NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Enforcement Approach to CIP Version 5 under RAI

March 18, 2014

Tobias Whitney, Manager of CIP Compliance

RELIABILITY | ACCOUNTABILITY

Purpose of the Transition Program

Address V3 to V5 Transition issues.

Provide a clear roadmap for V5 steady-state.

Justify budget for V5 implementation and compliance.

Foster communication and knowledge sharing.

Support all entities in the timely, effective, and efficient transition to CIP Version 5

CIP V 5 Transition Program Elements

Periodic Guidance

- A new transition guidance will be provided after V5 Order

Implementation Study

- 6 entities with strong compliance cultures
- 6-8 month implementation of V5 for certain facilities
- Lessons learned throughout and after study phase

Compliance and Enforcement

- Integration with RAI
- Identify means and method to address self-corrective processes and internal controls

Outreach & Communications

- New website created for all Transition Program activity

Training

- Quarterly training opportunities will be provided to industry

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Purpose of RAI

- A strategic initiative to transform the current compliance monitoring and enforcement program that:
  - Focuses on high reliability risk areas
  - Reduces unnecessary administrative burdens
- Main goals:
  - Building on the success of Find, Fix, Track and Report (FFT)
  - Design a compliance program that:
    - Recognizes an entity's risk to reliability
    - Appropriately scopes audits and applies proper audit techniques and approaches
    - Evaluates and uses management controls to gain reasonable assurance of compliance which promotes reliability
  - Reduce unnecessary administrative burdens of the compliance monitoring and enforcement program on all stakeholders.

2013 Year End Progress Report

Auditor Handbook

- The first version of auditor handbook was completed.
- Training and rollout efforts to occur in 2014.

Prototypes and Pilot Programs

- The results to-date of pilot programs are being compiled.
- Evaluation criteria has been finalized
- The assessment timeline and 2014 deliverables are set.

Improvements to Self-Reporting

- User guide to support improved self reporting process completed in December 2013.
- Request for broader industry review in January 2014.

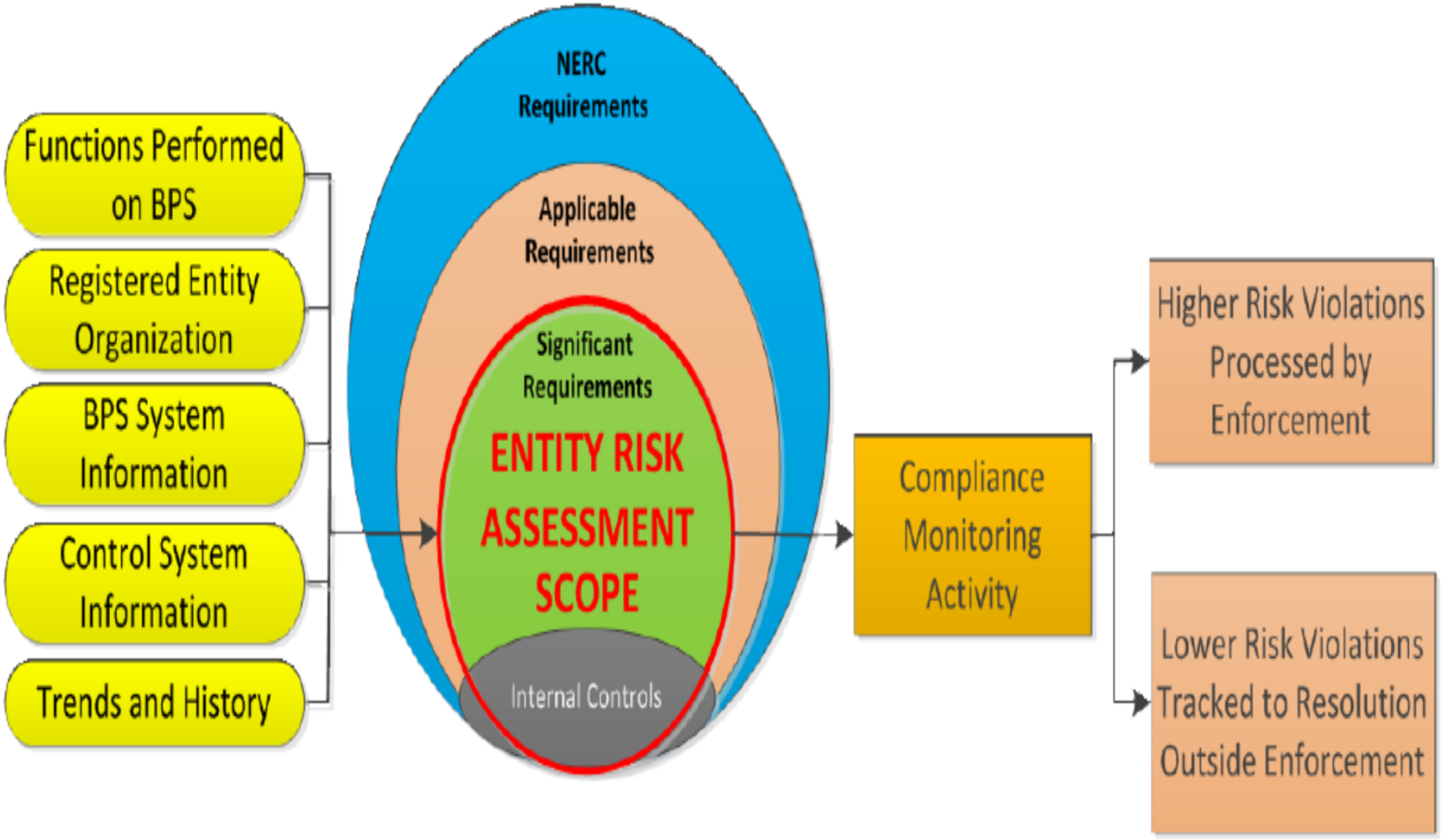
FFT Enhancements

- Triage process implemented across ERO by January 1, 2014 to expedite disposition of minimal risk issues.
- Enforcement pilots to test aggregation and exercise of enforcement discretion underway.

V5 Compliance and Enforcement Steady State

- V5/RAI Key Program Elements (based on Evaluation Criteria)
  - Risk Assessment
    - The Regional Entity will develop a transparent but customized compliance profile based on the Registered Entity's impact to the grid.
    - The Risk Assessment will be shared with the Registered Entity so that it understands how it will be monitored as part of the compliance profile.
  - Internal Controls Reliance
    - The Registered Entity's internal control practices will be provided and reviewed by the Regional Entity.
    - The Regional Entity will evaluate the level of the entities internal control program to tailor compliance activities in conjunction with the Risk Assessment.
  - Aggregation of Noncompliance
    - Based on the level of controls reliance and the Risk Assessment, Registered Entities may be able to log minimal risk noncompliance.

RAI Approach



Hypothetical: Mega

Facts:

On January 1, the Mega Electric Co. discovers, during a routine patch assessment, that it did not assess security patches on 1 **(1 of 393 systems)** Protected Cyber Asset (PCA) issued in **November** of the prior year. The missing patch was for the **Adobe application** running on a **Historian**.

Mega has an instance of noncompliance with CIP-007-5 R2 Part 2.2.

CIP-007-5 R2 Part 2.2

CIP-007-5 — Cyber Security – Systems Security Management

R2. Each Responsible Entity shall implement, ~~in a manner that identifies, assesses, and corrects deficiencies,~~ one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

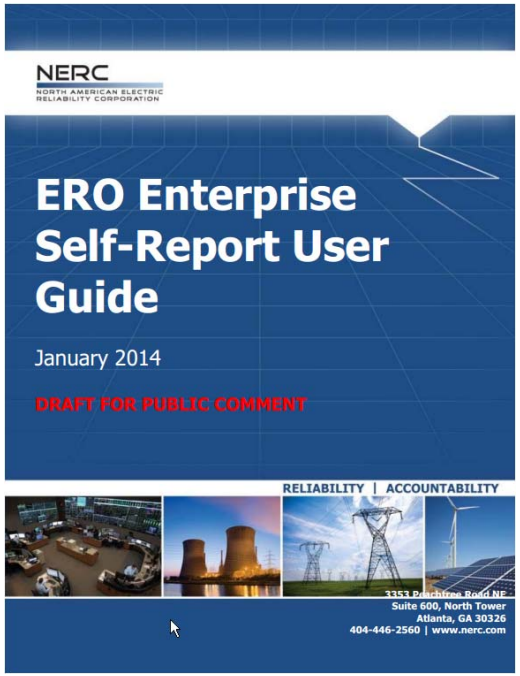
M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	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	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

Hypothetical: Mega

Mega determines, based on an analysis of all of the facts and circumstances, that the noncompliance posed a **minimal risk**

to the reliability of the BPS.



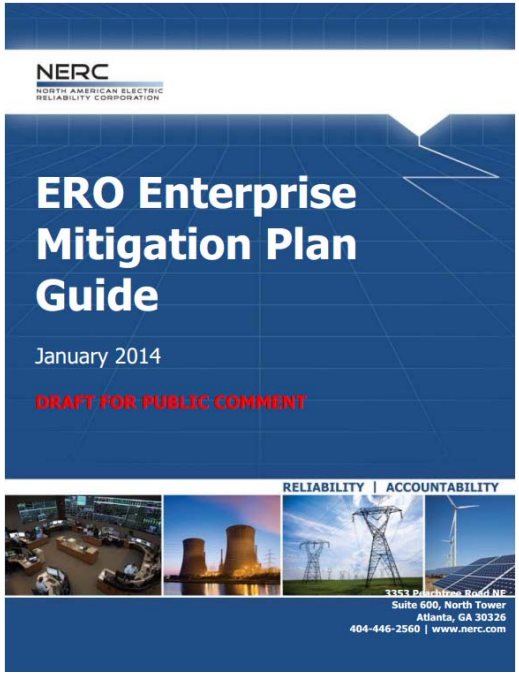
A draft is available at:

www.nerc.com/pa/comp/Pages/Reliability-Assurance-Initiative.aspx

Hypothetical: Mega

Mega identifies and completes mitigating activities that address:

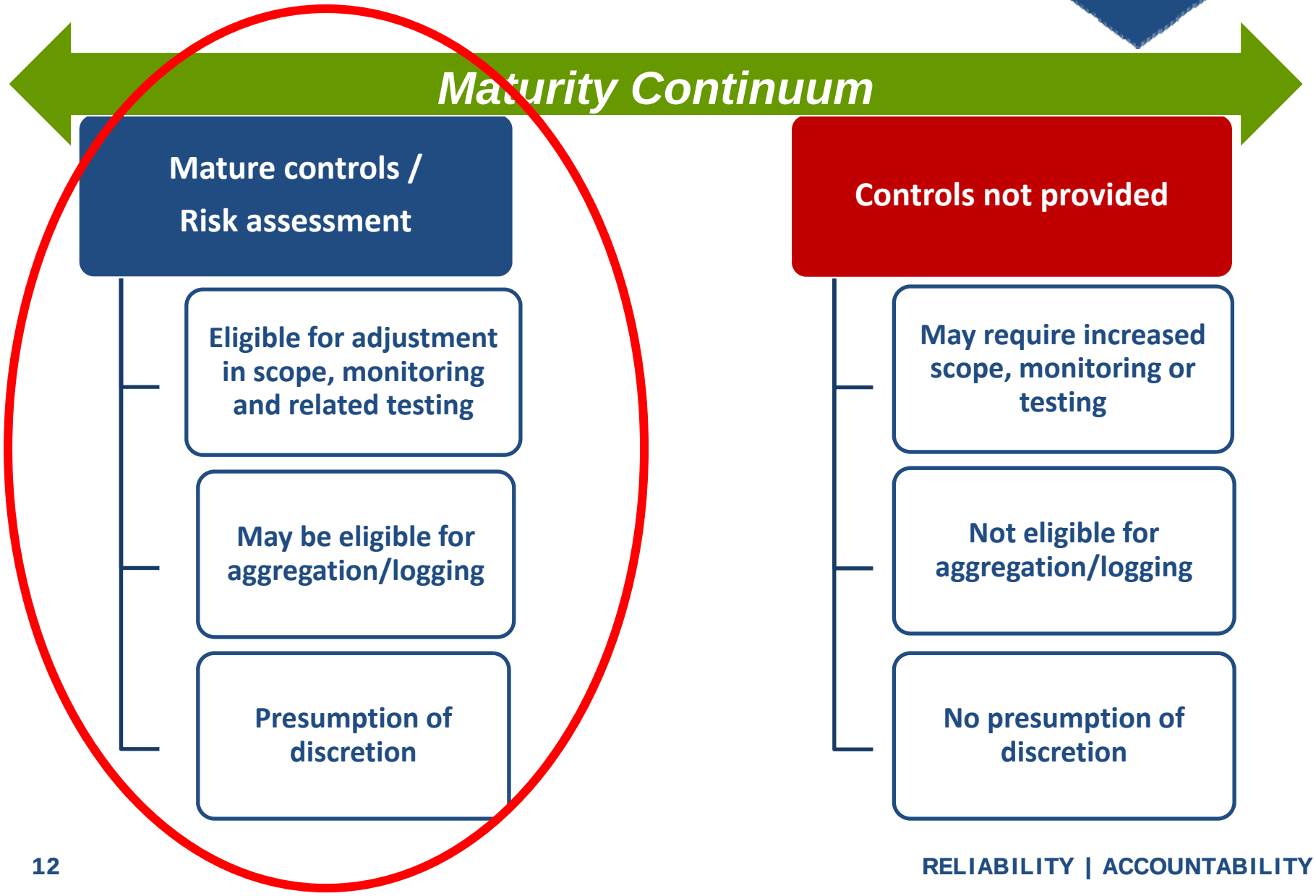
1. the missed patch evaluations, and
2. the reasons why it failed to conduct the evaluations in November.



A draft is available at:

www.nerc.com/pa/comp/Pages/Reliability-Assurance-Initiative.aspx

End-State RAI Processes



Scenario A: Aggregation Path

Scenario A:

Mega had previously demonstrated mature cyber security controls to its Regional Entity according to an accepted methodology. Therefore, it had been allowed to aggregate its minimal risk issues.

Because Mega has identified this issue as posing a **minimal risk to reliability**, it will track the facts and circumstances surrounding this noncompliance in a tracking spreadsheet (or in the Regional Entity portal, once that is available).

Sample Aggregation Tracker

Region	Name of Entity	NCR		Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
REGION NAME (REGION ACRONYM)	ENTITY NAME (ENTITY ACRONYM) Exactly how it appears in the NERC compliance registry	NCRXXXXX	Make sure the version was mandatory and enforceable during the duration of the violation ex. - CIP-004-3	R If the violation implicates multiple sub-requirements: R1; R1.1; R1.2	Include discovery date, applicable registered functions, and Standard and Requirement at issue. On DATE, ENTITY ACRONYM determined that, as a [Function(s) applicable to the violation], it had an issue of [Standard and Requirement] because	Describe the factors that mitigated the actual risk and potential risk. This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. o Discuss mitigating factors in place during the duration of the violation which prevented moderate to serious or substantial risk o Risk assessments must be based on facts, not assumptions o Risk assessments also should specifically identify and describe any defensive measures or compensating mechanisms that were available to mitigate risk posed by the noncompliance, as well as the extent to which these measures and mechanisms actually performed to alleviate risk during the period in which a responsible entity was in violation. o Size and location can be an element of the risk assessment but should not be the primary mitigating factor o "No actual impact" to the BPS is not necessarily a minimal risk and is not sufficient to support a minimal risk finding o Cannot be minimal risk if the noncompliance reveals a serious shortcoming in the registered entity's reliability-related processes o No "after-the-fact" determinations of risk. Additionally, if the subsequent application of a revised process or methodology resulted in the same outcome, that by itself is not a sufficient mitigating factor. • Example of a deficient risk statement: "After further review of the entity's risk based assessment methodology, the facility in question was not a critical asset and did not require the same protections afforded to critical assets." o "Documentation Only" issues • Noncompliance occurred because the entity failed to document that the action was performed, not because the entity failed to perform an action • Noncompliance with a requirement listing the "action" as keeping records, procedure, signature, etc., is performance, and not "documentation only" noncompliance	To mitigate this issue, ENTITY ACRONYM: 1) past tense activity; 2) past tense activity; and 3) past tense activity. OR To mitigate this violation, ENTITY ACRONYM will complete the following mitigation activities within XX days: 1) future activity; 2) future activity; and 3) future activity. Describe mitigating activities that fix the issue and also prevent recurrence. Maintain evidence to support completion of mitigation activity.

Issue Description

Description of Remediated Issue
Include discovery date, applicable registered functions, and Standard and Requirement at issue. On DATE, ENTITY ACRONYM determined that, as a [Function(s) applicable to the violation], it had an issue of [Standard and Requirement] because . . . .

Mega should provide sufficient details to assist its Regional Entity in making a fair and informed assessment of the noncompliance.

These details should include method of discovery, corrective actions taken, time horizon of compliance, duration of noncompliance, and the full details surrounding the noncompliance itself.

Risk Assessment

Description of the Risk Assessment
Describe the factors that mitigated the actual risk and potential risk. This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. o Discuss mitigating factors in place during the duration of the violation which prevented moderate to serious or substantial risk o Risk assessments must be based on facts, not assumptions o Risk assessments also should specifically identify and describe any defensive measures or compensating mechanisms that were available to mitigate risk posed by the noncompliance, as well as the extent to which these measures and mechanisms actually performed to alleviate risk during the period in which a responsible entity was in violation. o Size and location can be an element of the risk assessment but should not be the primary mitigating factor o "No actual impact" to the BPS is not necessarily a minimal risk and is not sufficient to support a minimal risk finding o Cannot be minimal risk if the noncompliance reveals a serious shortcoming in the registered entity's reliability-related processes o No "after-the-fact" determinations of risk. Additionally, if the subsequent application of a revised process or methodology resulted in the same outcome, that by itself is not a sufficient mitigating factor. • Example of a deficient risk statement: "After further review of the entity's risk based assessment methodology, the facility in question was not a critical asset and did not require the same protections afforded to critical assets." o "Documentation Only" issues • Noncompliance occurred because the entity failed to document that the action was performed, not because the entity failed to perform an action • Noncompliance with a requirement listing the "action" as keeping records, procedure, signature, etc., is performance, and not "documentation only" noncompliance

In assessing risk, Mega should consider all factors that mitigated the actual and potential risk, taking care to avoid after-the-fact determinations.

Only minimal risk issues are eligible for aggregation. Moderate risk issues should be self-reported.

Mitigating Activity

Description and Status of Mitigation Activity
To mitigate this issue, ENTITY ACRONYM: 1) past tense activity; 2) past tense activity; and 3) past tense activity. OR To mitigate this violation, ENTITY ACRONYM will complete the following mitigation activities within XX days: 1) future activity; 2) future activity; and 3) future activity. Describe mitigating activities that fix the issue and also prevent recurrence. Maintain evidence to support completion of mitigation activity.

Mega must log its efforts to mitigate the noncompliance.

Mitigating activities should both resolve the noncompliance and prevent recurrences.

Scenario A: Mature Controls and Aggregation

- Mega will submit its aggregation tracker to its Regional Entity on a periodic basis for review.
- There is a presumption that the noncompliance will not trigger an enforcement action and will qualify for **enforcement discretion**.
- During the Triage Process, the Regional Entity will either confirm the presumption or determine whether:
  - More information is required prior to determining the level of risk and disposition track; or
  - The noncompliance does not qualify for discretion and will be enforced.

What is Enforcement Discretion?

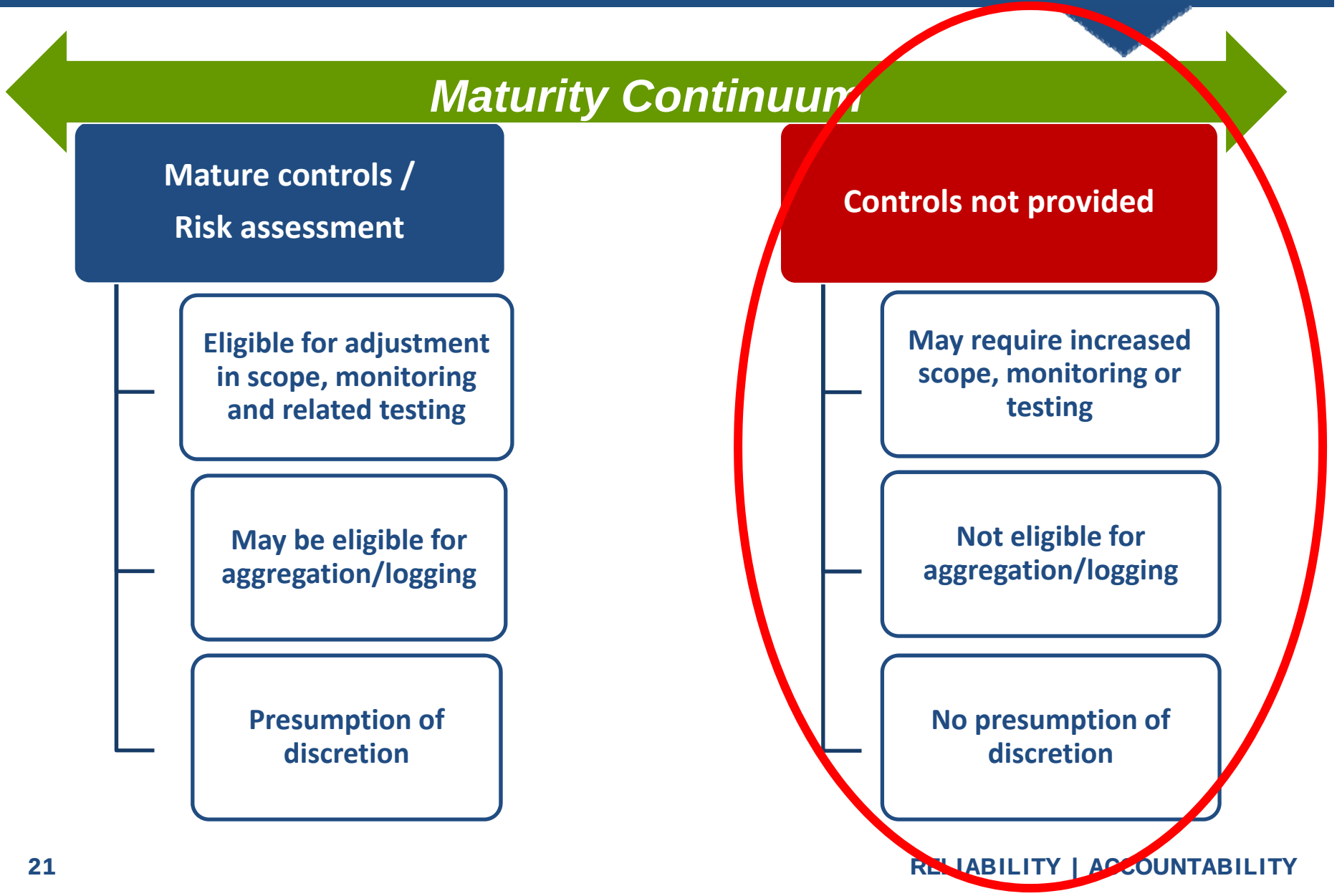
- For a registered entity with demonstrated internal controls that has been allowed to aggregate minimal risk issues, there is a *rebuttable presumption* that a Regional Entity will decline to enforce self-identified, minimal risk issues.
- If Mega's Regional Entity exercises discretion, Mega will be informed of the result, and the noncompliance will not be enforced.
- NERC and FERC will review the exercise of discretion, and NERC will provide guidance and training to Regional Entities as necessary.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Rebutting the Presumption of Discretion

- Mega's Regional Entity may decide to enforce the noncompliance if the circumstances suggest that Mega's management practices surrounding the implementation of its patch assessment procedure are failing:
  - Mega failed to identify its noncompliance in a timely manner;
  - Mega mischaracterized the risk posed by the noncompliance; the noncompliance actually posed a moderate or greater risk to reliability;
  - Mega has missed patch assessments on several recent occasions, demonstrating a failure to mitigate properly in the past;
  - Mega failed to mitigate this issue properly, resulting in repeat occurrences a few months later; or
  - Other facts and circumstances indicate broader programmatic failures.

End-State RAI Processes



Scenario B: Controls Not Demonstrated

Scenario B:

Mega has not demonstrated to its Regional Entity that it has mature cyber security controls and has not been allowed to aggregate minimal risk issues.

Mega has identified its noncompliance with CIP-007-5 R2 Part 2.2 as posing a **minimal risk to reliability** and has decided to submit a Self-Report to its Regional Entity.

Scenario B: No Demonstrated Controls / Self-Report

- Mega submits its Self-Report to its Regional Entity for review.
- During the Triage Process, the Regional Entity will determine whether:
  - The issue in fact poses a minimal risk and qualifies for the exercise of **enforcement discretion**;
  - More information is required prior to determining the level of risk and disposition track; or
  - The noncompliance does not qualify for discretion and will be enforced (*the noncompliance could qualify for FFT treatment*).

Scenario B: Enforcement Discretion

- A Regional Entity may decline to enforce self-identified, minimal risk issues – even from an entity without mature internal controls.
- Mega's noncompliance will be eligible for enforcement discretion. However, there is no presumption of discretion.
- If Mega's Regional Entity exercises discretion, Mega will be informed of the result, and the noncompliance will not be enforced.

Scenario C: A Twist

Scenario C:

Mega missed its patch assessments in November. It resumed patch assessments on January 1 for patches released in December.

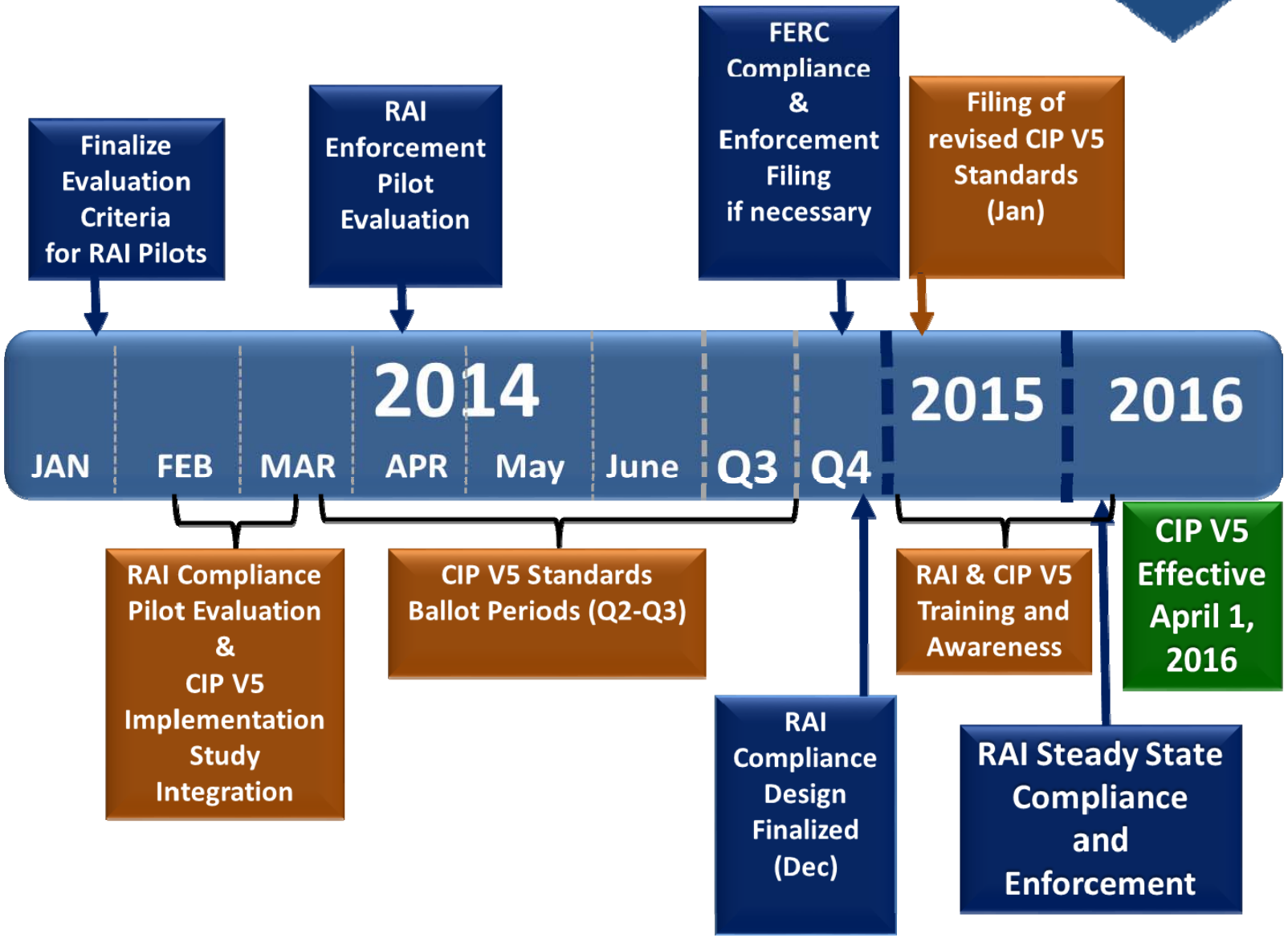
During an Audit two years later, Mega's Regional Entity discovers the noncompliance.

The Regional Entity has identified this issue as posing a **minimal risk to reliability.**

Scenario C: Triage and Enforcement Discretion

- During the triage process, the Regional Entity will determine whether:
  - To decline to pursue this minimal-risk Spot Check finding through the exercise of **enforcement discretion**;
  - More information is required prior to determining the level of risk and disposition track; or
  - The noncompliance does not qualify for discretion and will be enforced.
- While discretion is still available, there is no presumption of discretion for minimal risk issues that are not self-identified.
- Failure to self-identify noncompliance could indicate broader programmatic failures, weighing against discretion in this case and potentially future cases.

CIP V5 Revisions and RAI Timeline



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Thank you.