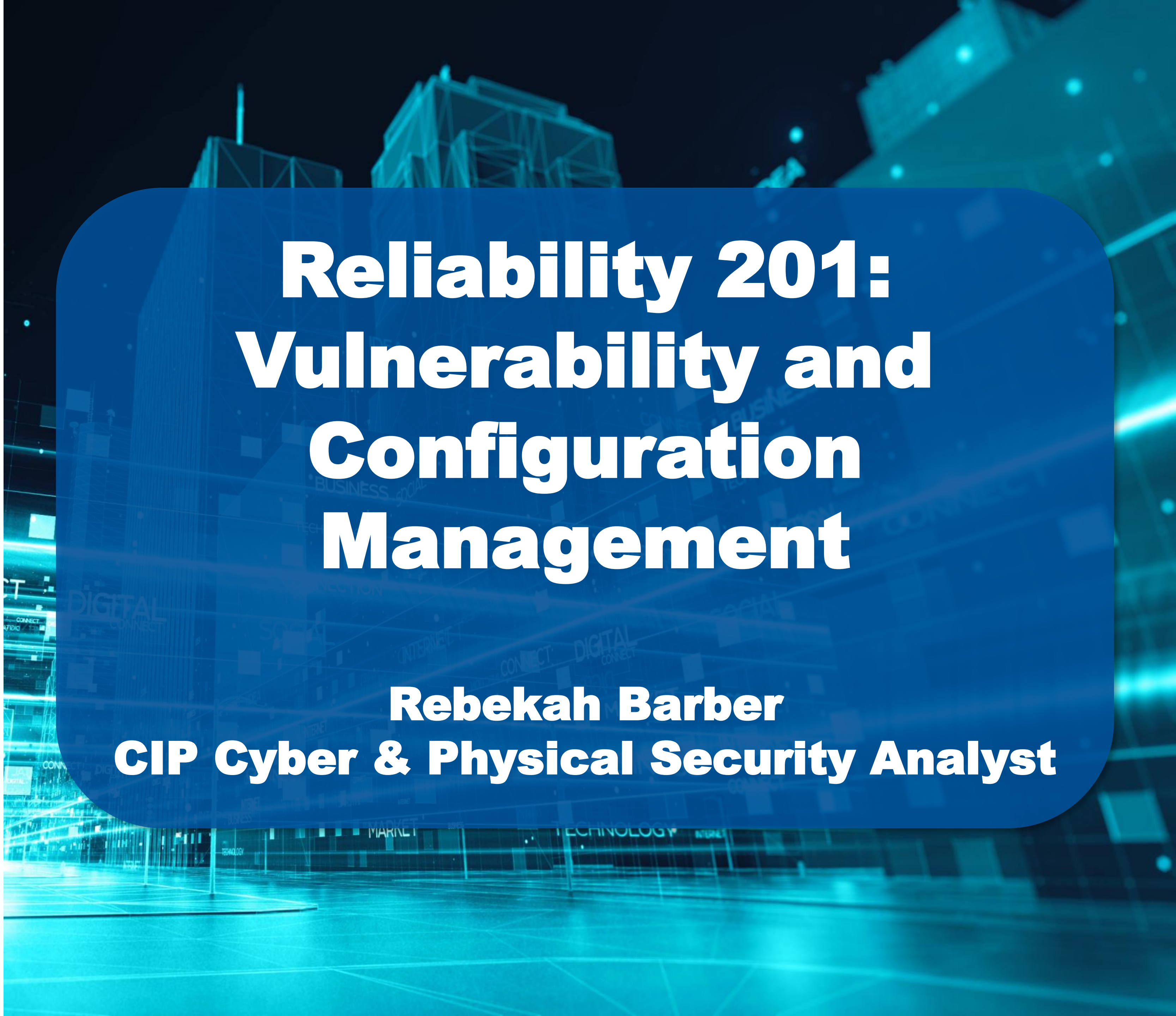
RELIABILITY 101 & 201



Reliability 201: Vulnerability and Configuration Management

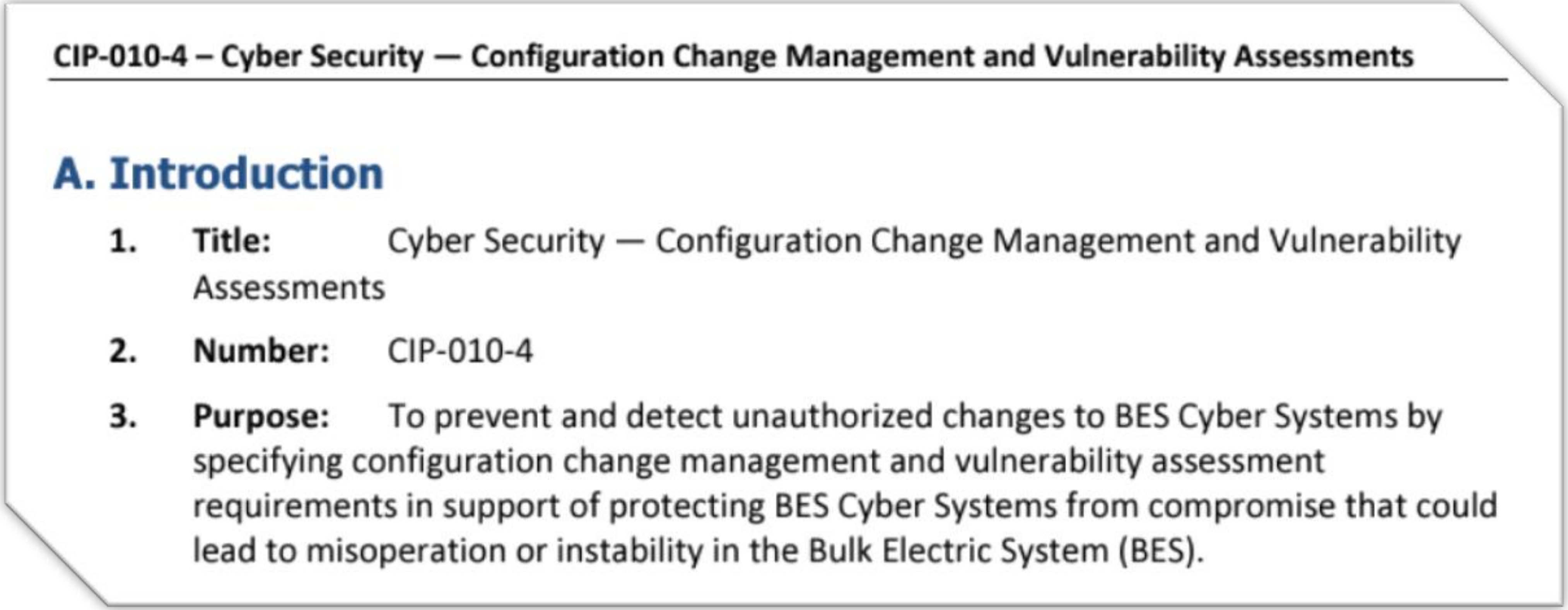
Rebekah Barber
CIP Cyber & Physical Security Analyst

Antitrust Admonition

Texas Reliability Entity, Inc. (Texas RE) strictly prohibits persons participating in Texas RE activities from using their participation as a forum for engaging in practices or communications that violate antitrust laws. Texas RE has approved antitrust guidelines available on its website. If you believe that antitrust laws have been violated at a Texas RE meeting, or if you have any questions about the antitrust guidelines, please contact the Texas RE General Counsel.

Notice of this meeting was posted on the Texas RE website and this meeting is being held in public. Participants should keep in mind that the listening audience may include members of the press, representatives from various governmental authorities, and industry stakeholders.

The Purpose



CIP-010-4 – Cyber Security — Configuration Change Management and Vulnerability Assessments

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-4

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

CIP-010-4 R1 and R2

Baselines

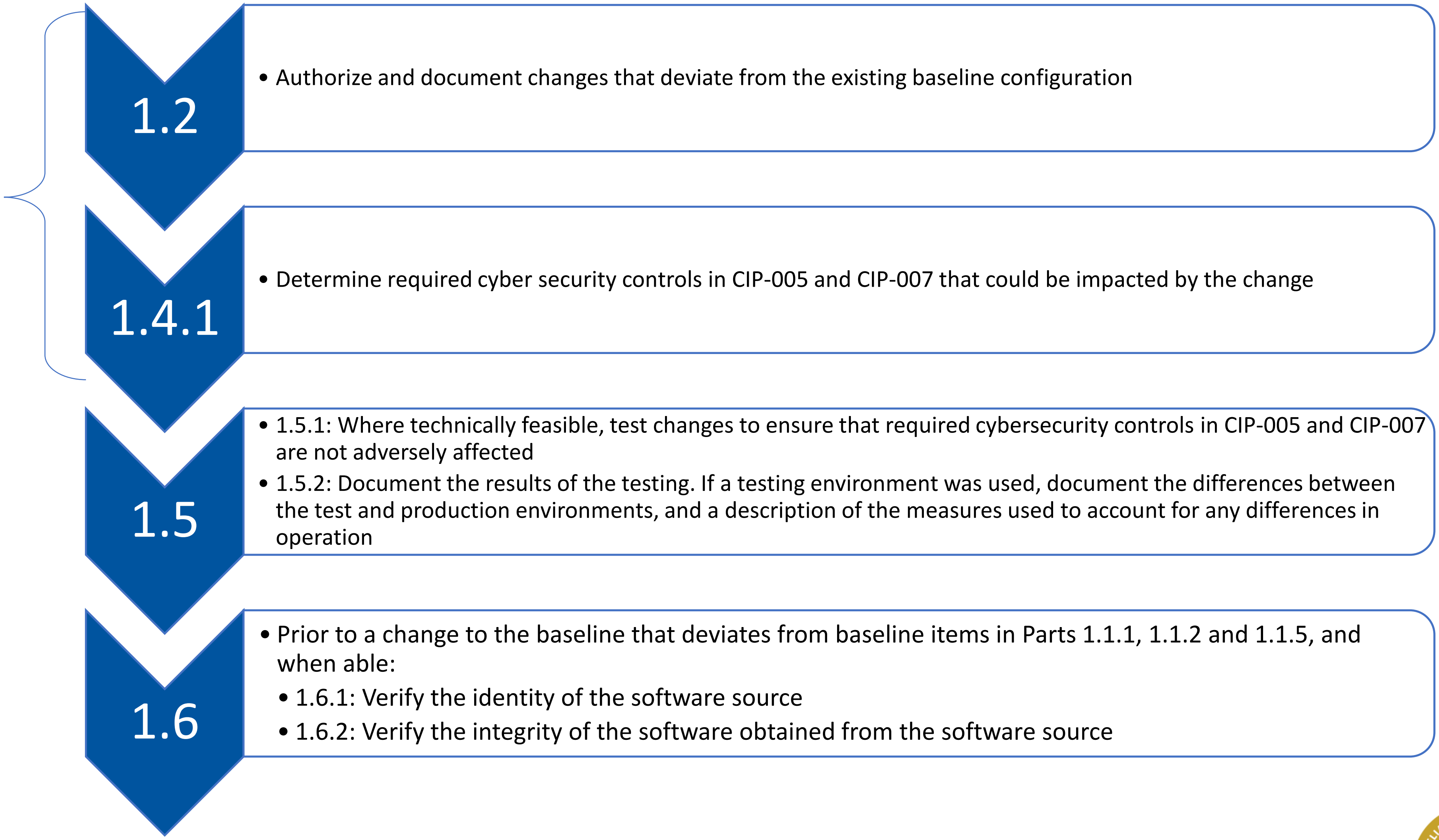
Establishing the Baseline

R1 Part 1.1: Develop a baseline configuration individually or by group, which shall include the following items:

- 1.1.1. Operating systems(s) (including version) or firmware where no independent operating system exists
- 1.1.2. Any commercially available or open-source application software (including version) intentionally installed
- 1.1.3. Any custom software installed
- 1.1.4. Any logical network accessible ports
- 1.1.5. Any security patches applied

High & Medium Impact BES Cyber Systems and their Associated EACMS, PACS, and PCA

Pre-Change to the Baseline



High & Medium Impact BES Cyber Systems and their associated EACMS, PACS, and PCA

1.2

- Authorize and document changes that deviate from the existing baseline configuration

1.4.1

- Determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change

High Impact BES Cyber Systems

1.5

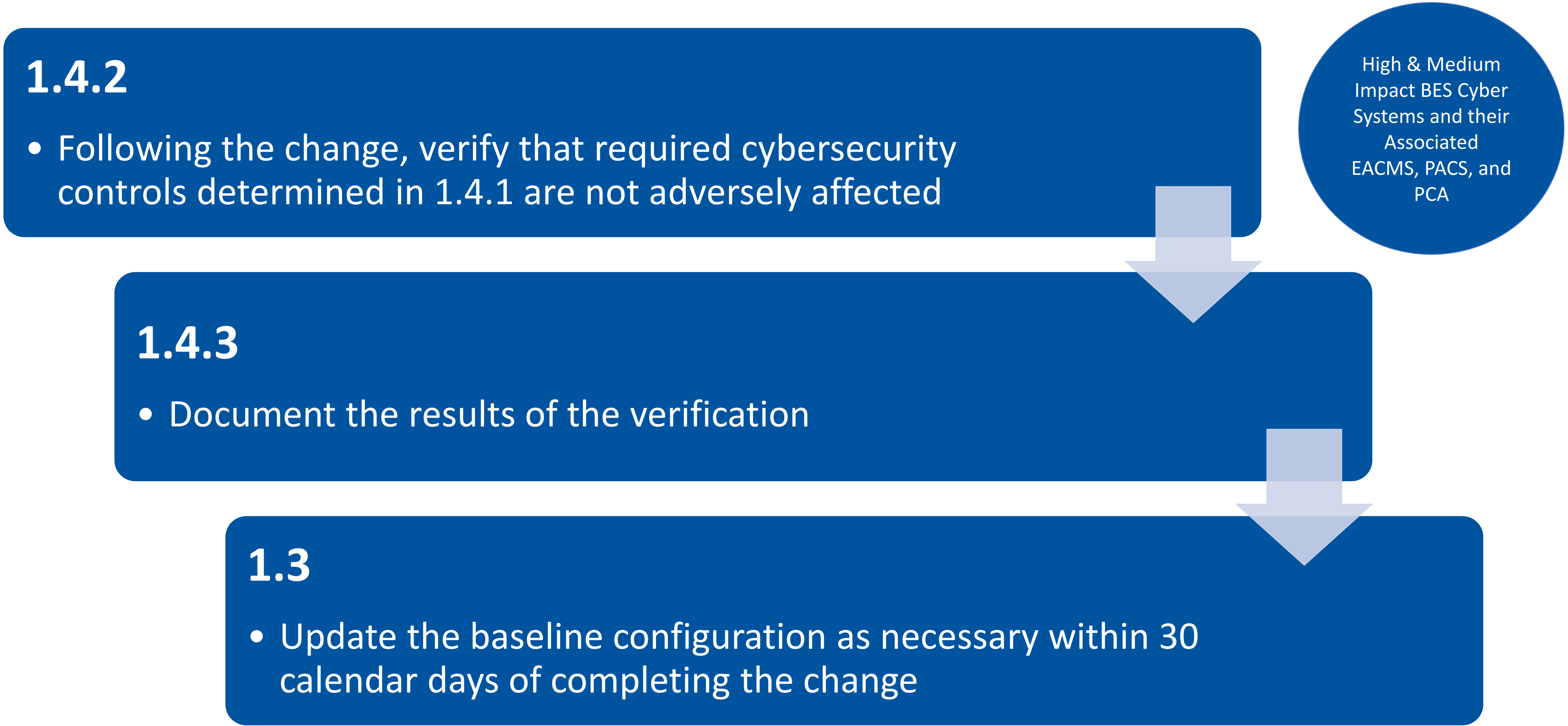
- 1.5.1: Where technically feasible, test changes to ensure that required cybersecurity controls in CIP-005 and CIP-007 are not adversely affected
- 1.5.2: Document the results of the testing. If a testing environment was used, document the differences between the test and production environments, and a description of the measures used to account for any differences in operation

High & Medium Impact BES Cyber Systems and their associated EACMS and PACS

1.6

- Prior to a change to the baseline that deviates from baseline items in Parts 1.1.1, 1.1.2 and 1.1.5, and when able:
  - 1.6.1: Verify the identity of the software source
  - 1.6.2: Verify the integrity of the software obtained from the software source

Post-Change to the Baseline



High & Medium Impact BES Cyber Systems and their Associated EACMS, PACS, and PCA

1.4.2

- Following the change, verify that required cybersecurity controls determined in 1.4.1 are not adversely affected

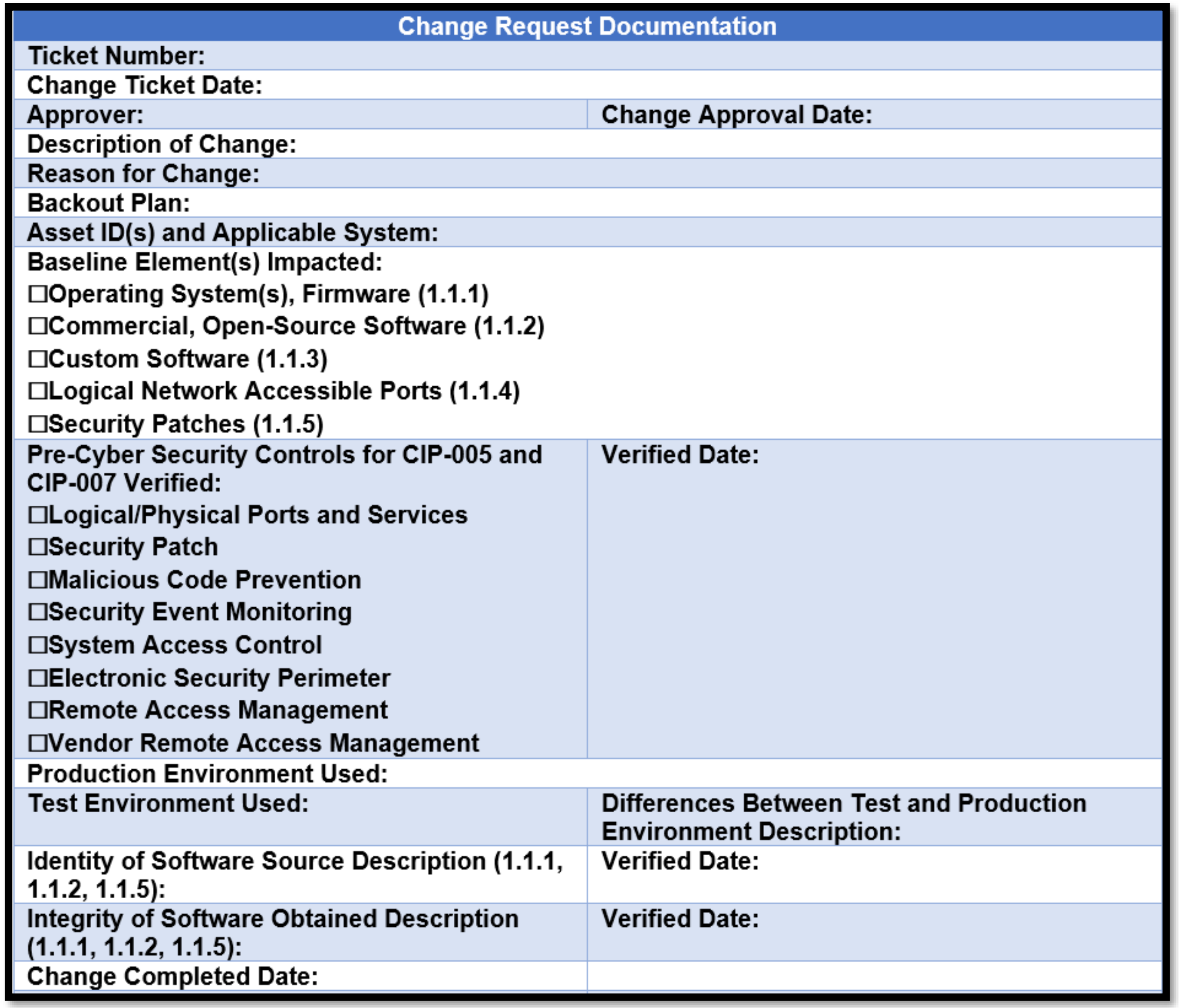
1.4.3

- Document the results of the verification

1.3

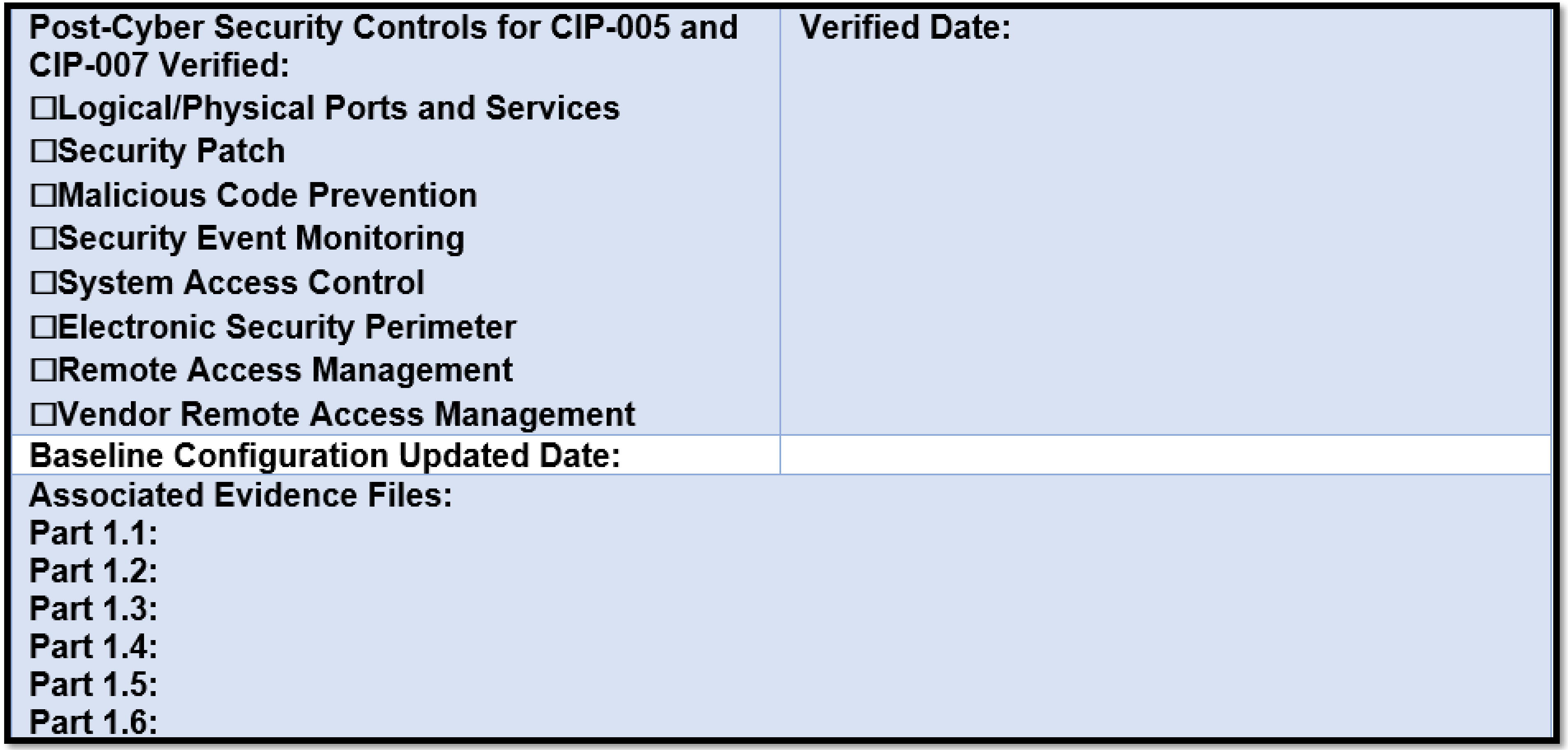
- Update the baseline configuration as necessary within 30 calendar days of completing the change

Example Change Ticket – Pre-Change



Change Request Documentation	
Ticket Number:	
Change Ticket Date:	
Approver:	Change Approval Date:
Description of Change:	
Reason for Change:	
Backout Plan:	
Asset ID(s) and Applicable System:	
Baseline Element(s) Impacted: ☐Operating System(s), Firmware (1.1.1) ☐Commercial, Open-Source Software (1.1.2) ☐Custom Software (1.1.3) ☐Logical Network Accessible Ports (1.1.4) ☐Security Patches (1.1.5)	
Pre-Cyber Security Controls for CIP-005 and CIP-007 Verified: ☐Logical/Physical Ports and Services ☐Security Patch ☐Malicious Code Prevention ☐Security Event Monitoring ☐System Access Control ☐Electronic Security Perimeter ☐Remote Access Management ☐Vendor Remote Access Management	Verified Date:
Production Environment Used:	
Test Environment Used:	Differences Between Test and Production Environment Description:
Identity of Software Source Description (1.1.1, 1.1.2, 1.1.5):	Verified Date:
Integrity of Software Obtained Description (1.1.1, 1.1.2, 1.1.5):	Verified Date:
Change Completed Date:	

Example Change Ticket – Post-Change



Post-Cyber Security Controls for CIP-005 and CIP-007 Verified: □Logical/Physical Ports and Services □Security Patch □Malicious Code Prevention □Security Event Monitoring □System Access Control □Electronic Security Perimeter □Remote Access Management □Vendor Remote Access Management	Verified Date:
Baseline Configuration Updated Date:	
Associated Evidence Files: Part 1.1: Part 1.2: Part 1.3: Part 1.4: Part 1.5: Part 1.6:	

Monitoring for Changes

R2: High Impact BES Cyber Systems

- Monitor for changes to the baseline configuration at least once every 35 calendar days
- Document and investigate any detected unauthorized changes

CIP-010-4 R3

Vulnerability Assessments

Vulnerability Assessments

High & Medium Impact BES Cyber Systems and their associated EACMS, PACS, and PCA	3.1	Conduct a paper or active vulnerability assessment at least once every 15 calendar months
High Impact BES Cyber Systems	3.2	Where able, perform an active vulnerability assessment in a test or production environment at least once every 36 calendar months Document the results of the testing, and if a test environment was used, the differences between the test and production environment
High impact BES Cyber Systems and their associated EACMS and PCA	3.3	Prior to adding a new applicable Cyber Asset to production, perform an active vulnerability assessment, except under CIP exceptional circumstances and for Cyber Assets that model an existing baseline configuration of an existing Cyber Asset

Vulnerability Assessments

High & Medium Impact BES Cyber Systems and their Associated EACMS, PACS, and PCA

3.4: Document the results of the assessments and the action plan created to remediate or mitigate any vulnerabilities identified including the planned date of completion and execution status.

Best Practices

DETAILED PROCESS DOCUMENTATION

LAYERED INTERNAL CONTROLS

AUTOMATION

Contact Us

Texas Reliability Entity, Inc.

Email: compliance@texasre.org

Phone: 512-583-4900