm screen.
- **Preventive Control**: Sunbear added email notifications that are sent to the on-duty plant operator, the on-duty operations shift supervisor, and applicable compliance personnel each time the AVR status changes.

2.6 Mitigation—Example 4

Mitigation

Peer Review Exercise Four

CIP-007-6 R2

Review a mitigation and participants identify deficiencies.

2.6 Mitigation—Example 4

Original Mitigation Activities Description (minus dates)

1) Sunbear installed the missing security patches.
2) Sunbear updated its process to require personnel to review security patch information and manually document security patch information when the vulnerability assessment tool is down.
3) Sunbear also updated its process to add a monthly review of security patches to determine whether any patches have not been evaluated, installed, or added to a security patch mitigation plan.

2.6 Mitigation—Example 4

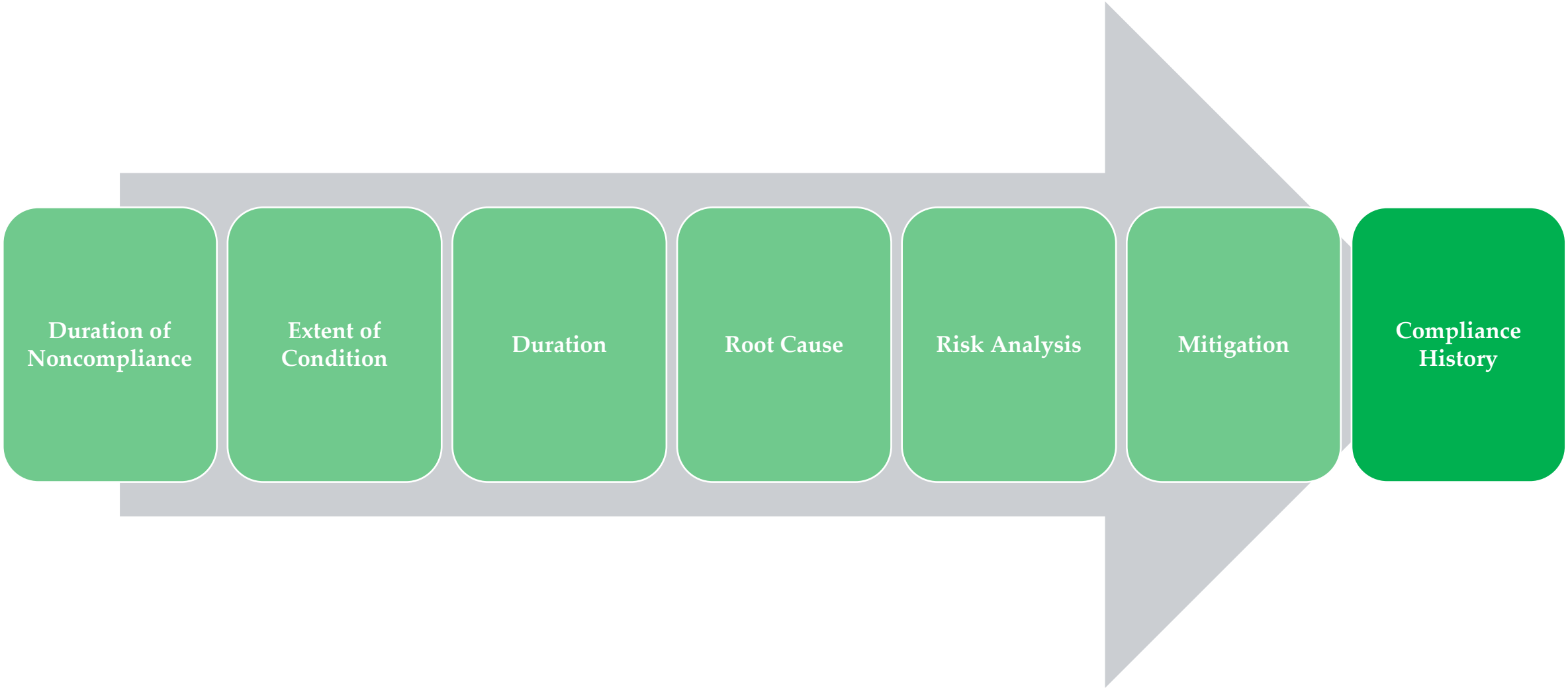
Improved Mitigation Activities Description (minus dates)

- **Remediating Activity**: Sunbear installed the missing security patches.
- **Preventive Control**: Sunbear updated its process to require personnel to review security patch information and manually document security patch information when the vulnerability assessment tool is down.
- **Preventive Control**: Sunbear trained all its personnel on the updated process.
- **Detective Control**: Sunbear also updated its process to add a monthly review of security patches to determine whether any patches have not been evaluated, installed, or added to a security patch mitigation plan.
- **Preventive Control**: Sunbear worked with its vulnerability assessment tool provider to gain assurances that the first quarter outages were anomalies and that Sunbear's vulnerability assessment tool provider had taken appropriate corrective action, including installing redundancy and fixing the issues that caused the outages.

Known Best Practices

- Ensuring that controls are appropriately mapped to applicable Reliability Standards and Requirements to ensure reliability and security of the BES
- Including how applicable employees are informed of changes to procedures
- Including detailed control descriptions in compliance and controls programs documentation
- Linking implemented controls to documentation on objectives and related risks
- Retaining documentation supporting the operation of internal controls such that the design and operating effectiveness of internal controls can be demonstrated and evaluated
- Entities should consider an independent review and evaluation of their internal controls and other compliance activities related to the reliability and security of the BES

2.6 Mitigation



WECC

Electric Reliability and Security for the West

www.wecc.org

<Public>

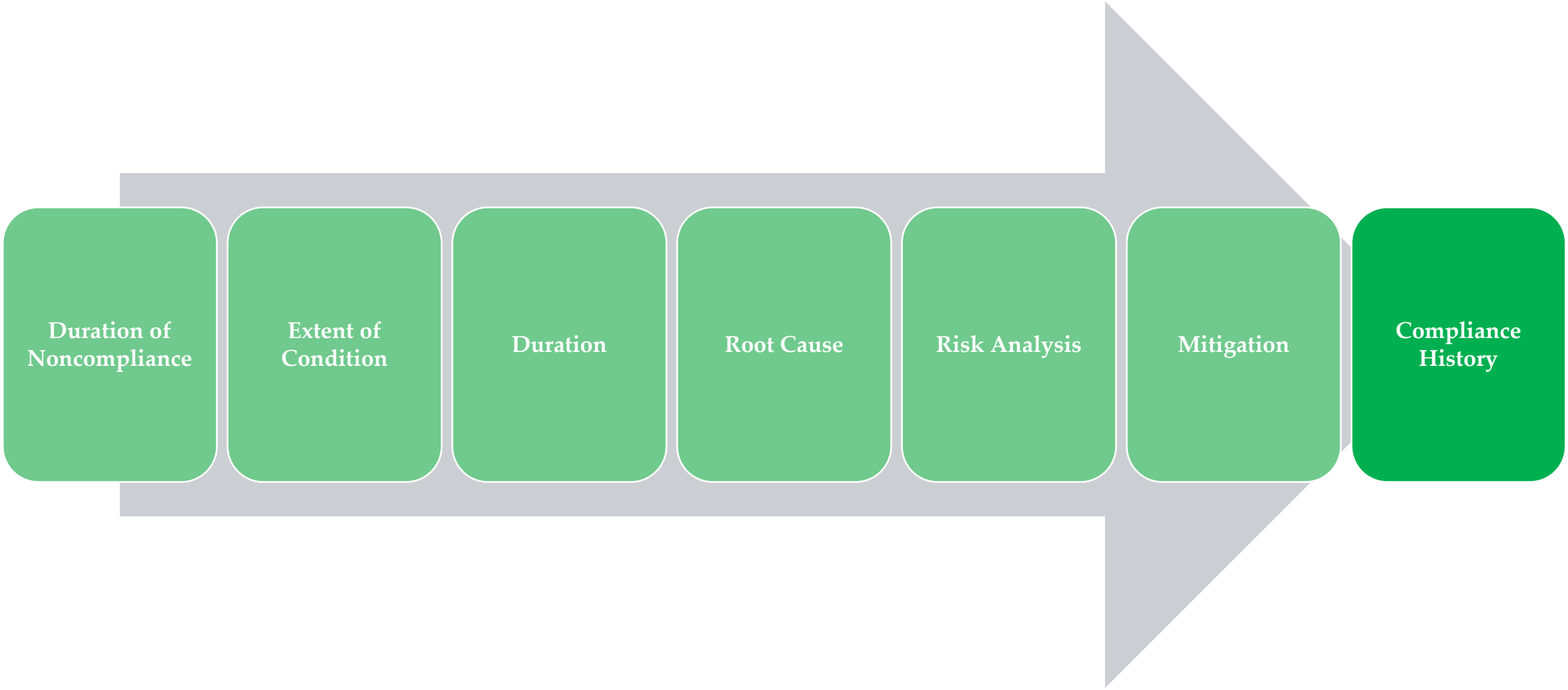
WECC

WECC Enforcement Training:

2.7 Compliance History

WECC Enforcement Staff

2.7 Compliance History



Section Learning Plan

1

Conceptual Foundation

- Application of concept to non-NERC situations (Spoiled Milk)

2

Teaching Exercises

- Present examples and then demonstrate WECC's Analysis and Disposition Language
- FAC-003-4 & CIP-004-6

Conceptual Foundation

Five-year look-back

Noncompliance with the same Root Cause

Affiliates with same violation

Conceptual Foundation

Two-step Process for Determining Compliance History

Step 1: Determining Relevancy—a prior instance of noncompliance is relevant when the two below elements are met:

- Five-year Lookback Period (end date of the prior noncompliance and start date of the current noncompliance)
  - NERC ROP Appendix 4B (NERC Sanction Guidelines)
    - Section 3.3.1 Aggravating Factor: Repetitive Violations and Compliance History
- NERC ROP Appendix 4C (Compliance Monitoring and Enforcement Program)
  - Section 4A.1 Compliance Exception Process
    - "Compliance Exceptions are not included in a Registered Entity's compliance history for penalty purposes"
- Prior processed instances of noncompliance for Entity (and its affiliates) that involve the same *or similar* Standard and Requirement

Conceptual Foundation

- What does "or similar" mean?
  - Version Mapping—Ensuring the inclusion of all similar versions of the Standard and Requirement
- Affiliates:
  - The relevant compliance history of the parent/affiliates are analyzed if an Entity has:
    - A parent or affiliate relationship(s); and
    - The organizations share a common NERC compliance program.
      - Exists when the affiliate is operated by, or whose compliance activities are conducted by, the same parent/affiliate company.
      - Factors to consider when analyzing control of the affiliate include whether the affiliate has: (a) its own compliance policies, processes, and procedures, (b) its own committee to monitor and oversee compliance, and (c) its own compliance officer.

Conceptual Foundation

Two-step Process for Determining Compliance History

Step 2: Determining Aggravation (Analyzed Factors)

- Facts and Circumstances (repetitive violations)—indicative of programmatic or systemic failures
  - Root Cause—same root cause should have prevented current noncompliance
  - Mitigations—prior mitigating activities should have current noncompliance
  - Duration
- High-Frequency Activities (e.g., frequently violated CIP standards)
- Method of Discovery
  - Self-Reported through internal controls, or found via Audit/Self-Certification
- Compliance Exception Treatment Exceptions (NERC ROP Appendix 4C Section 4A.1)
  - "consider a history of Compliance Exceptions where the failure to fully remediate the underlying noncompliance matter contributes to a subsequent serious or substantial noncompliance
  - "assess subsequent noncompliance to determine whether a Registered Entity should continue to qualify for Compliance Exception treatment"

Conceptual Foundation

Analyzed Factors (continued)

- Entity Size
- Strong Internal Controls
- Self-identification
- Nature of the Reliability Standard
- Implementation of a new Standard/Requirement or a new version of a Standard/Requirement
- Different Assets, Business Units, and/or Personnel

Conceptual Foundation

If the instant noncompliance warrants aggravation based on the Entity's relevant compliance history, WECC will determine the level of aggravation or if aggravation is ultimately warranted based on the nature, scope, and risk of the prior noncompliance and instant noncompliance.

Relevant compliance history does not necessarily mean the risk designation and/or the disposition track for the current noncompliance must be elevated (analysis of aforementioned factors). Depending particularly on the level of risk posed by the instances of noncompliance that comprise the Entity's compliance history, CE or FFT treatment may still be warranted for new moderate or minimal risk issues.

- Types of Aggravation:
  - Elevation of the disposition track
    - Example: processed as an FFT as opposed to a CE
  - Elevation of the risk level
    - Example: the risk will be treated as moderate as opposed to minimal
  - Elevation of monetary and/or non-monetary penalties

Section 2.7—Concept Example

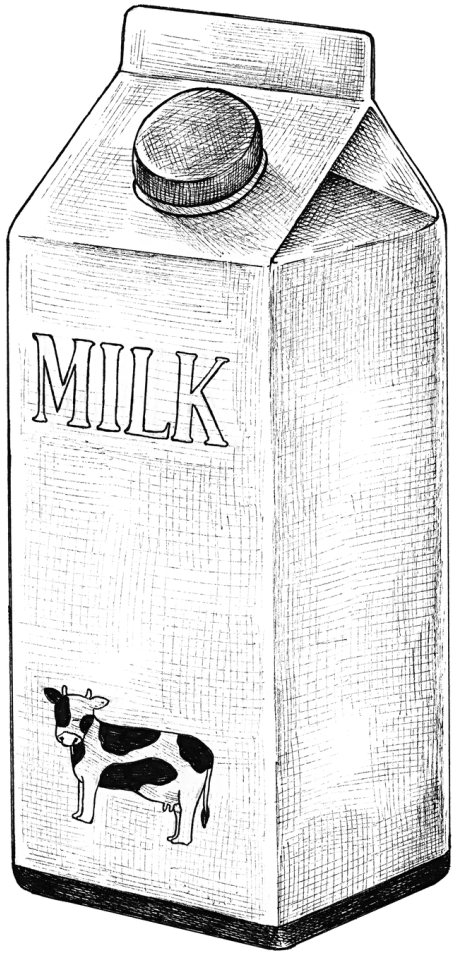
Compliance history

Conceptual Example

MILK-001

Application of concept to non-NERC situation

2.7 Compliance History

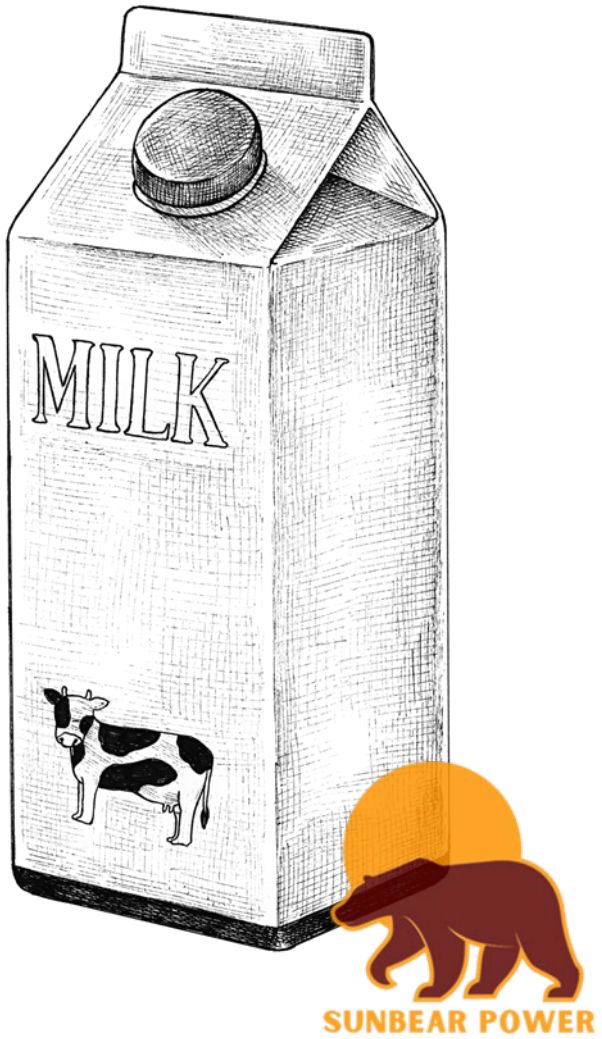


Food Standard:

SNBR-MILK-001

Pasteurized milk must be discarded on or before the expiration date listed on each carton.

2.7 Compliance History



Fact Pattern

- Sunbear has had two previous violations of MILK-001 in the past five years, however they had different root causes, and the mitigation for those cases would not have prevented the spoiled milk from occurring.
- The first instance was filed under WECCXXXX. In September of 2019, Sunbear identified one gallon of milk that was not discarded before its expiration date. Although Sunbear had logged weekly milk inspections, the milk had been pushed to the back of the fridge and went unnoticed during visual inspections. The root cause was assessed to be inadequate training for refrigerator inspection.
- The second instance was filed under 2020-XXXX. In June of 2020, Sunbear discovered 10 gallons of expired milk. This incident was determined to be COVID-related noncompliance. Sunbear moved to a remote workforce model on a Tuesday, before the Friday refrigerator inspection date. When employees returned to the office after six months, all stored milk was presumed to be spoiled and discarded based on their past expiration dates.

2.7 Compliance History

Analysis

Sunbear has previously violated the same Standard and Requirement (MILK-001) within the five-year lookback period.

- Therefore, Sunbear has **relevant** compliance history.

Due to the different root causes for the two prior instances of noncompliance, the prior mitigations would not have prevented the current instance of noncompliance from occurring.

- Therefore, Sunbear does not have **aggravating** compliance history.

2.7 Compliance History

Example Disposition Language

WECC determined that the Entity's compliance history should not serve as a basis for elevating the disposition track for this noncompliance.

The Entity had two previous, relevant violations of MILK-001.

In the first instance, the root cause was assessed to be inadequate training for refrigerator inspection.

The second instance was determined to be COVID-related noncompliance. Sunbear moved to a remote workforce model on a Tuesday, before the Friday refrigerator inspection date. When employees returned to the office after six months, all stored milk was presumed to be spoiled and discarded based on their past expiration dates.

However, in this current instance, the root cause was determined to be too short of an electrical cord, and that the employee in charge of Milk Monitoring was on sick leave while the back-up Milk Monitor was not informed of their absence. The mitigation for the prior instances would not have prevented or detected the instant noncompliance.

2.7 Compliance History

Compliance History

Example One

FAC-003-4 R2

No Compliance History

2.7 Compliance History

Analysis

- Sunbear has never violated FAC-003-4 R2, or a similar standard requirement from a previous version of the standards.
- Therefore, there is neither **relevant** nor **aggravating** compliance history.

Example Disposition Language

WECC considered the Entity's compliance history and determined that there were no relevant instances of noncompliance.

2.7 Compliance History

Compliance History

Example Two

CIP-004-6 R4

Applicable Compliance History

2.7 Compliance History

Analysis

- Sunbear has previously violated CIP-004-6 R4.
- There is **relevant** but not **aggravating** Compliance History.

Example Disposition Language

WECC determined that Sunbear's compliance history should not serve as a basis for elevating the disposition track for this noncompliance.

Sunbear has one previous, relevant violation of CIP-004-6 R4.

The previous instance was due to human performance issues when an engineer, who had been trained properly, made an error and allowed contractors to use his laptop to access BES Cyber Assets for maintenance activities.

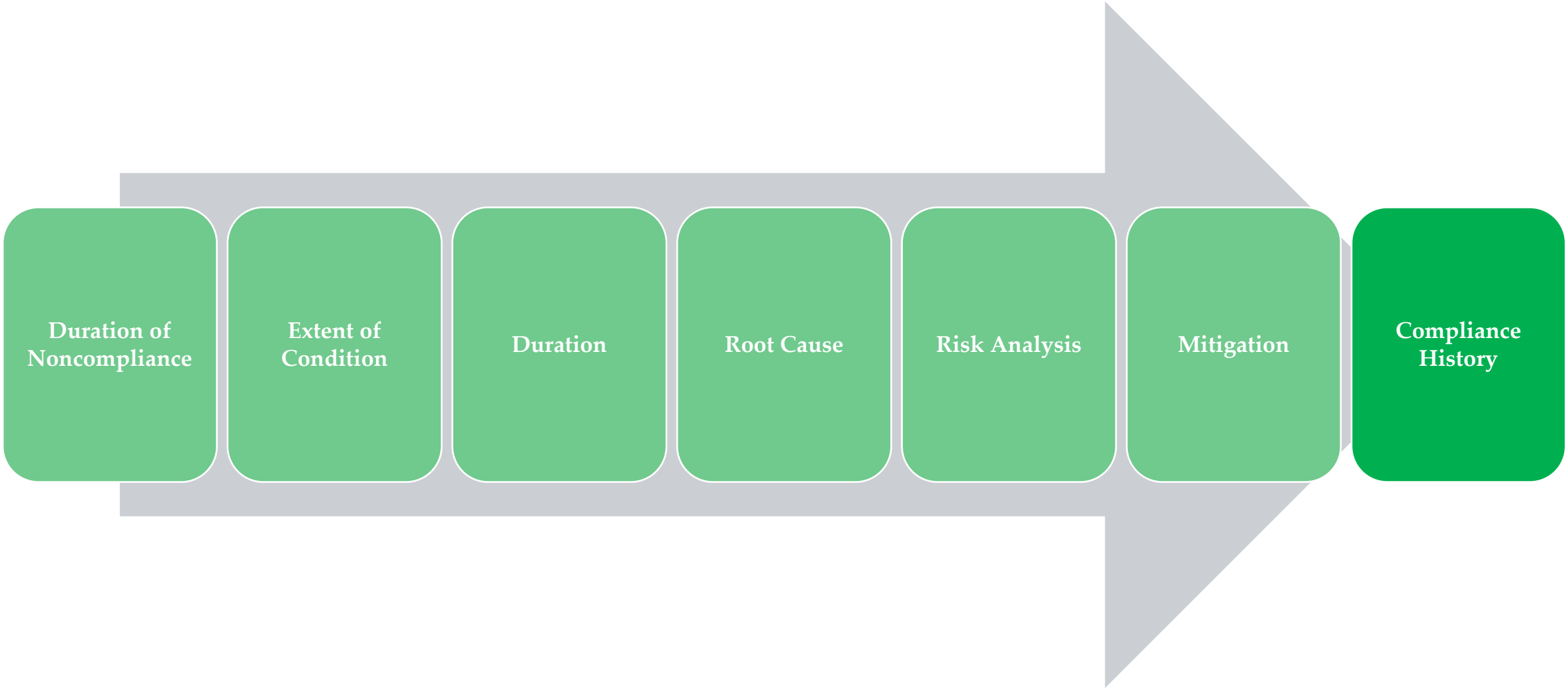
However, in this current instance, lack of controls and training were the cause of the noncompliance, and the mitigation for the prior instance would not have prevented or detected the instant noncompliance.

2.7 Compliance History

What if there is Relevant and Aggravating Compliance History?

1) Can potentially elevate the disposition track based on the facts and circumstances of the instant and prior violations.
    - CE -> FFT -> SNOP -> FNOP
2) Can potentially consider an increase to the monetary penalty based on the facts and circumstances of the instant and prior violations.

2.7 Compliance History



WECC

Electric Reliability and Security for the West

www.wecc.org

WECC

WECC Enforcement Fundamentals:

Noncompliance Processing

WECC Enforcement Staff

Enforcement Fundamentals Overview

Enforcement Background

- Introduction
- Enforcement Function
- The Magnificent Seven
- Enforcement Processing
- Self-Logging Program

1

Noncompliance Reporting

- Building the Story
- Description of Noncompliance
- Extent of Condition
- Duration
- Risk to BES
- Root Cause
- Mitigation
- Compliance History

2

Noncompliance Processing

- Enforcement Review
- Findings
- Preliminary Screen
- PNC Review
- Enforcement
- Disposition
- Closing Case

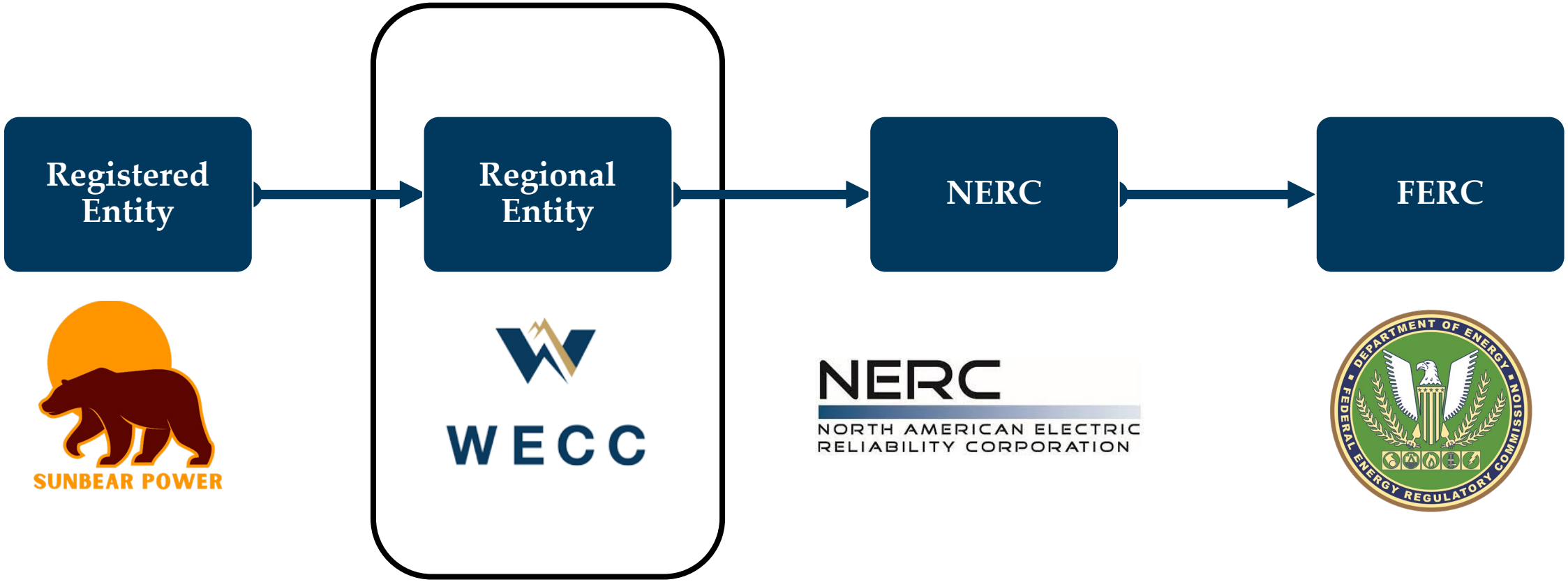
3

Practice & References

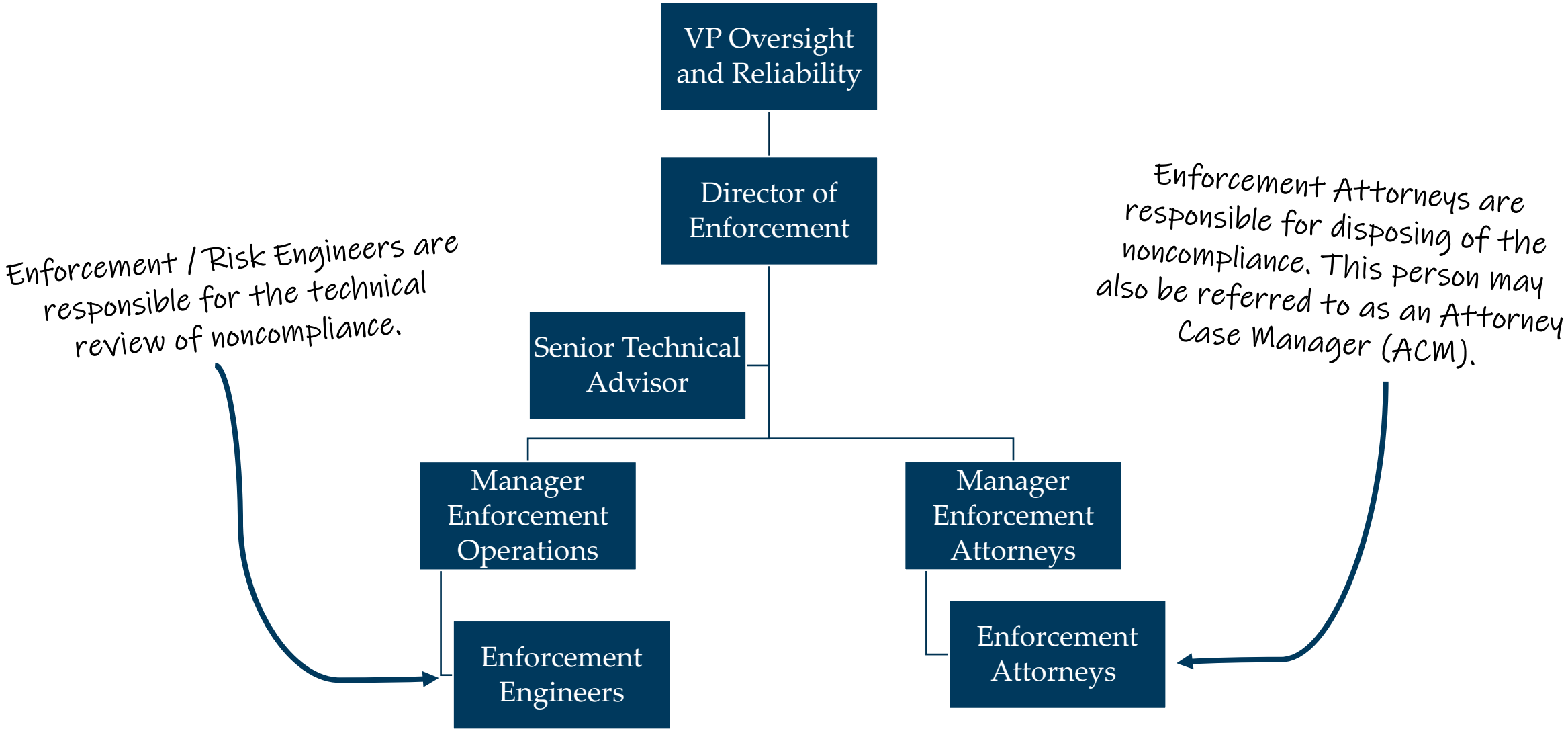
- Practice Cases
- Job Aids
- References

4

Noncompliance Routing



WECC Enforcement Organization



Enforcement Processing

Enforcement Processing

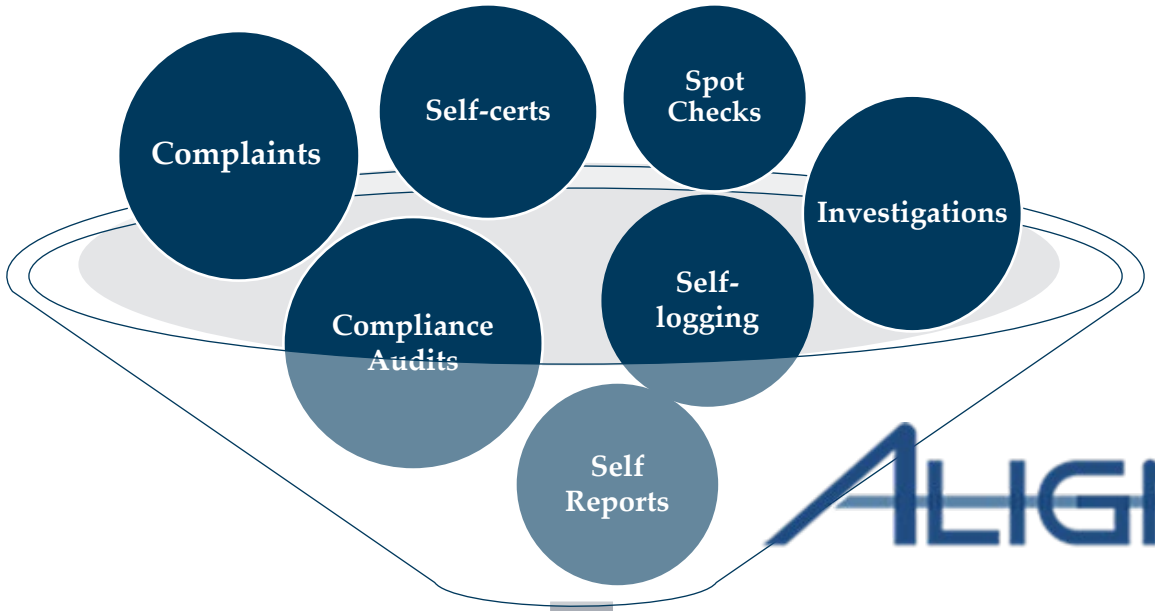
Enforcement Processing

Registered Entities can create self-logs or self-reports.

WECC can also create audit findings, spot checks, and self-certifications.

Once any finding is submitted for review, Align will automatically create a mitigation record to pair with that finding.

Compliance Monitoring Process



FINDING

MITIGATION RECORD

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

MIDWEST RELIABILITY ORGANIZATION
SERC
WECC
TEXAS RE
RELIABILITY FIRST
NPCC, Inc.

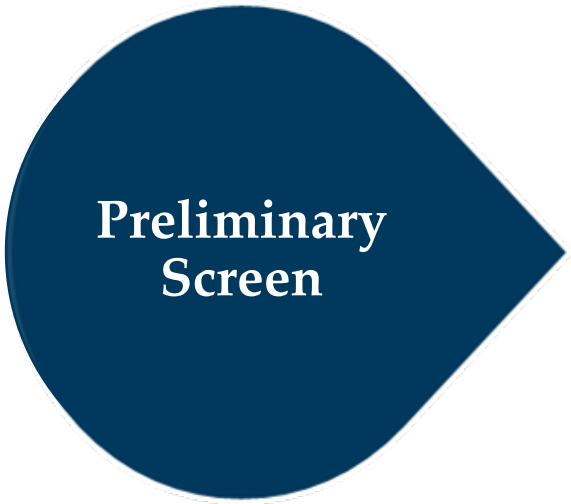
Compliance Audit Noncompliance

<Public>

Self-Certification Noncompliance

Enforcement Processing

Enforcement Processing

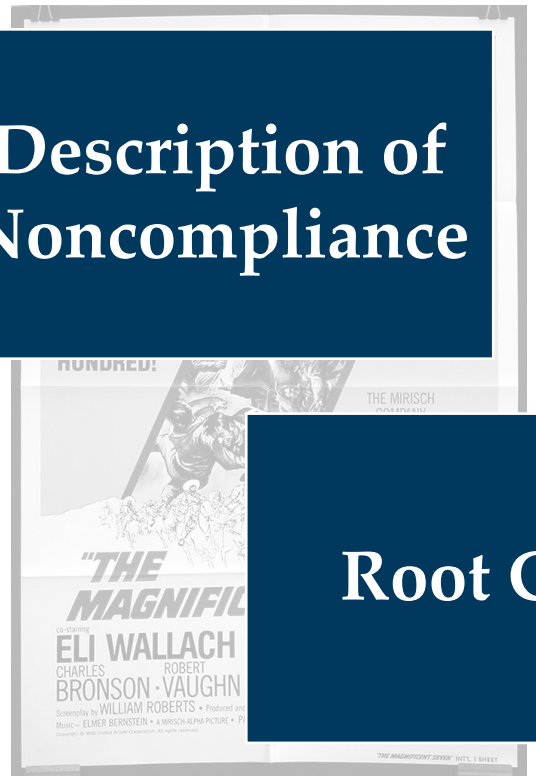


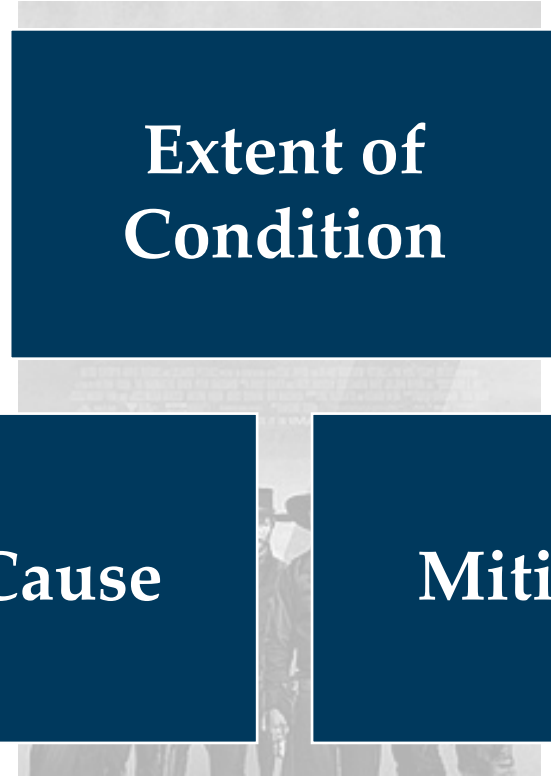
- Compliance Program Coordinators check the following
  - the entity allegedly involved in the potential noncompliance is registered
  - the Reliability Standard & Requirement to which the evidence of potential noncompliance relates is applicable to a reliability function for which the entity is registered
  - if known, the potential noncompliance is not a duplicate of one that is currently being processed
- After screening Align status changes from "Preliminary Screening" to "PNC Screening"

Enforcement Processing

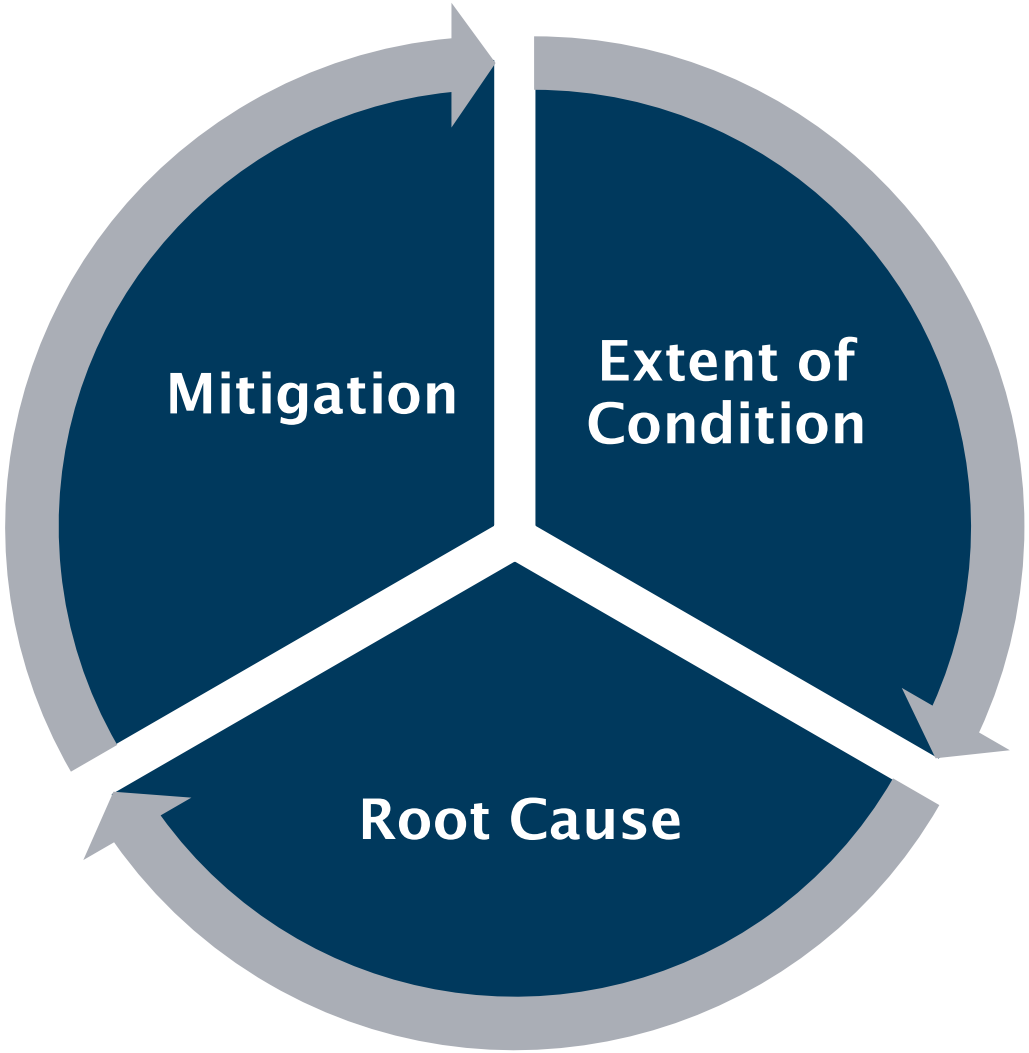
Magnificent Seven

- Description of Noncompliance
- Extent of Condition
- Duration
- Risk to BES
- Root Cause
- Mitigation
- Compliance History





Essential Interplay



RFI Circumstances

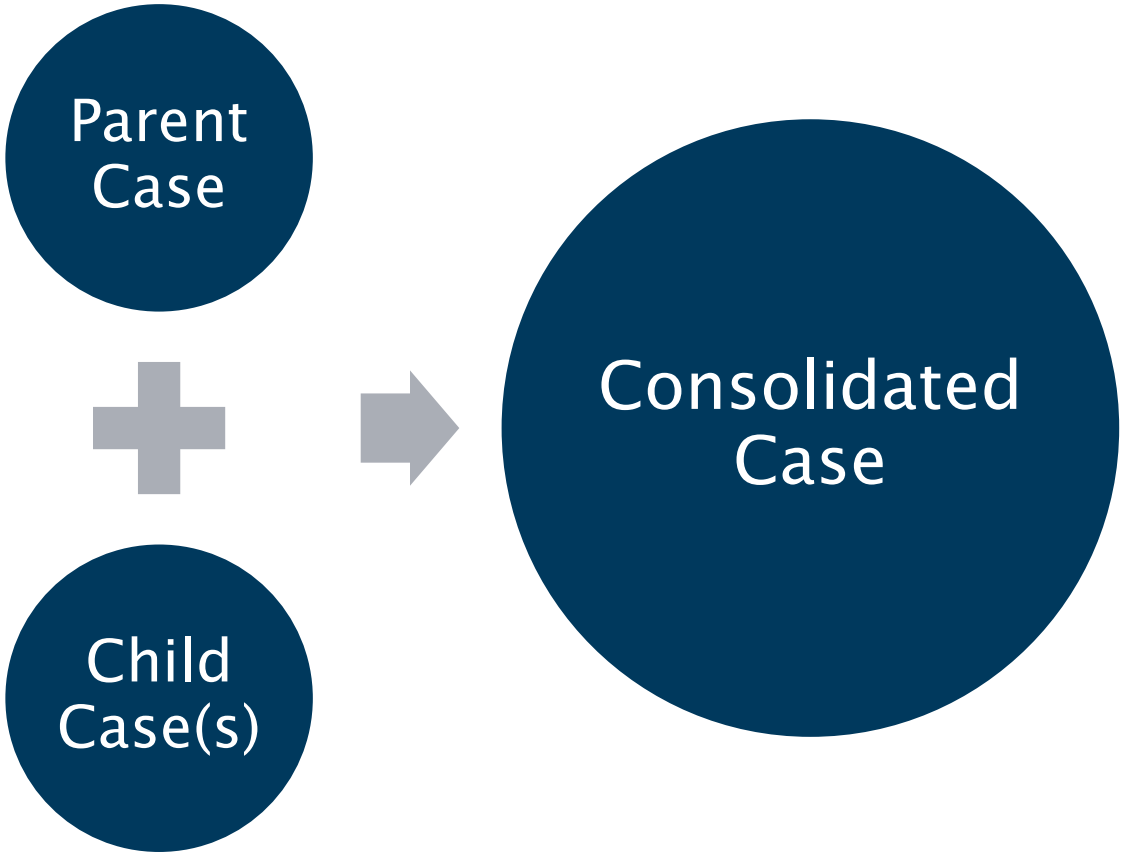
- Its implied but not written
- We aren't sure what you are saying
- We aren't experts in your system
- We need more information
- No first-hand experience
- Confusing timeline

Why?

- Align
- Meetings
- Emails
- Phone calls

How?

Consolidation

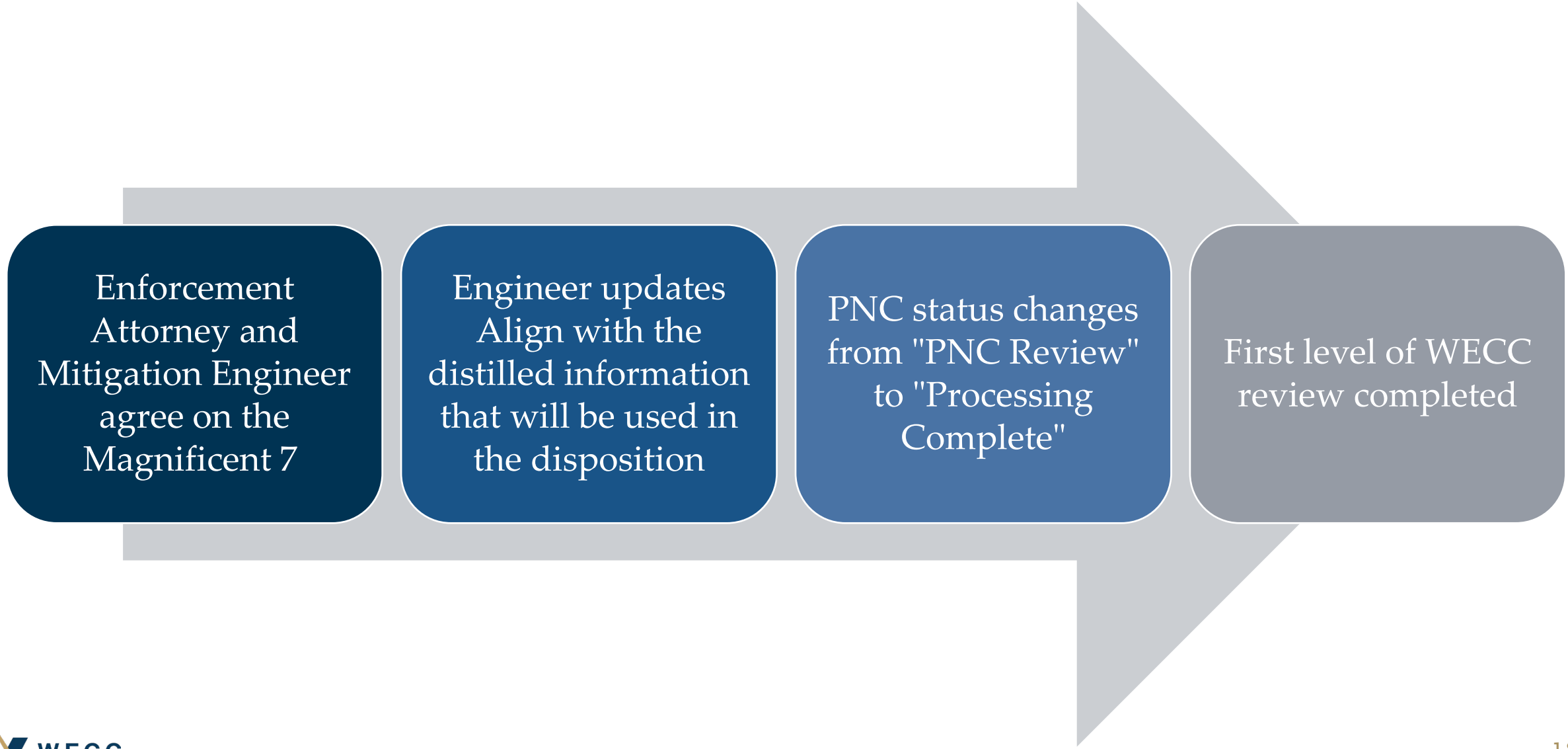


- Can only consolidate when:
  - Open PNC's

  AND
  - Same Standard and Requirement

  AND
  - Same or similar Root Cause
- Purpose
  - Simplify analysis
  - Simplify mitigation

Processing Complete

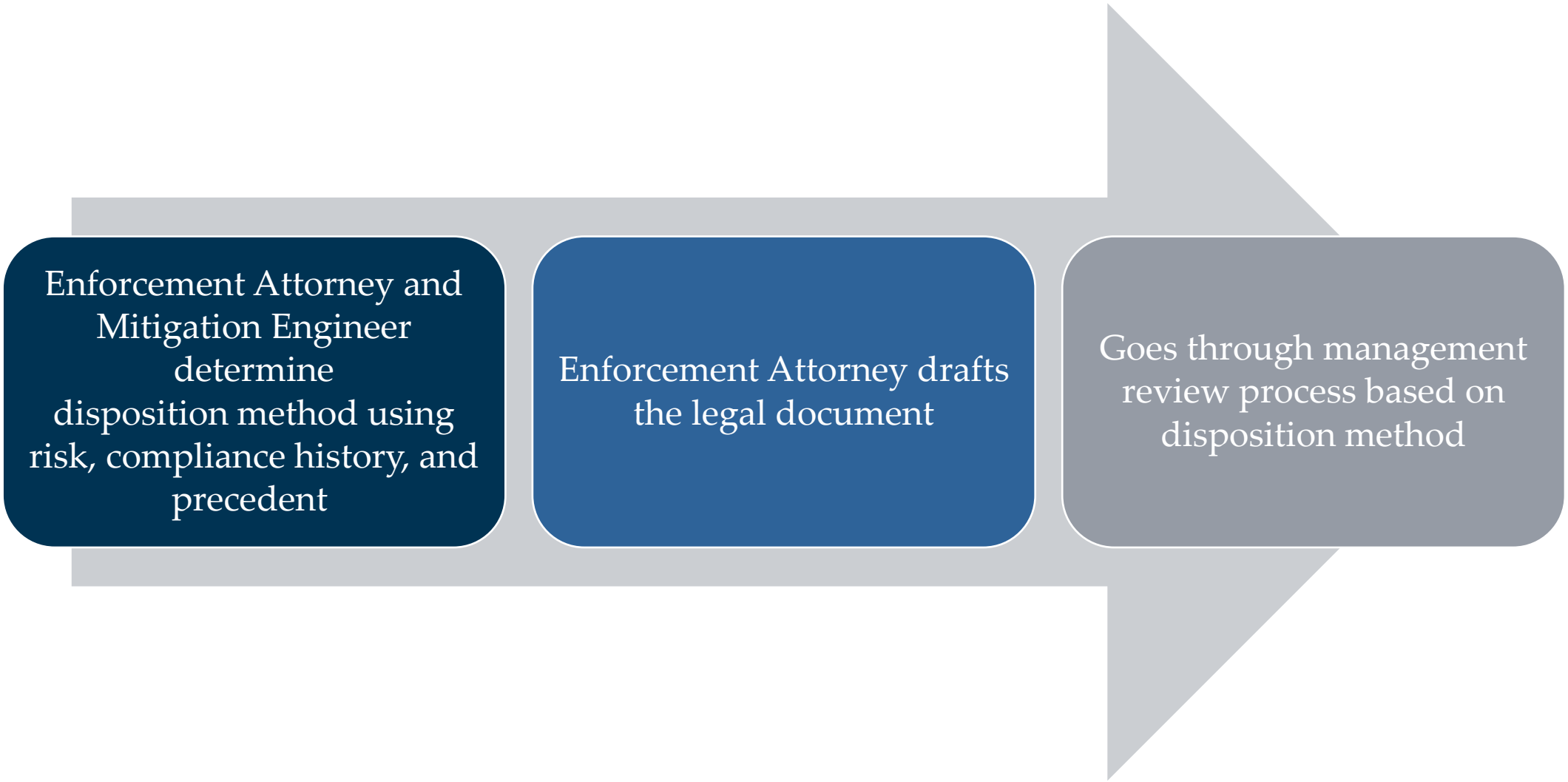


Enforcement Processing

- Majority of the analysis occurs during this phase
- After confirming information WECC will edit/update the finding in Align with the distilled information used in their analysis
  - This does ***NOT*** overwrite entity submission, it is a separate set of fields in Align
  - NERC/FERC use this information in their reviews
- Once information is updated and advanced the PNC Status changes from "PNC Screening" to "Enforcement Processing"

Enforcement Processing

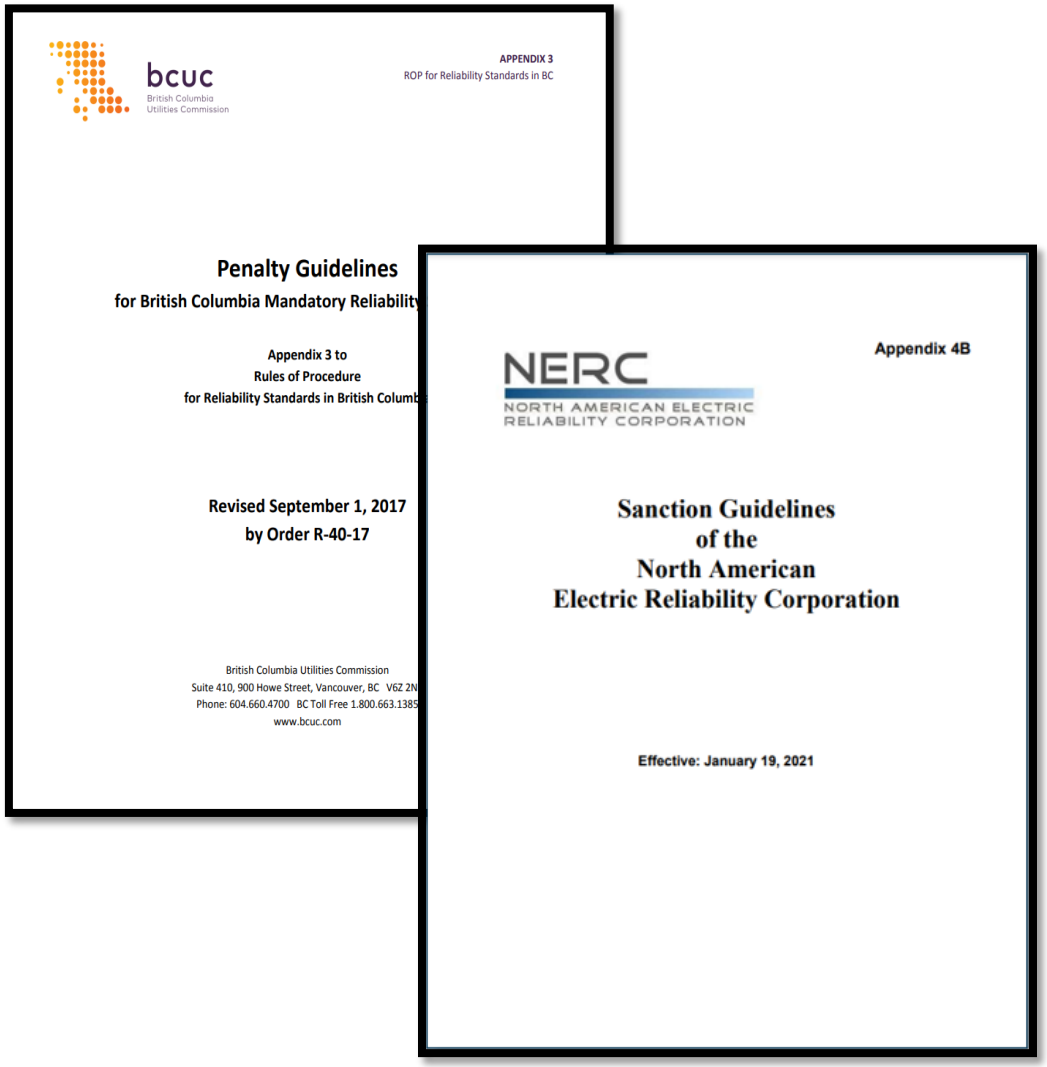
Disposition



Disposition Method Determination

Disposition Method	Risk
Dismissal	
Compliance Exception (CE)	Minimal
Find, Fix, Track and Report (FFT) and BC Find, Fix, Track (BC FFT)	Minimal or Moderate
Settlement/Spreadsheet Notice of Penalty (SNOP)	Minimal or Moderate
Settlement/Full Notice of Penalty (FNOP)	Can be any risk, but typically Serious/Substantial
Notice of Alleged Violation Penalty and/or Sanction (NAVAPS)	Any risk
BC Notice of Alleged Violation (BC NOAV)	Can be any risk but typically Moderate or Serious

Disposition



Penalty Determination if SNOP, FNOP, or NAVAPS

- Determine base penalty amount
  - Violation risk factor and violation severity level table
  - Entity size
  - Assessed risk
  - Violation duration
  - Violation time horizon
- Adjustment factors
  - Mitigating factors
  - Aggravating factors
- Review other comparable cases to ensure consistency of assessed penalty with prior filings

Management Reviews

Dismissal-Consolidation	• Manager approval
Dismissal-For Cause	• Manager and Director approval
Compliance Exception	• Manager approval
FFT and BC FFT	• Manager approval
SNOP, FNOP, NAVAPS, or BC NOAV Penalty $0 - < $50,000	• Manager and Director approval
SNOP, FNOP, NAVAPS, or BC NOAV Penalty ≥ $50,000 and/or nonmonetary penalty	• Manager, Director, and VP RSO approval

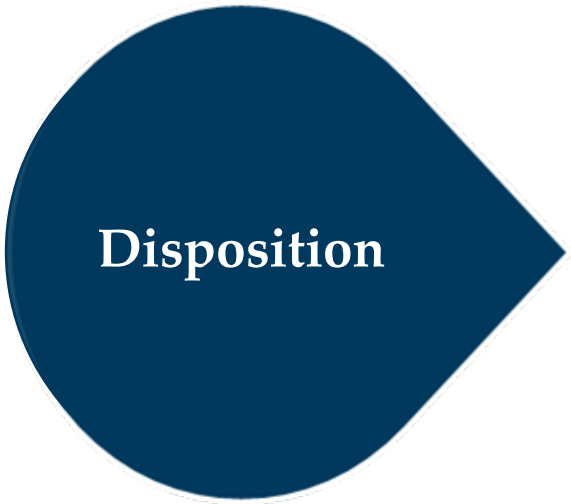
Filing

Dismissals-For Cause	Filed with NERC or BCUC Filed on ongoing basis NERC has 30-day review period
CE and FFT	Filed with NERC in monthly batch NERC files with FERC FERC has 60-day review period
BC FFT and BC NOAV	Filed with BCUC Filed on ongoing basis BCUC FFT Acceptance Letter or Order of Confirmed Violation
SNOP/FNOP Settlements and NAVAPS	Filed with NERC Filed on ongoing basis Pre-filing meetings with FERC for all FNOP settlements NERC files with FERC FERC has 30-day review period

Dismissals

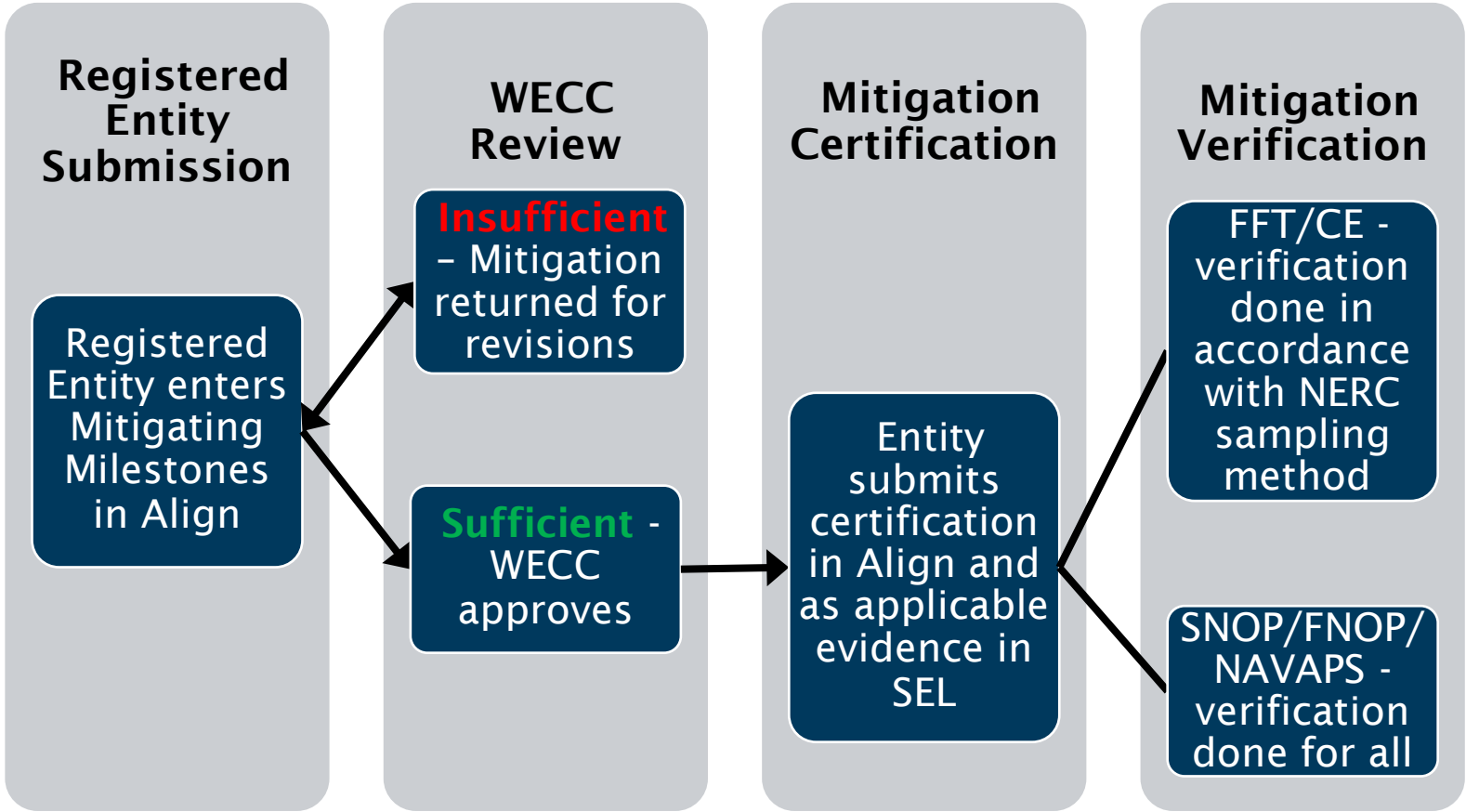
- Dismissals can be "triggered" at any point enforcement process before the case is closed
- Dismissal for cause require evidence of positive compliance
- Dismissals receive a full technical review equivalent to upholding findings
- Dismissal of Audit findings must be approved by Entity Monitoring team as well
- NERC requests certain dismissals be present to NERC Legal prior to Filing to ensure regional consistency

Enforcement Processing



- Enforcement Attorney draft the disposition document
- Mitigation Engineers review document for technical accuracy
- Legal Manager reviews the disposition
  - Note: Mitigation will be approved at this step
- If needed based on disposition the Enforcment director and Vice President review the disposition
- Compliance Program Coordinator ensure all details match Align, send Disposition to NERC for review
- NERC approves the disposition
- Once NERC approves the PNC status changes from "Enforcement Processing" to the Type of disposition (CE, FFT, etc.)

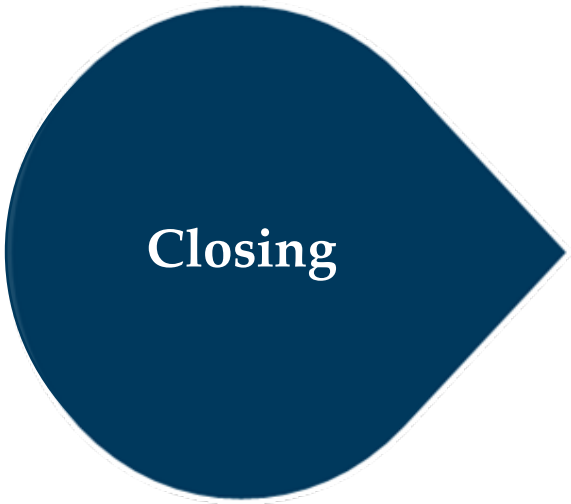
Mitigation Life Cycle



Align Status	Draft	CEA Processing	(NERC Approval) Active	Verification	Complete

Enforcement Processing

Enforcement Processing



When the disposition is closed, so are all the EAs, PNCs, findings, and mitigations contained within it.

Closing

United States

- Filing approved by FERC
- Mitigation certified complete by Registered Entity
- Mitigation completion verified by WECC (*if applicable*)
- FFT Affidavit submitted (*if applicable*)
- Monetary penalty paid (*if applicable*)
- Nonmonetary penalty completed (*if applicable*)

British Columbia

- Attestation of mitigation completion
- Entity response to NOAV (*if applicable*)
- BCUC Order Confirming Violation (*if applicable*)
- BCUC letter accepting BC FFT (*if applicable*)
- BCUC Order approving Mitigation
- BCUC letter accepting Attestation

WECC

Electric Reliability and Security for the West

www.wecc.org