

Controls and RISC

NPCC Entity Risk Assessment (ERA) Group

NPCC 2019 Spring Compliance Workshop
Mystic CT
May 22, 2019



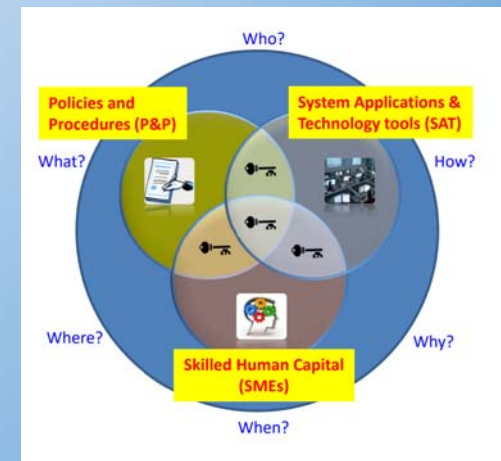
Ben Eng

NPCC, Manager ERA

CONTROLS - What are they?

- a) Procedures, Policies, Guides, Practices, Instructions, Studies
- b) Spreadsheets, Databases, Lists, Passwords, Patches, Barriers, Work Management, Reminders
- c) Staff, contractors; trained to do their jobs; certified if necessary
- d) All of the above

<https://www.npcc.org/Compliance/Entity%20Risk%20Assessment/Forms/Public%20List.aspx>



CONTROLS - Why do we have controls?



- a) Because I'm a "Control Freak" and I like to be in charge.
- b) Because if I don't have them, I'll be found non-Compliant during a NERC Audit, Spot Check or Self Certification.
- c) Because it's in vogue to have them. Everyone else says they have them and I don't want to be the odd person that doesn't.
- d) Because fully implemented controls (tested and monitored) help ensure consistent, rigorous achievement of goals in a timely manner. Controls are used to mitigate Risks.
- e) All of the above

RISKS – What are they?



- a) a situation involving exposure to danger.
- b) the possibility of losing something of value (such as physical health, social status, emotional well-being, or financial wealth) resulting from a given action or inaction, planned or unplanned).
- c) Vary depending on your “environment”: Health, Safety, Financial, Career, Education, Travel, Weather, City/Rural, Gender, Religion, Politics....
- d) Can be mitigated to an acceptable level by use of controls
- e) All of the above

RISK QUESTIONS - Relevant to your role in the Electric Power Industry



Q1: Are my personal risks the same as my company's risks?

A1: No, they are not

Q2: How do I find out what Risks affect my company?

A2: Great news! The *ERO Reliability Risk Priorities Report* published in 2018 provides a comprehensive prioritized list of Risks relevant to the Electric Power Industry

<https://www.nerc.com/comm/RISC/Related%20Files%20DL/ERO-Reliability- Risk Priorities- Report Board Accepted February 2018.pdf>

Reliability Issues Steering Committee (RISC) Report Excerpts



Key Observations: Note item 4

The RISC has identified a number of key observations regarding emerging risks to the reliability of the BPS to focus the industry's efforts. These key observations are:

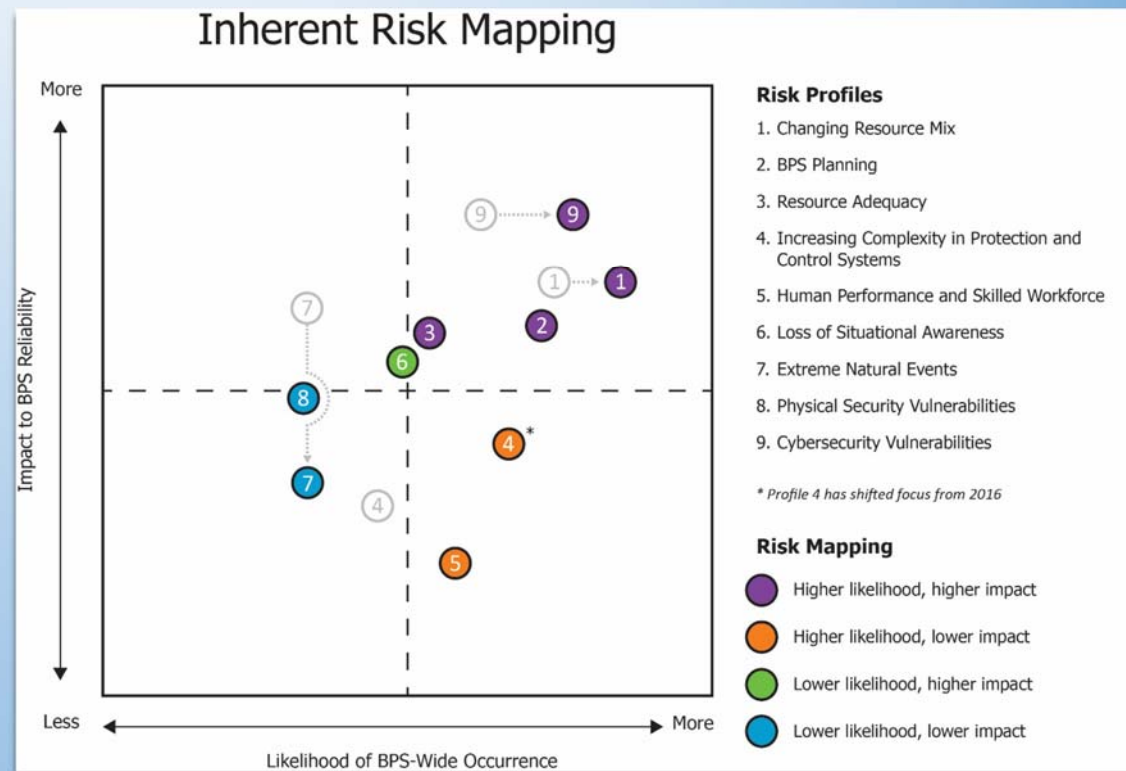
1. The fast pace of change of the resource mix;
2. Interdependence between the energy and communication sectors;
3. Increased complexity of the power system's automated control systems due to the increased use of power electronics and digital controls, and the risks of negative interaction between those control systems;
4. Ongoing evolution and complexity from determined actors using cyber technologies;
5. Changing workforce skills needed to reliably implement the new control facilities involved in the power system; and
6. Addressing BPS impacts associated with emerging reliability risks is placing increased demands for coordination among policy makers and regulatory authorities, including the need for increased coordination among provincial, federal, and state regulatory authorities, with due consideration of jurisdictional boundaries.

Reliability Issues Steering Committee (RISC) Report Excerpts

“...the RISC recommends the highest priority be given to those risk profiles that have been identified as having the higher likelihood/higher impact.”

Higher Likelihood, Higher Impact

- Cybersecurity Vulnerabilities (RP #9)
- Changing Resource Mix (RP #1)
- BPS Planning (RP #2)
- Resource Adequacy (RP #3)



End of Presentation “A”



Thank you

Please provide your attention to the next presenters:
Mike Bilheimer, Duong Le and Emile Khan



Controls for Cyber Security Risks

NPCC Entity Risk Assessment (ERA) Group



NPCC 2019 Spring Compliance Workshop
May 22, 2019
Mystic, CT

Identified Risks – Presentation Focus



- ERO Reliability Risk Priorities, February 2018
 - **Risk Profile #9: Cybersecurity Vulnerabilities**
 - **Risk #6** - A lack of staff that is knowledgeable and experienced in cybersecurity of control systems and supporting IT/OT networks (historically separate organizations and skillsets). This risk is symptomatic across all industries and is a risk because it hinders an organization's ability to prevent, detect, and respond to cyber incidents due to organizational silos.
 - **Risk #7** -The rapid growth in sophistication and widespread availability of tools and processes designed to exploit vulnerabilities and weaknesses in BPS technologies and in connected IT networks and systems

Source: https://www.nerc.com/comm/risc/related%20files%20dl/ero-reliability-risk_priorities-report_board_accepted_february_2018.pdf

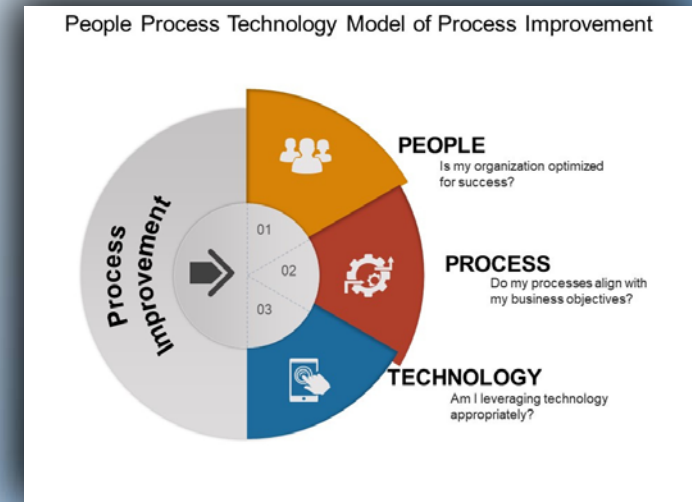
2018 RISC Report – Controls

Each control should identify key elements that ensure effective and efficient operation:

- People
- Process
- Technology

Each of these elements should contain the following attributes :

- Development
- Implementation/Maintenance
- Continuous Improvement



Controls should be **both effective and efficient**. Development, implementation /maintenance and continuous improvement are critical.

2018 RISC Report – Cyber Risk #6 - A lack of staff that is knowledgeable and experienced in cybersecurity of control systems and supporting IT/OT networks (historically separate organizations and skillsets). This risk is symptomatic across all industries and is a risk because it hinders an organization's ability to prevent, detect, and respond to cyber incidents due to organizational silos.



Key Inputs for Control Design:

Entity Staffing Levels

- Do you have adequate staffing resources?
- Can current staffing level support the organization as it grows?

Organizational Silos

- Internal Department/Group Coordination
- Senior leadership involvement and oversight
- Historically separate organizations and skillsets
- Ownership of Task
- Cross Training

Hiring Requirements

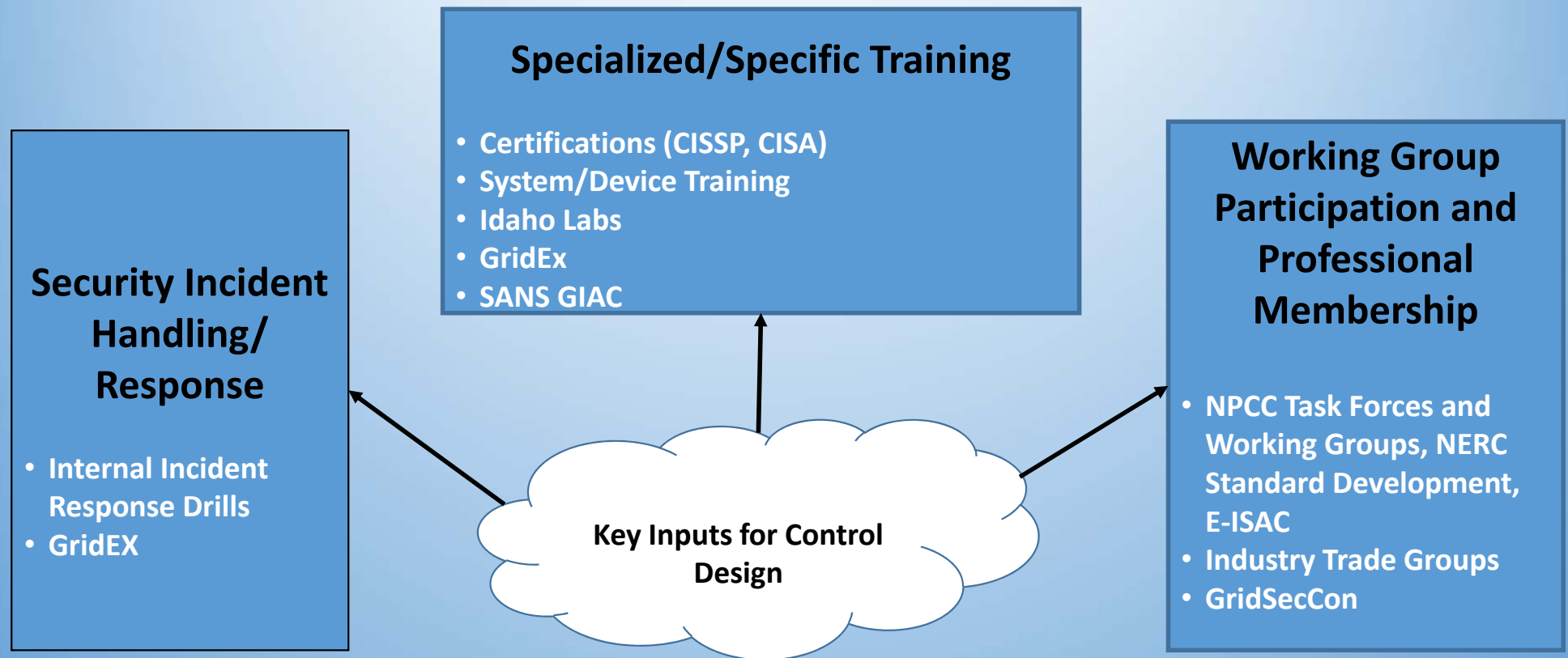
- Position Required Skill Sets
- Contractor Vs Employee

Staff Knowledge and Experience

- Does the Entity Staff have the correct knowledge and experience to maintain the cyber systems they are responsible for?

These elements should be considered for designing key controls for this risk.

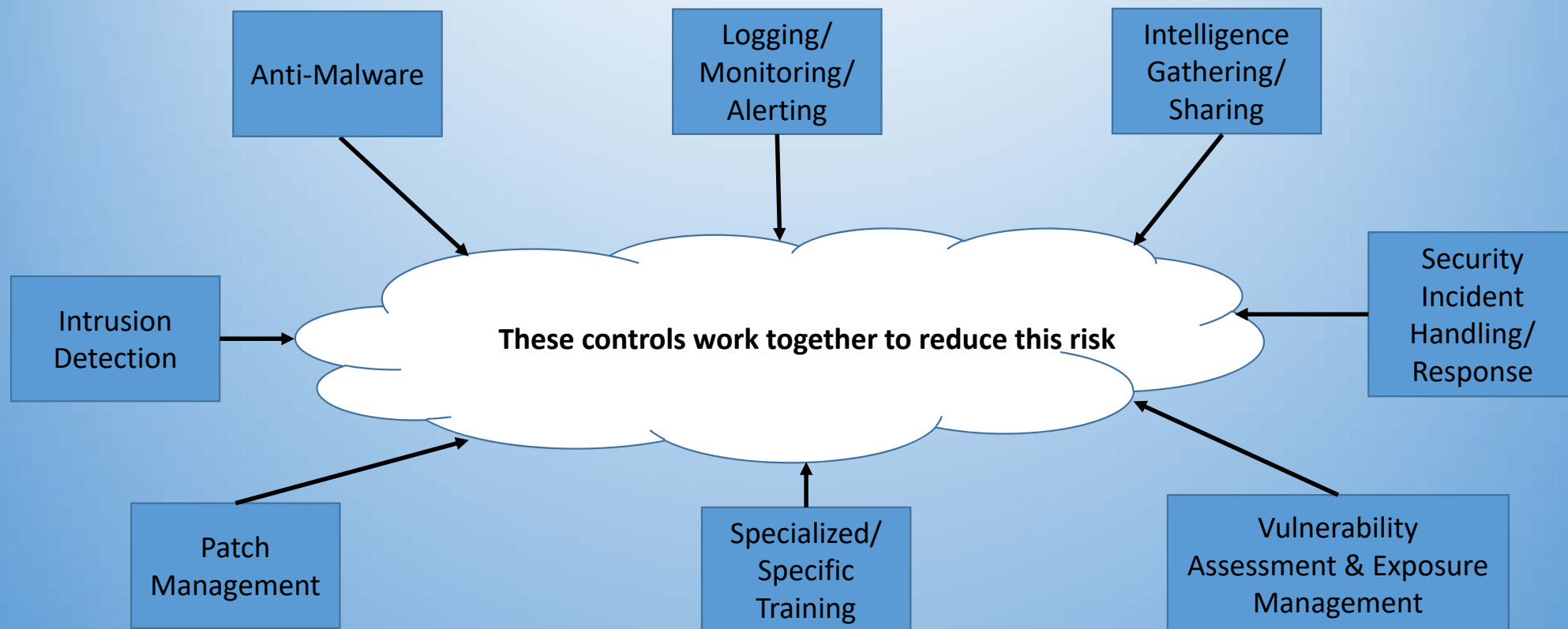
2018 RISC Report – Human Capital Knowledge and Experience



2018 RISC Report – Cyber Risk #7 - The rapid growth in sophistication and widespread availability of tools and processes designed to exploit vulnerabilities and weaknesses in BPS technologies and in connected IT networks and systems.



Key Controls/Control Areas for this Risk:



2018 RISC Report – People, Process, Technology



Intrusion Detection

People – Security Architecture, Security Operations Team, Audit/Compliance

Process – Monitoring, Update, Detection, Response

Technology – NIDS, HIDS, Network/Host/Application Firewalls, Exercises

Intelligence Gathering/Sharing

People – Security Architecture, Security Operations Team, Audit/Compliance, Vendors

Process – Intelligence Gathering/Evaluation/Sharing

Technology – Intelligence Sharing Platforms/Services

Patch Management

People – Security Architecture, Security Operations Team, System Administrators, Vendors

Process – Patch Monitoring, Patch Assessment, Patch Deployment, Vulnerability Assessment

Technology – Patch Monitoring, Patch Deployment, Vulnerability Assessment

Anti-Malware

People – Security Architecture, System Administrators, End User, Security Operations Team, Audit/Compliance

Process – Monitoring, Update, Detection, Response, Hardening

Technology – NIDS, HIDS, AV, Whitelisting

Specialized/Specific Training

People – Security Architecture, Security Operations Team, Human Resources, System Administrators, Users

Process – Skills/Knowledge Assessment, Training Plan

Technology – Training Systems/Platforms, Skills Assessment, Exercises

Vulnerability Assessment & Exposure Management

People – Security Architecture, System Administrators, Security Operations Team, Audit/Compliance, Vendors

Process – Vulnerability Assessment, Exposure Mitigation

Technology – Vulnerability Assessment Tools, Exercises

Logging/Monitoring/Alerting

People – Security Architecture, System Administrators, End User, Security Operations Team, Audit/Compliance, Vendors

Process – Monitoring, Log Review, Detection, Response

Technology – Cyber Assets, Log Collection, SEIM, Exercises

Security Incident Handling/Response

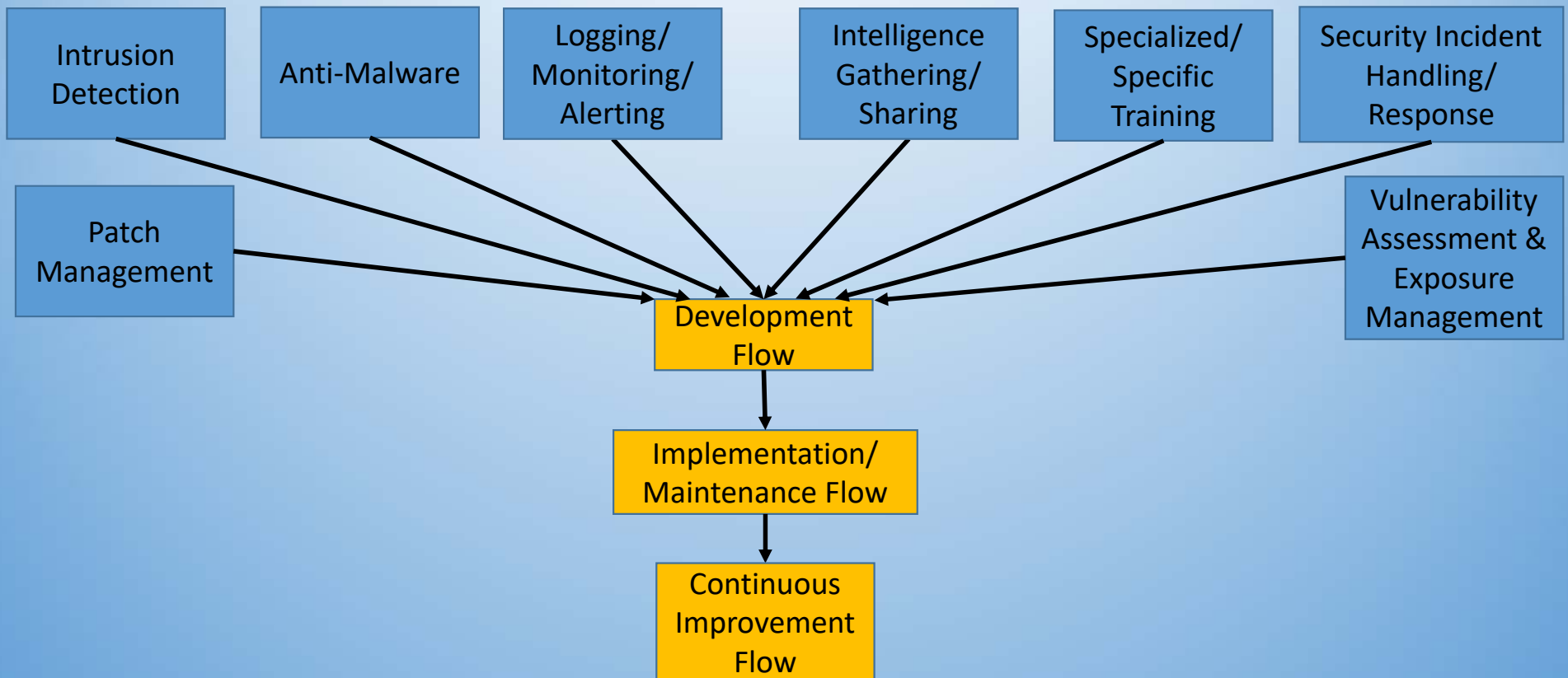
People – Security Architecture, Security Operations Team, Audit/Compliance, System/Network Administrators, Vendors

Process – Identify, Contain, Eradicate, Recover, Improvement

Technology – Investigation, SEIM, Evidence Preservation, System Images, Recovery, Exercises

2018 RISC Report – Cyber Risk #7

Control Flow Development, Implementation/Maintenance, Continuous Improvement:



2018 RISC Report – Control Flow: Development

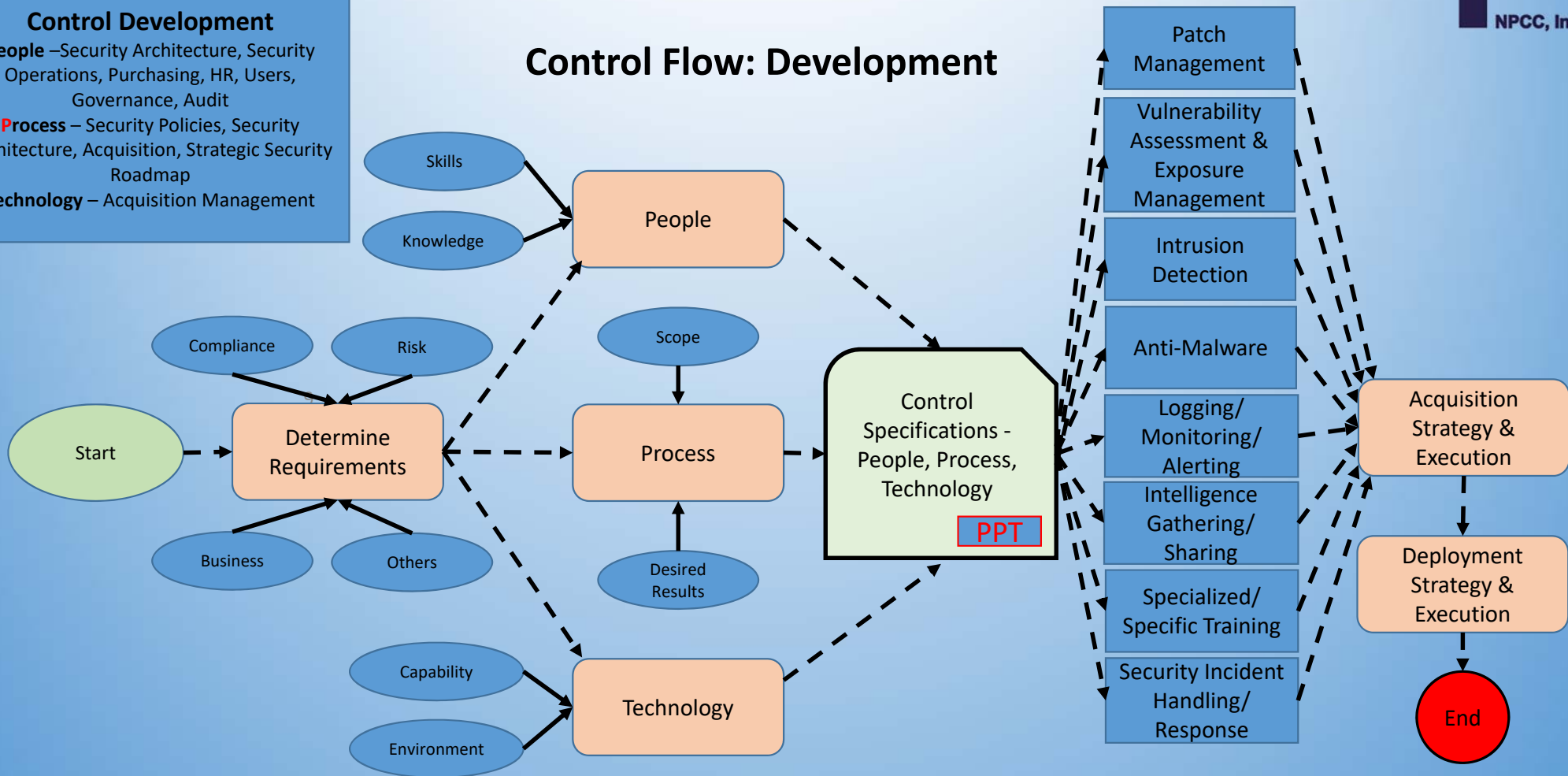
Control Development

People – Security Architecture, Security Operations, Purchasing, HR, Users, Governance, Audit

Process – Security Policies, Security Architecture, Acquisition, Strategic Security Roadmap

Technology – Acquisition Management

Control Flow: Development



2018 RISC Report Risk #7 – Control Flow: Implementation/Maintenance

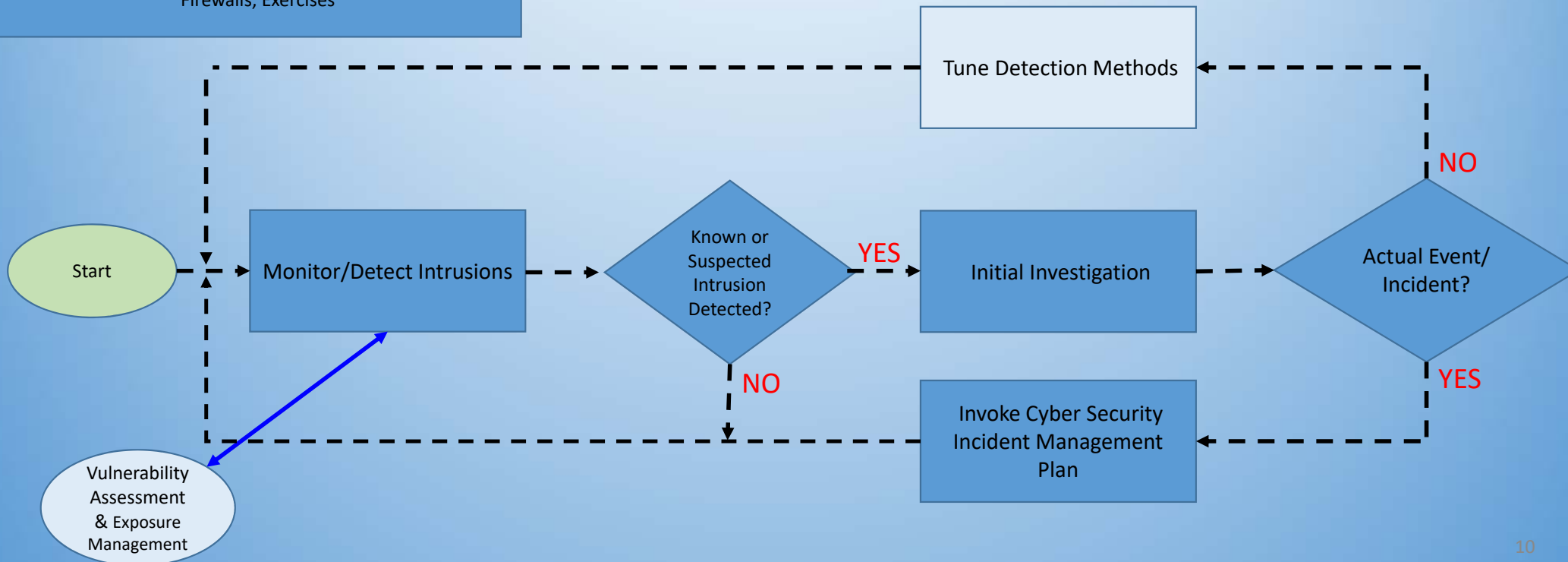


Intrusion Detection

People – Security Architecture, Security Operations Team, Audit/Compliance

Process – Monitoring, Update, Detection, Response

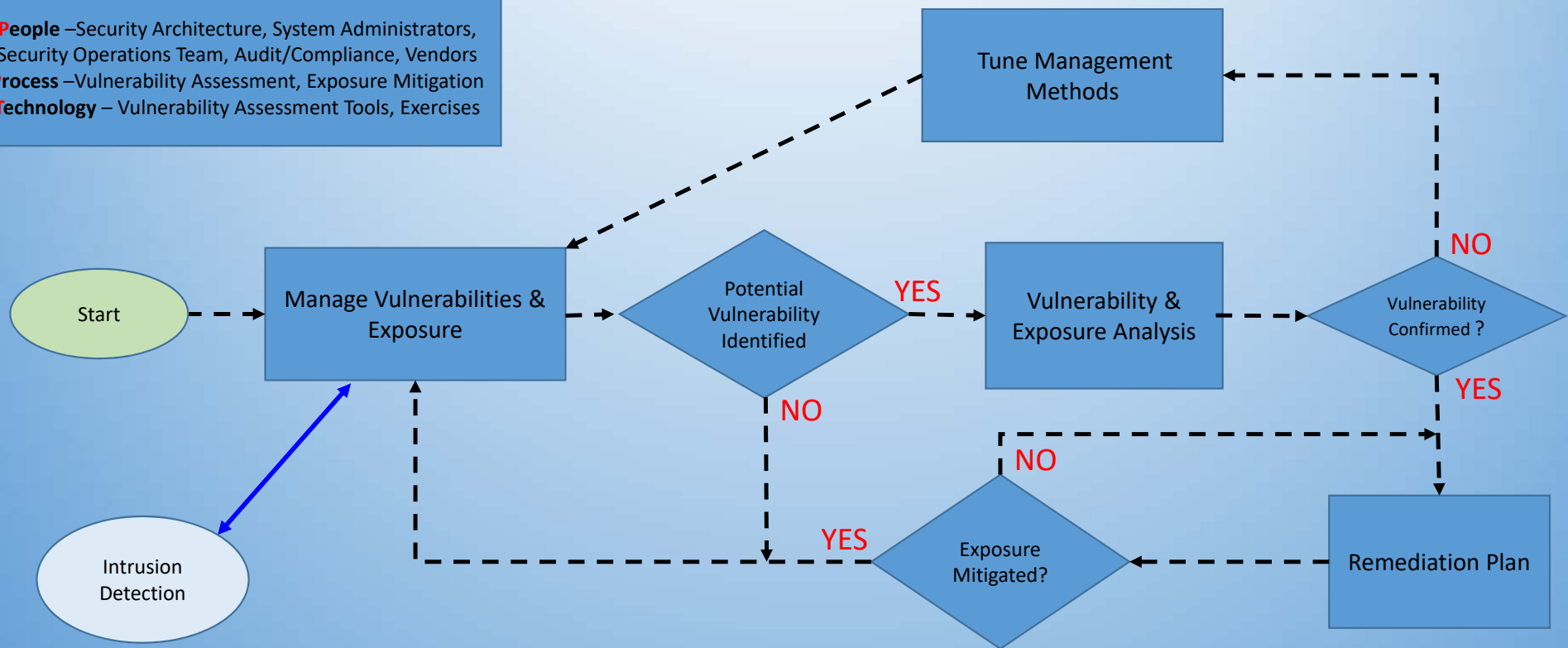
Technology – NIDS, HIDS, Network/Host/Application Firewalls, Exercises



2018 RISC Report Risk #7 – Control Flow: Implementation/Maintenance

Vulnerability Assessment & Exposure Management

People –Security Architecture, System Administrators, Security Operations Team, Audit/Compliance, Vendors
Process –Vulnerability Assessment, Exposure Mitigation
Technology – Vulnerability Assessment Tools, Exercises



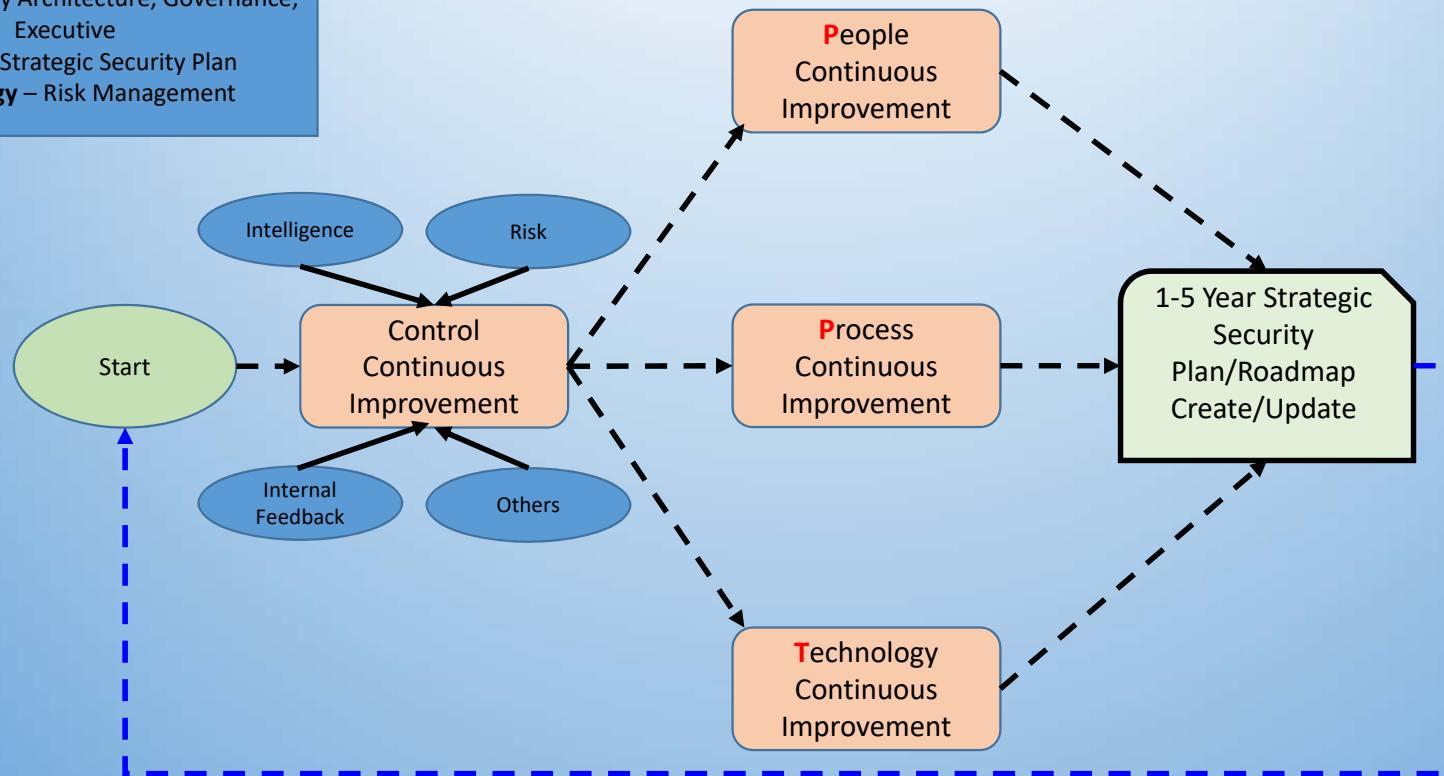
2018 RISC Report – Control Flow: Continuous Improvement

Control Continuous Improvement

People – Security Architecture, Governance, Executive

Process – Strategic Security Plan

Technology – Risk Management



Summary



Key points to consider:

- Identify and document **People, Process, Technology** Key Controls/Control Areas
- Develop Control Flows for **Development, Implementation/Maintenance and Continuous Improvement**
- One size doesn't fit all

Questions?

Email: ERA@NPCC.org





Compliance Monitoring

John Muir

Director, Compliance Monitoring

Agenda

- Standards Update
- Compliance Oversight Plans
- New Evidence Submittal Process
- PRC-005 Data Requests
- CIP Evidence Request Tool
- BES Cyber System Questionnaire



Standards Updates

1/1/19

BAL-005-1. Replaced BAL-005-0.2b and BAL-006-2

FAC-001-3. Replaced FAC-001-2

TOs to ensure that new or materially modified Facilities must be within a BA's metered boundary.

4/1/19

BAL-002-3. Replaced BAL-002-2(i).

Clarified exception to Requirement 1.1.

EOP-004-4. Replaced EOP-004-3.

EOP-005-3. Replaced EOP-005-2.

EOP-006-3. Replaced EOP-006-2.

EOP-008-2. Replaced EOP-008-1.

Clarifies the critical methodology requirements for Emergency Operations, while ensuring strong planning, reporting, communication and coordination across the Functional Entities. In addition, the revisions are intended to streamline the standards and apply Paragraph 81 criteria.



Standards Updates

7/1/19

PER-003-2. Replaces PER-003-1.

Defines NERC certificates as identified in the NERC System Operator Certification Program Manual.

TPL-007-3. Replaces TPL-007-1, Supersedes TPL-007-2

Mitigate the risk of instability, uncontrolled separation, and Cascading as a result of geomagnetic disturbances (GMDs) through application of Operating Procedures and strategies that address potential impacts identified in a registered entity's assessment.

1/1/20

CIP-003-7. Replaces CIP-003-6

Revised to address (1) the definition of LERC and (2) transient devices.

Standards Updates

7/1/20

CIP-005-6. Replaces CIP-005-5.

SPS-RAS

Part 2.4 method to determine remote access sessions

Part 2.5 method to disable active remote access sessions

CIP-010-3. Replaces CIP-010-2.

SPS-RAS

Part 1.6 for existing baseline deviation, verify identity of source and integrity of software.

CIP-013-1. New.

Develop, implement and review supply chain risk management plans for high and medium BCS

Standards Updates

10/1/20

PRC-027-1. New.

Establish a process for developing new and revised Protection System settings for BES Elements to operate in the intended sequence during Faults; and stipulates certain attributes that must be included in the process.

Periodically perform Protection System Coordination Studies and/or compare existing Fault current values to established Fault current baselines for Protection Systems applied on BES Elements that are identified as being affected by changes in Fault current. (10/1/2026)

Utilize the process established in accordance with Requirement R1.

PER-006-1 New.

GO plant personnel responsible for Real-time control to train on the operational functionality of Protection Systems and RAS that affect generating Facility output.

Compliance Oversight Plans

- COP Template approved for ERO-wide use.
- Captures how an Region will monitor a registered entity's compliance with selected NERC Reliability Standards based on entity-specific risks.
- Does NOT change any obligation for a registered entity to be compliant with all NERC Reliability Standards.
- Will be generated for each entity that is on the schedule for 2019, and shared with the entity.
- Eventually every entity will have one.

Compliance Oversight Plans

Contents:

- Purpose – What it is and is not.
- Analysis and Results – Communicates identified risks for the specific registered entity
- Oversight Strategy – Places the entity in one of 4 categories to prioritize compliance monitoring
- Appendices: IRA Results Summary, ICE Results Summary, Standards / Requirements associated with identified risks

New Evidence Submittal Process

- Beginning in 2019, no longer using the Submittal folder on NPCC Drive
- Each entity will have their own folder on NPCC Drive for an on-site or off-site audit
- Will be used by the entity to submit audit documentation, i.e. completed RSAWs, evidence, completed ETS', pre-audit data
- Will be used by the NPCC Audit Team to share documentation with the entity, i.e. ETS, PRC-005 sampling, audit reports

New Evidence Submittal Process (cont'd)

- A link to the folder for your audit and password needed to access the folder will be provided to you during the audit kickoff call
- Updated Submittal Instructions provided with the Audit Notification Package

Pre-Audit Data Requests

GO/TO

- List of BES equipment that has been modified or replaced during the audit period.
- List of the protection equipment that is covered under PRC-005

Company supplied spreadsheet (Excel only) ensure the spreadsheet contains the following for each piece of equipment:

equipment ID

last (previous) test date

current test date

next scheduled test date

Battery type (NICAD, VRLA, VLA)



Pre-Audit Data Requests

GO

- Provide one-line diagrams of your facilities, indicating interconnection point and ownership demarcation where appropriate.

TO

- Provide a system diagram of your BES.



CIP Evidence Request Tool

Evidence Request Tool now Mandatory

- Effective May 1st, all entities receiving an onsite CIP audit will be required to use the CIP Evidence Request Tool (ERT).
- The tool must be completed in full.
- However, as an alternative to submitting the ERT to NPCC, audited entities may make the ERT available for remote offsite review and submit redacted lists to NPCC to support evidence sampling processes.

Handling and Retention of Evidence

- You will be asked to upload all audit submittals including the ERT to NPCC Drive
- The Primary Auditor will move your submittal to a secure server that is owned, maintained and physically resides in a protected zone within NPCC's office
- Access (electronic and physical) to this server is highly restricted
- All evidence is handled and retained in accordance with applicable NPCC policies and procedures
- NPCC will maintain the official audit record
- For those entities that provide only remote access to their data, an encrypted flash drive will be used as the official audit record, and all evidence that is provided for the audit will be copied there.

Handling and Retention of Evidence

- For those entities that provide only remote access to their data
 - an encrypted flash drive will be used as the official audit record, and all evidence that is provided for the audit will be copied there.
 - All presentations, ERT and or Evidence Tracking Sheets, will also be collected onto the flash drive.
 - The flash drive will be retained by the entity under a Custodial Agreement, until the completion of the next audit.

The ERT's Structure

- An Excel workbook with 19 worksheets or tabs
- 4 tabs contains evidence requests
- 14 tabs are to be completed by the audited entity

Key Pre-Audit ERT Milestones

Day 0: You will receive the Audit Notification Letter

Day 30: Pre-audit Survey and Level 1 requests are due

Day 90: RSAWs and supporting evidence, Level 2 requests and NPCC specific requests are due

Day 104: You may receive 'Level 3' requests, which are requests beyond what is in the ERT

Day 114: Responses to 'Level 3' requests are due

Day 120: Onsite portion of audit begins

Handling of Level 3 Requests and Beyond

- Level 3 requests and beyond will be tracked using NPCC's Evidence Tracking Sheets (ETS), which many of you are already familiar with
- Level 4 requests and beyond would be considered onsite requests

Additional Notes

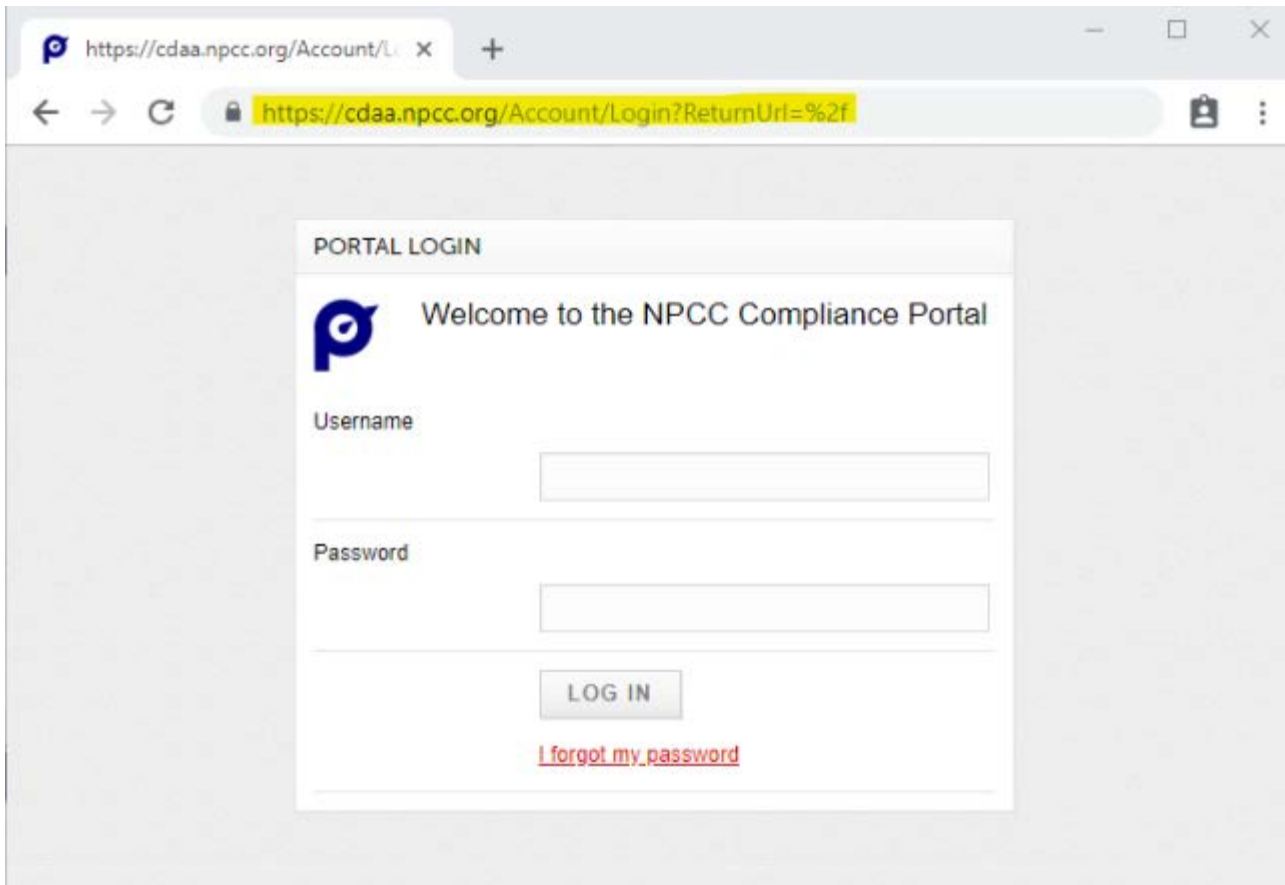
- You will still be required to submit RSAWs, but you can cite any evidence that you may have already supplied in response to an ERT request in your RSAW so that you don't have to submit the evidence twice
- In addition to any cited evidence you may have already provided, you may need to provide a supplemental submittal to support your RSAW responses



BES Cyber System Questionnaire

- Located in the CDAA on your Company Info page
- Replaces the previous questions that asked you to indicate whether you had CCAs
- Three new questions:
 - Do you have high impact BES Cyber Systems?
 - Do you have medium impact BES Cyber Systems?
 - Do you have low impact BES Cyber Systems?
- Responses are simply 'Yes' or 'No' and will only be used for planning purposes (audits, self-certs, etc.)
- We had asked for your responses by February 1, 2019
- 102 Entities have not responded. We will be sending out a reminder next week.
- Thank you to the 112 that have.

Step 1 – Login to the CDAA



A screenshot of a web browser displaying the NPCC Compliance Portal login page. The browser's address bar shows the URL <https://cdaa.npcc.org/Account/Login?ReturnUrl=%2f>. The page content includes a header "PORTAL LOGIN" and a welcome message "Welcome to the NPCC Compliance Portal" next to the NPCC logo. Below this, there are input fields for "Username" and "Password", a "LOG IN" button, and a red link that says "I forgot my password".

<https://cdaa.npcc.org>



Step 2 – Go to Company Info

NPCC Compliance Portal

HOME

SYSTEM ADMINISTRATION

> Change Password

> My Contact Information

> Search Contacts

> Add New Contact

> Company Info

TFES

SELF-CERTIFICATIONS

SELF-REPORTS

SCOPE EXPANSIONS

COMPLAINTS

MITIGATION PLANS

NON-COMPLIANCE

PERIODIC DATA SUBMITTALS

QUESTIONNAIRE

EDIT ENTITY: A TEST COMPANY

SAVE

CANCEL CHANGES

DELETE

CREATE PDF

MAILING ADDRESS

Address Line 1:

1 Window Place

Address Line 2:

City:

New York

Country:

US

State:

New York

Zip:

10000

BES CYBER SYSTEMS

Do you have high impact BES Cyber Systems? *

☐ Yes

☐ No

☒ Unspecified

Do you have medium impact BES Cyber Systems? *

☐ Yes

☐ No

☒ Unspecified

Do you have low impact BES Cyber Systems? *

☐ Yes

☐ No

☒ Unspecified

Step 3 – Select Responses

EDIT ENTITY: A TEST COMPANY

SAVE **CANCEL CHANGES** **DELETE** **CREATE PDF**

MAILING ADDRESS

Address Line 1:

1 Window Place

Address Line 2:

City:

New York

Country:

US

State:

New York

Zip:

10000

BES CYBER SYSTEMS

Do you have high impact BES Cyber Systems? *

☐ Yes

☒ No

☐ Unspecified

Do you have medium impact BES Cyber Systems? *

☒ Yes

☐ No

☐ Unspecified

Do you have low impact BES Cyber Systems? *

☐ Yes

☒ No

☐ Unspecified

Step 4 – Save Changes

EDIT ENTITY: A TEST COMPANY

SAVE CANCEL CHANGES DELETE CREATE PDF

MAILING ADDRESS

Address Line 1: 1 Window Place

Address Line 2:

City: New York

Country: US

State: New York

Zip: 10000

BES CYBER SYSTEMS

Do you have high impact BES Cyber Systems? * ☐ Yes ☒ No ☐ Unspecified

Do you have medium impact BES Cyber Systems? * ☒ Yes ☐ No ☐ Unspecified

Do you have low impact BES Cyber Systems? * ☐ Yes ☒ No ☐ Unspecified



Questions?

cip@npcc.org

Risk Assessment, Mitigation, and Enforcement Process

May 22, 2019

Scott Nied

Jenifer Vallace Farrell

Damase Hebert

Jason Wang

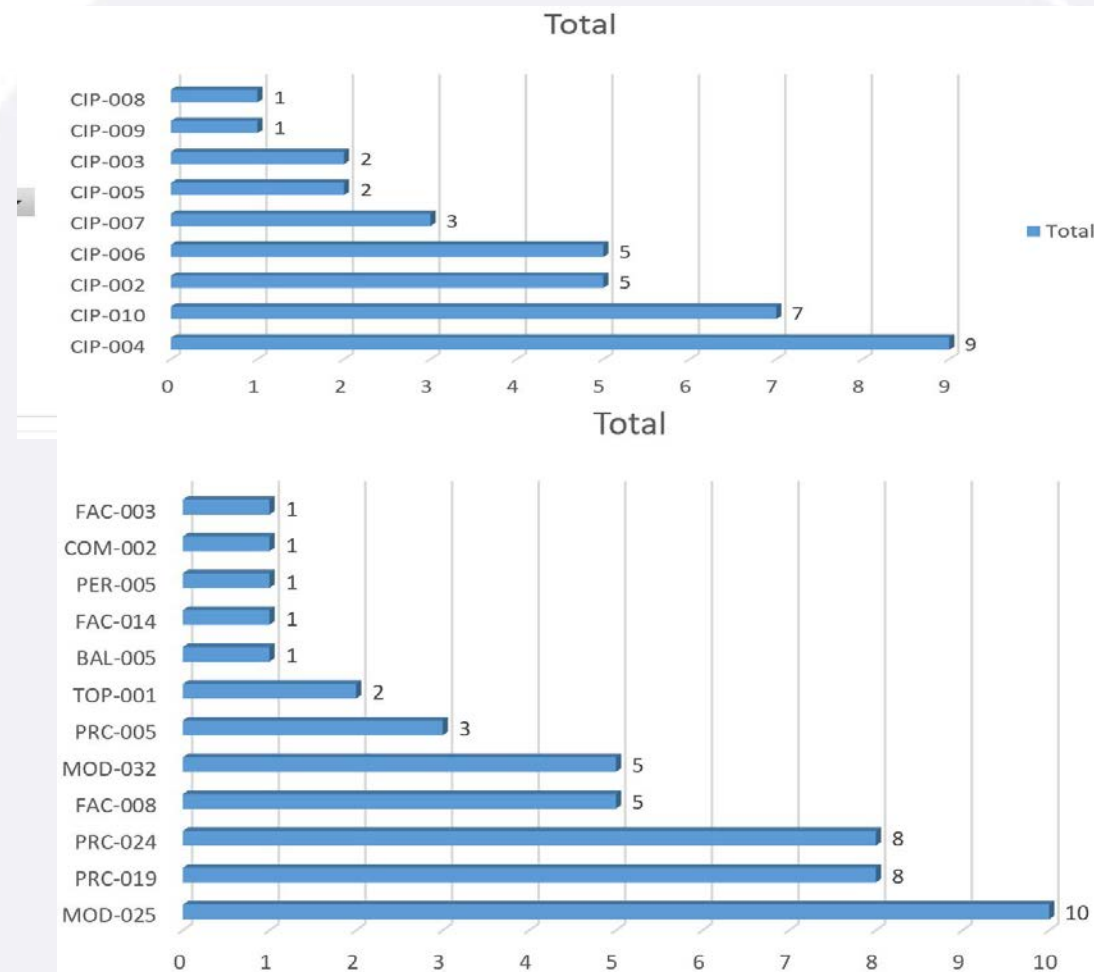
NPCC actions focus on...

- Thorough understanding - 5W1H
- Root Cause
- Wide view in mitigation activities
- Prevent recurrence
- Assess, Educate, Guide, Inform

Trends

- Implementation Plan Related, July 1, 2019:
 - PRC-019, PRC-024, MOD-025
- FAC-008
- PRC-005 is decreasing
- TOP-001-4, R13 – RTA for TOP's
- CIP-002, CIP-004, CIP-006, CIP-010

NPCC Trends for 2019



Objectives

- Understanding NPCC Enforcement Needs
- Understanding how NPCC Enforcement makes a determination
- Address Frequently Asked Questions

Enforcement Duration

- On average, it takes a noncompliance approximately 6-10 months to be completed. (From PNC Submittal to Final Disposition)

WHY DOES IT TAKE THIS LONG?

Enforcement Action Review

- **Violation Description**
 - Discovery Method
 - Standard/Requirement
 - Start/End Dates
 - Root Cause and contributing causes
- **Requirement change**
 - NPCC changes requirement
 - Sends an email Entity
 - Retain the same NERC Violation #
- **Risk Assessment**
- **Mitigation Activities**
- **Compliance History**

CIP & O&P Self Report Guides

- <https://www.npcc.org/Compliance/Default.aspx>



LATEST DOCUMENTS		
TYPE	TITLE	POSTED DATE
	Updated Spring 2019 Prelim Workshop Agenda	5/1/2019
	20190430_NPCC Compliance Registry	4/30/2019
	20190430_NPCC Compliance Registry	4/30/2019
	CDAA CIP Self Report Entry Guidance	4/1/2019
	CDAA O&P Self Report Entry Guidance	4/1/2019

CIP & O&P Self Report Guides

- Copy and paste each answer field into the appropriate self-report section.

Provide Detailed Description and Cause of Possible Violation	How was the Standard and Requirement violated? How did it happen?	Answer 1
	How was the issue discovered? Was the issue discovered by an internal control? If discovered through detective controls, explain how the detective control led to the discovery of the noncompliance. In addition, provide an explanation of the detective control's adequacy or if it needs improvement to help detect similar issues earlier.	Answer 2
	Identify all contributing causes in order to effectively correct the instant issue and prevent recurrence. What was the root cause?	Answer 3
	# of Cyber Assets, PSPs, Individuals, accounts, or BES CSI storage locations in scope	Answer 4
	Unique Identifier for each Cyber Assets, PSPs, Individuals, accounts, or BES CSI storage locations in scope.	Answer 5
	What is the impact level of the BES Cyber System associated with the Cyber Assets, PSPs, Individuals, accounts, or BES CSI	Answer 6

ADD NEW SELF-REPORT: (NEW)

SAVE **CANCEL CHANGES**

Has this Possible Violation previously been reported to other Regions: * ☐ Yes ☐ No

Date Possible Violation was discovered: *

Beginning Date of Possible Violation: *

End or Expected End Date of Possible Violation: *

Is the violation still occurring? * ☐ Yes ☐ No

Provide detailed description and cause of Possible Violation: *

Answer 1

Answer 2

Answer 3

Answer 4

Answer 5

Answer 6

CIP-010 R1 Description Example

CIP Description of Noncompliance

- ABC company found that it failed to classify BES Cyber Assets, Protected Cyber Assets and Electronic Access Control or Monitoring Systems. The documentation issue was the result of human error.

Questions?

- How was the issue discovered?
- How many Cyber Assets were not identified?
- What is the function of the Cyber Assets in scope?
- What caused the documentation issue?

CIP-010 R1 Description Example

CIP Better Description of noncompliance

- On Jan 1, 2019 ABC company found that it failed to classify 10 BES Cyber Assets, 5 Protected Cyber Assets and 2 Electronic Access Control or Monitoring Systems, after performing its annual site walkthrough. The Cyber Assets were part of a new SCADA system that was on boarded on Dec 1, 2018 and the Compliance Manager was not aware of the project.

Key Details

- Includes how issue was discovered
- Includes the scope of the issue
- Includes start date of the issue
- Includes root cause details
- Includes function of the BES Cyber Assets

Cause Analysis

Root Cause Methods

- Events and Causal Factor Analysis
- Change Analysis
- Barrier Analysis
- Management Oversight and Risk Tree (MORT) Analysis
- Human Performance Evaluation
- Kepner-Tregoe Problem Solving and Decision Making
- https://www.nerc.com/pa/rrm/ea/CA_Reference_Materials_DL/DOEGuidelinesforRootCause.pdf

Human Performance tools

- S-A-F-E-R
 - Summarize
 - Anticipate
 - Foresee
 - Evaluate
 - Review
- https://www.nerc.com/pa/rrm/ea/CA_Reference_Materials_DL/DOE%20-%20Vol%202%20Tools%20for%20Individuals%20Work%20Teams%20and%20Management.pdf

Risk Evaluation

Potential impact to the BPS

- System condition
- Size, nature, criticality, and location of facilities
- Scope and function of assets
- What systems, facilities, or staff were exposed?
- Misoperations, exceedances of system operating limits?
- Potential loss of a Protection System devices, degradation or loss of a BES element, or BES Cyber System or information?
- Potential affect to CIP-005 and CIP-007 controls

Factors reducing the Risk

- Likelihood
 - Internal controls
 - Size of facilities
 - Early detection
 - Duration
 - Redundancies
- <https://www.nerc.com/pa/comp/CE/Enforcement%20Actions%20DL/Registered%20Entity%20Self-Report%20and%20Mitigation%20Plan.pdf>

CIP-010 R1 Risk Example

CIP Impact Statement

- The issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Cyber Assets were afforded protections.

Questions?

- What are the potential consequences to the BES?
- What kind of protections were afforded?
 - Preventative Controls
 - Detective Controls
 - Corrective Controls

CIP-010 R1 Risk Example

CIP Better Impact Statement

- ABC company reduced the risk of Cyber Assets being rendered unavailable degraded or misused by restricting logical and physical access to individuals based on need. The systems are physical protected from unauthorized access via fenced enclosure, buildings with locked doors allowing only badged entry, and PSP's requiring badge and fingerprint to enter. The cyber systems are also equipped with file integrity monitoring software that would alert personnel to unauthorized changes.
- ABC company further included the cyber assets in its patch management program, monitors the systems with antivirus protection, and monitors the network in scope with its IDS system.
- ABC company personnel have been trained on incident handling and if a cyber security incident had occurred personnel would follow ABC companies CIP-008 process.

Key Details

- Identifies preventative, detective, and corrective controls
 - Restricted logical and physical access
 - Calls out layered physical protections
 - Identifies protections that were afforded:
 - Patching
 - Antivirus
 - File integrity monitoring
 - Identifies that personnel are trained to identify and correct issues

Mitigation

- Actions and Milestones
 - Steps to end noncompliance
 - Controls that reduce risk until the noncompliance can be mitigated
 - Steps to address the root cause
 - Controls to prevent recurrence
- Mitigation Completion
 - Submit evidence upon Mitigation Completion (includes Compliance Exceptions)

Evidence Retention (Data Hold)

- Notice of Preliminary Screen
 - This letter serves as official notice to preserve all documentation pertaining to the potential noncompliance.
 - Provides an NPCC Enforcement Contact

Evidence Retention Continued

- Notice of Compliance Exceptions
 - The data retention directive provided in the Notice of Preliminary Screen shall continue and the registered entity shall maintain evidence, including mitigation evidence, related to these Compliance Exception(s) for no less than **18 months** from **the later of**: (1) the date of this Notice of Compliance Exception; or (2) the date the registered entity completes the mitigation activities.
 - NPCC may verify completion of mitigation through an audit, spot check, random sampling, or other means.

Enforcement Outcomes

- **Dismissal**
- **Compliance Exception**
 - Minimal Risk, \$0, minimal paperwork
 - Not considered a “possible violation”; instead “potential non-compliance”
 - Do not verify mitigation
- **FFT**
 - Moderate risk, \$0 penalty still
 - Still efficient and focuses resources, a bit more paperwork
 - Not considered a “confirmed violation”; but still a “possible violation” is sent
 - Verify mitigation
- **SNOP / Full NOP**
 - \$ Involved
 - Short Settlement Form

Penalties

Appendix A: Base Penalty Amount Table

The following lists the Base Penalty amounts corresponding to combinations of Violation Risk Factor and Violation Severity Level.

	Violation Severity Level							
Violation Risk Factor	Lower		Moderate		High		Severe	
	Range Limits		Range Limits		Range Limits		Range Limits	
	Low	High	Low	High	Low	High	Low	High
Lower	\$1,000	\$3,000	\$2,000	\$7,500	\$3,000	\$15,000	\$5,000	\$25,000
Medium	\$2,000	\$30,000	\$4,000	\$100,000	\$6,000	\$200,000	\$10,000	\$335,000
High	\$4,000	\$125,000	\$8,000	\$300,000	\$12,000	\$625,000	\$20,000	\$1,000,000

NOTE: This table describes the amount of Penalty that could be applied for each day that a violation continues, subject to the considerations of Section 2.16 regarding frequency and duration of violations.

Factors associated with Penalties

- Risk to bulk power system (Primary Factor)
- Specific Facts and Circumstances of Violation (Primary Factor)
- Violation Risk Factor/Violation Severity Level
- Violation Time Horizon
- Violation Duration
- Discovery Method and How Discovered
- Settlement
- Compliance History / Repeat Violations

Factors associated with Penalties

- Aggravating
 - Intentional / concealment / impeding investigation
 - Management involvement/knowledge of bad behavior
- Mitigating
 - Admission
 - Internal Compliance Program
- Both
 - Cooperation
 - Extenuating Circumstances

Cooperation

- Cooperation is expected; prior to and during settlement
 - Timely and accurately responding to questions and inquiries
 - General politeness/respect
 - Keeping NPCC updated if answers will not be by expected date
 - Appropriate staff resources and availability
 - Immediate and effective steps to address noncompliance
-
- Candor/Disclosure
 - All facts; not just favorable facts
 - Providing NPCC with information unhelpful to your entity without a specific question asking for that information
 - Events Analysis participation (if appropriate)

Positive aspects of ICP

- Detects and Prevents Violations
- Organizational Culture – scaled to the size of company
- High level knowledge of content/operation of ICP (i.e. BOD and/or Executive/Senior Management)
- Training and dissemination of information
- Periodic evaluation of ICP
- Dedicated compliance staff

Mitigation vs. Above and Beyond

- Mitigation is required and includes:
 - Fixing the issue and
 - Taking actions to reduce the possibility violation reoccurs
- Above and Beyond Credits
 - Difficult to get
 - Cannot be something that was already planned and/or budgeted prior to identification of violation
 - Cannot be something that similarly situated entities have already done or are doing
 - Really needs to take it to next level

FAQ

- Self-Logging?
- CDAA Process Flow
- Transferring files (NPCC Drive)
 - Passwords
- How can I be compliant with...<Insert any standard/req>?
- How is the ERO addressing Cloud storage?

Self Logging

- Advantages of participation
 - Entities identify and document minimal risk issues
 - Entities provide update to Region quarterly
 - Identified issues will be (presumably) treated as Compliance Exceptions
 - *The burden is on Entity to provide a high quality report (See Self-Report Guidance)*
- Participation
 - Open to all entities
 - Send inquiry to: selflogging@npcc.org

CDAA Process Flow



- Screening in Progress – The possible noncompliance (PNC) has been received by the region. The region has 5 days to perform a preliminary screen which reviews 3 items.
- Review in Progress – The PNC has passed preliminary screen. A Subject Matter Expert is reviewing.
- Determination in Progress – An Enforcement member is reviewing the results of the SME review and determining the disposition of the PNC.
- Determination Completed – An enforcement member has completed the review. A disposition method will be sent to the PCO and PCC shortly.
- Sent to NERC – The disposition has been sent to NERC. The registered entity must first be notified prior to this disposition being sent to NERC.
- Filed with FERC – NERC has submitted the disposition to FERC.
- Pending Regional Closure - Region must confirm 3 items. Completion of mitigation, the release of data hold, and no FERC/NERC outstanding questions
- Closed

Transferring files (NPCC Drive)

- Directions included in every Preliminary Screen Notification
- An Enforcement Engineer/Analyst will provide How-to guide on request
 - Place your entire submittal into a Zip file.
 - Give the Zip file a unique and relevant name, e.g., *ABCCompany_PRC_005.zip*
 - *How-to guide will have link to access and password*

How can I be compliant with...<Insert any standard/req>?

- Review Effective Standards
 - <https://www.nerc.net/standardsreports/standardssummary.aspx>
- Review NERC Glossary of Terms
 - https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf
- Use Forums
 - North American Transmission Forum (NATF)
 - North American Generation Forum (NAGF)
 - Task force on Infrastructure security and Technologies (TFIST)

How is the ERO addressing Cloud Storage?

- 3/1/2019 – Tri-State Generation and Transmission Association submitted Standard Authorization Request (SAR) to clarify the CIP requirements related to BES CSI access to allow for alternative methods, such as encryption, to be utilized in the protection of BES CSI. (https://www.nerc.com/pa/Stand/Project201902BCSIAccessManagement/SAR_BES%20Cyber%20System%20IAM.pdf)
- 3/28/2019 through 4/26/2019 is a comment period.
- The SAR drafting team will review all responses received during the comment period to determine the next steps.
- Compliance Guidance for CIP-011-2 R1 to be developed
- Next Steps (~ 1 year):
 - Standard Revision Draft
 - Industry Approval
 - BOT Adoption

Questions?

