Controls and RISC

NPCC Entity Risk Assessment (ERA) Group

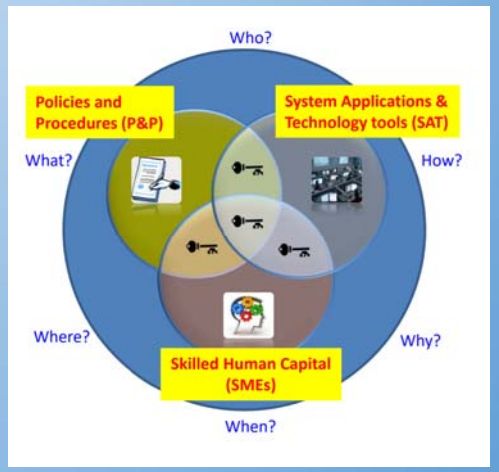
NPCC 2019 Spring Compliance Workshop
Mystic CT
May 22, 2019

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

NPCC, Inc.

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:

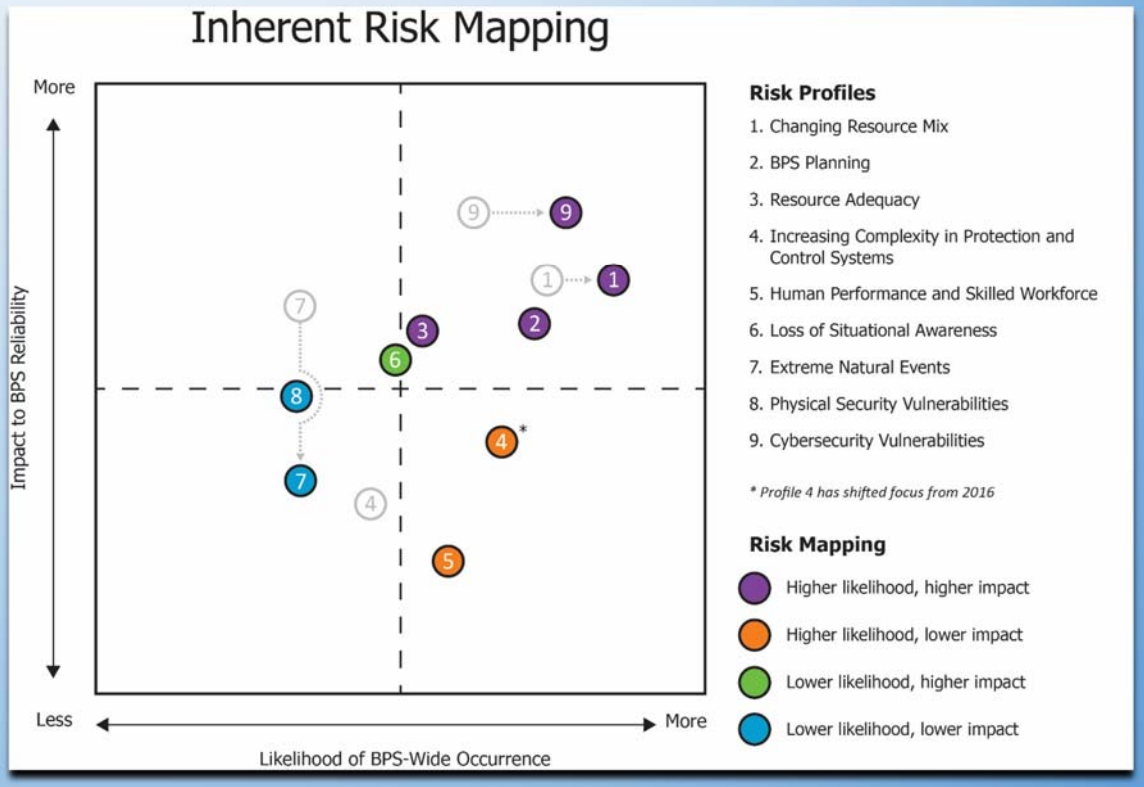
1. The fast pace of change of the resource mix;
2. Interdependence between the energy and communication sectors;
3. Increased complexity of the power system's automated control systems due to the increased use of power electronics and digital controls, and the risks of negative interaction between those 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"

NPCC, Inc.

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

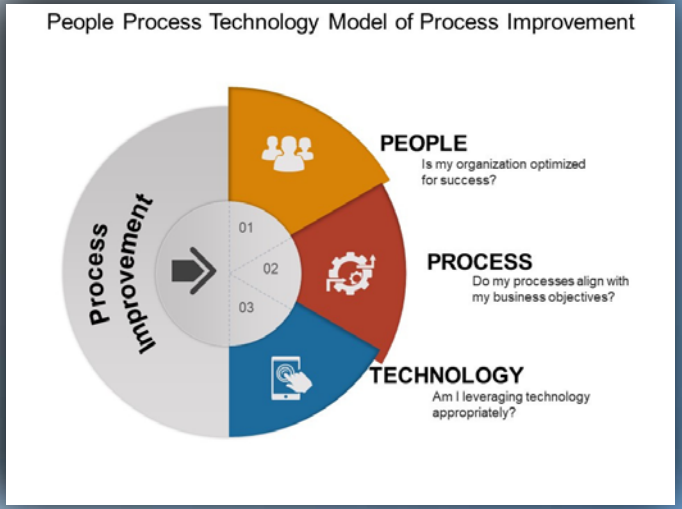
2018 RISC Report – Controls

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.

NPCC, Inc.

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

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

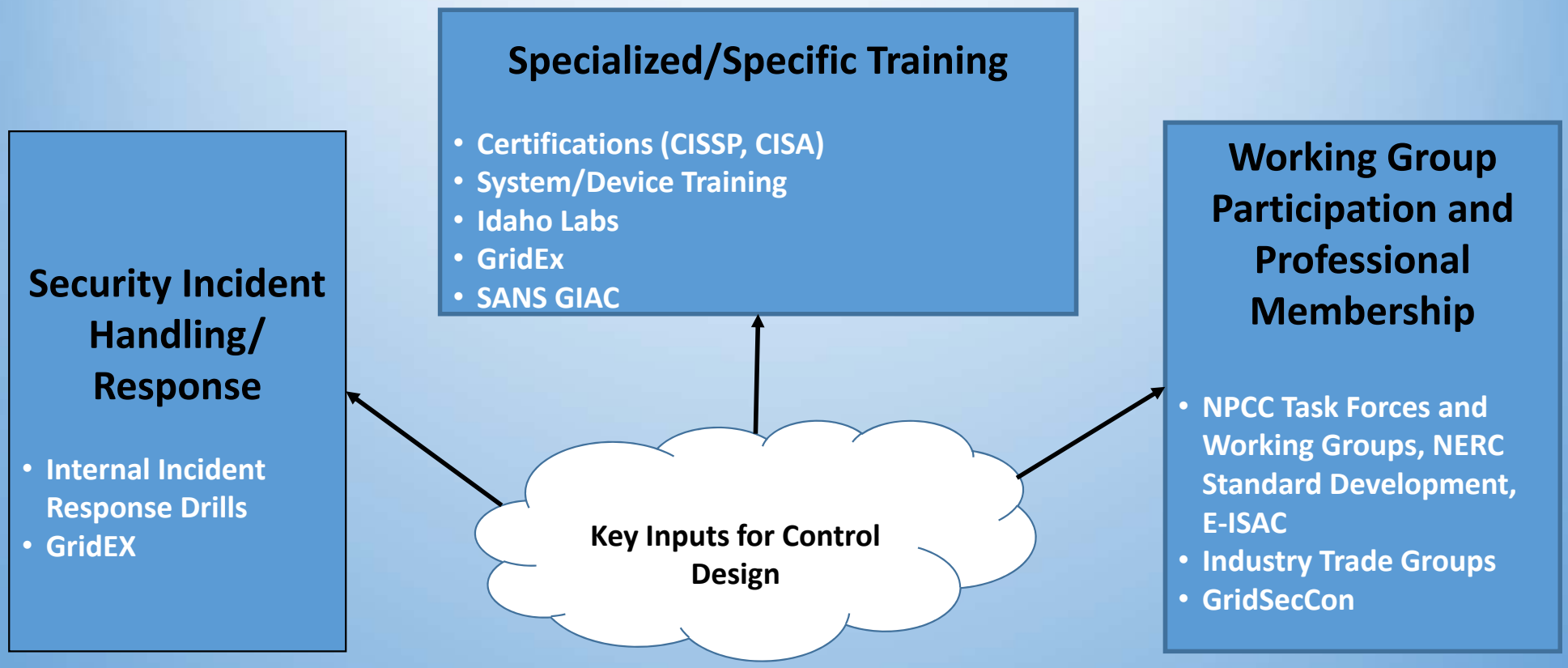
Hiring Requirements

- 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?

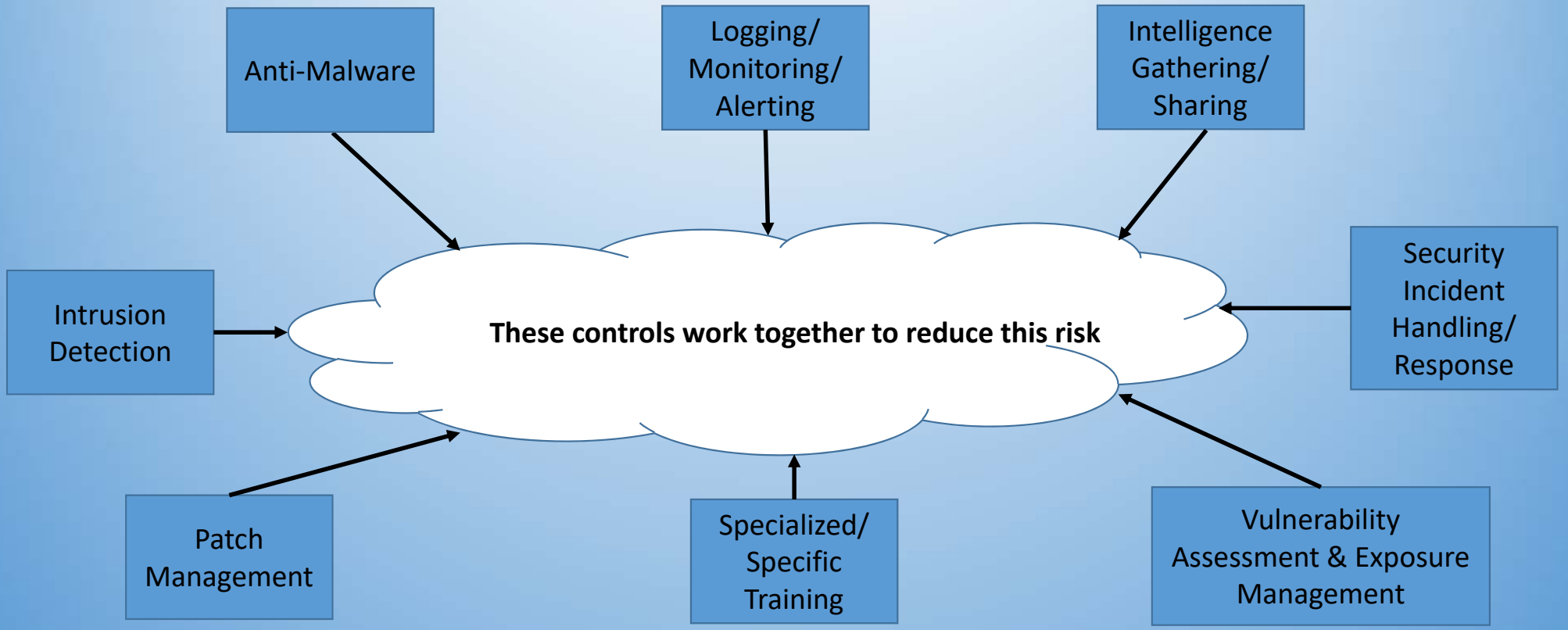
2018 RISC Report – Human Capital Knowledge and Experience



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.**

NPCC, Inc.

Key Controls/Control Areas for this Risk:



2018 RISC Report – People, Process, Technology

NPCC, Inc.

Intrusion Detection

People –Security Architecture, Security Operations Team, Audit/Compliance
Process – Monitoring, Update, Detection, Response
Technology – NIDS, HIDS, Network/Host/Application Firewalls, Exercises

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

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

Intelligence Gathering/Sharing

People –Security Architecture, Security Operations Team, Audit/Compliance, Vendors
Process – Intelligence Gathering/Evaluation/Sharing
Technology – Intelligence Sharing Platforms/Services

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

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

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

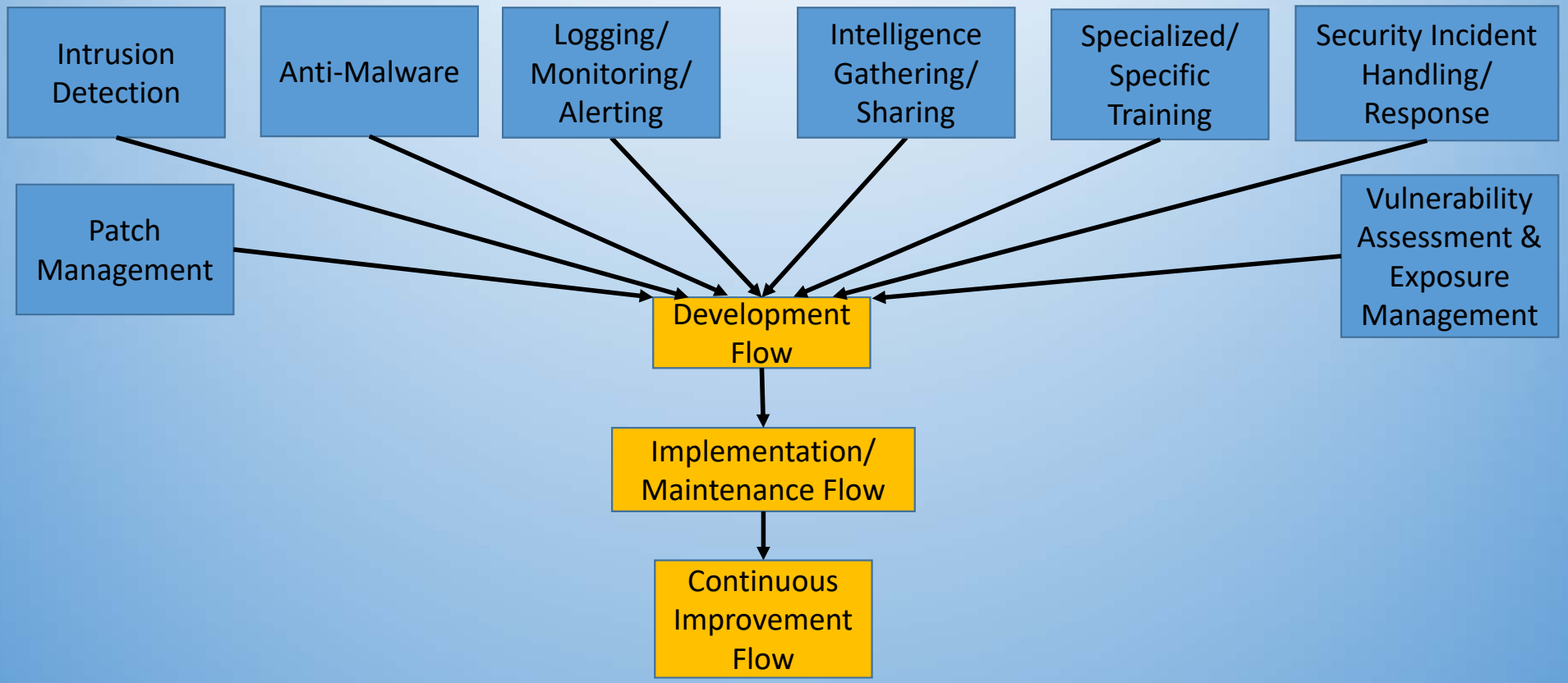
Vulnerability Assessment & Exposure Management

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

2018 RISC Report – Cyber Risk #7

NPCC, Inc.

Control Flow Development, Implementation/Maintenance, Continuous Improvement:



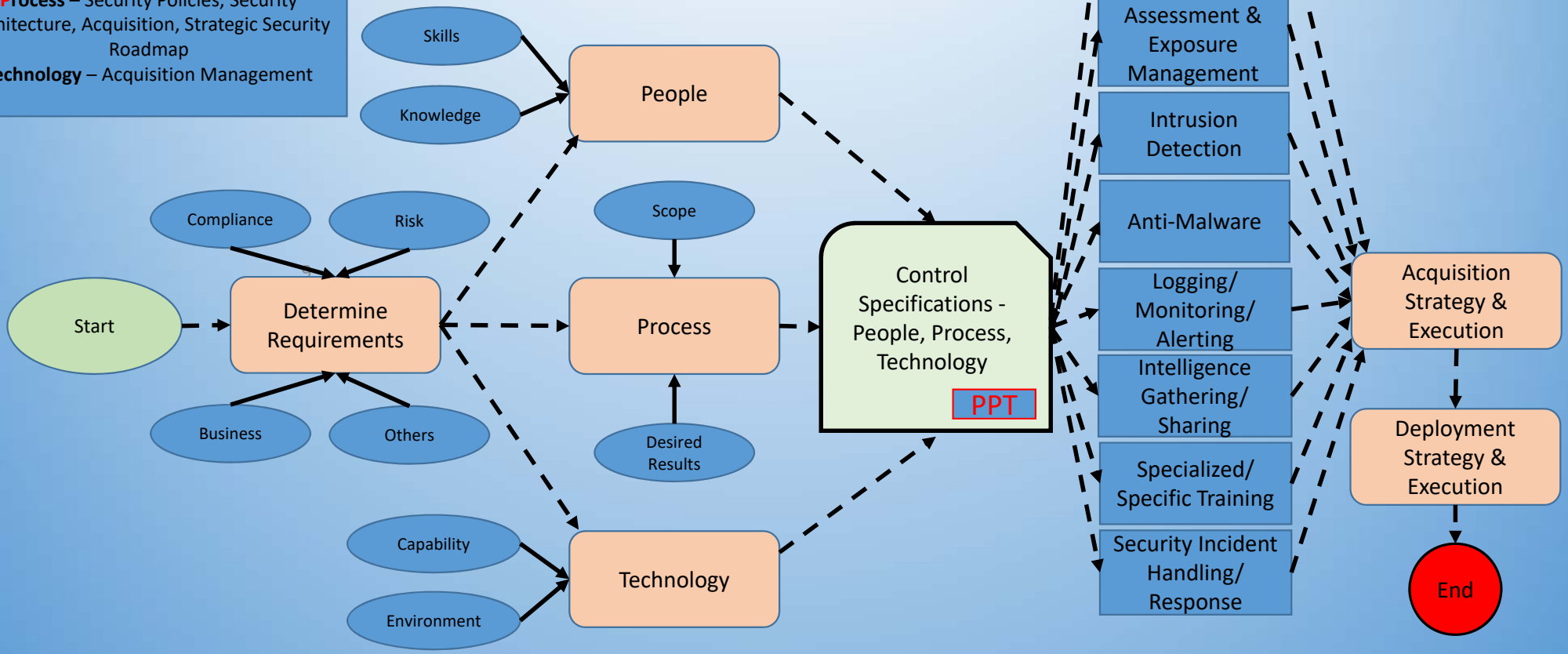
2018 RISC Report – Control Flow: Development

Control Development

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

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

Technology – Acquisition Management

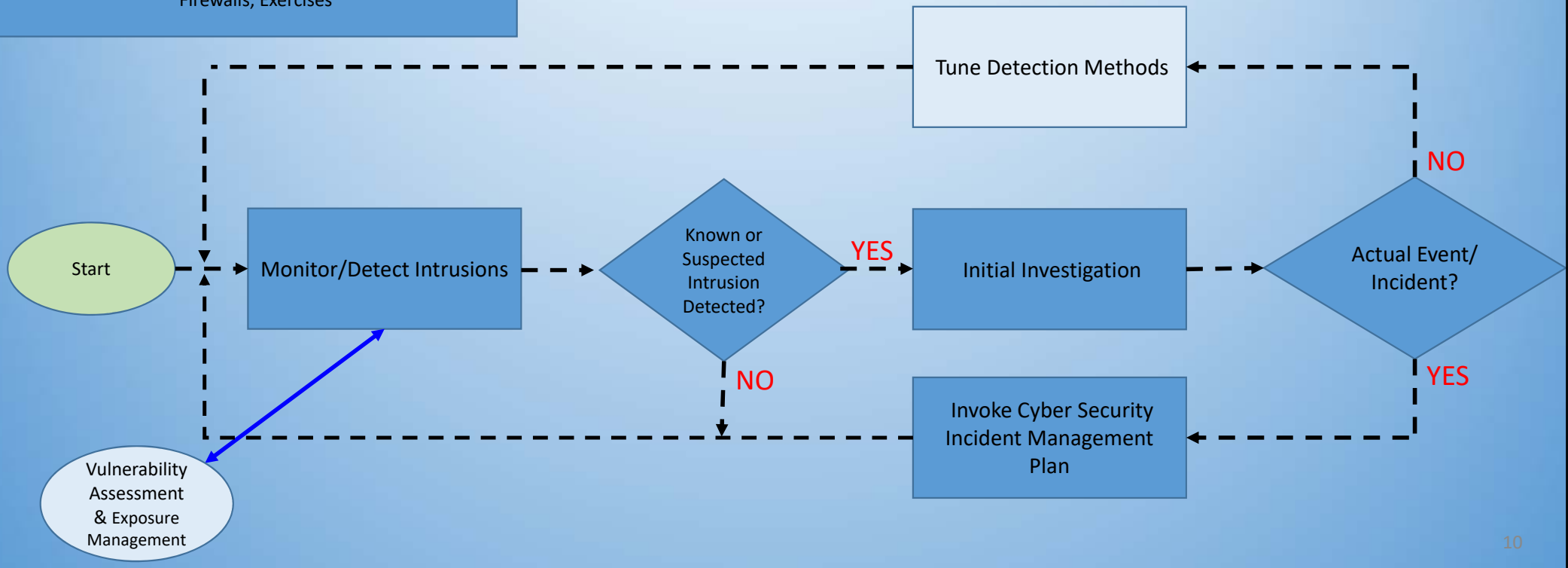


2018 RISC Report Risk #7 – Control Flow: Implementation/Maintenance

NPCC, Inc.

Intrusion Detection

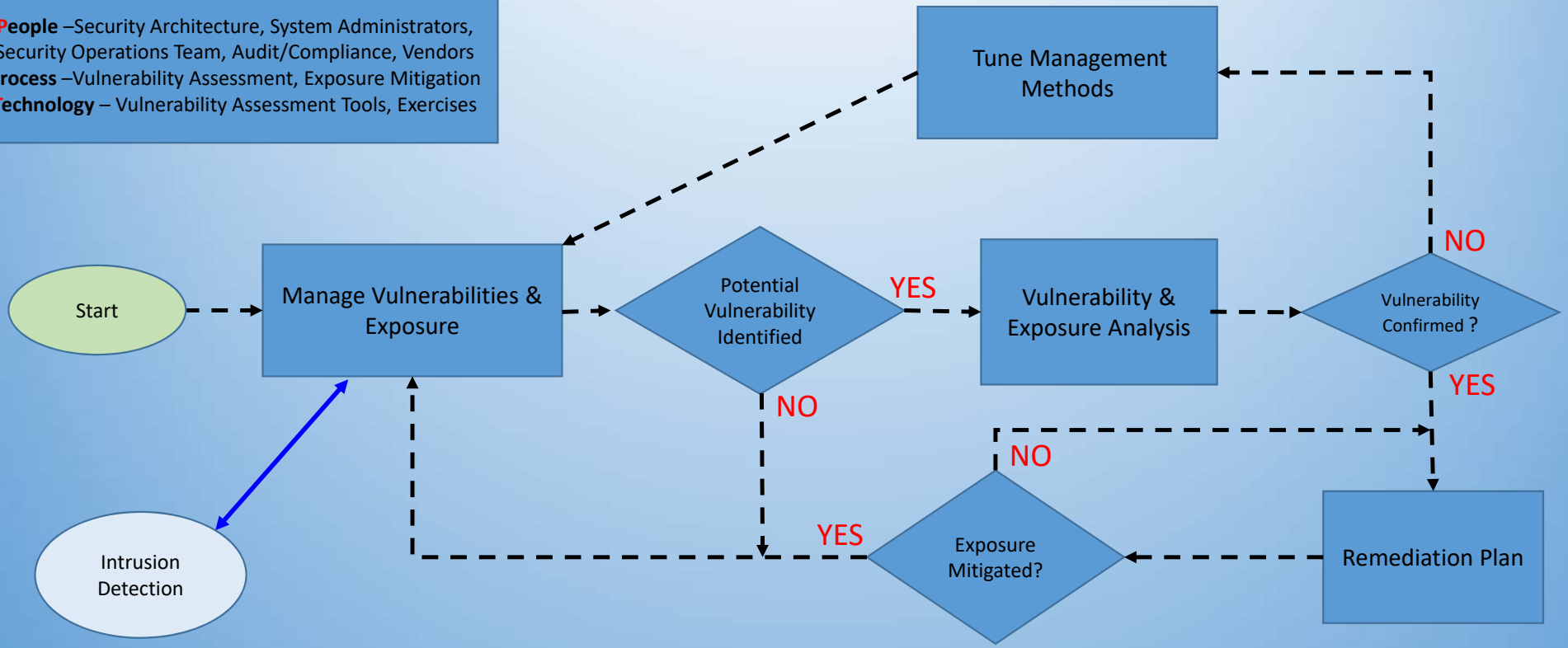
People –Security Architecture, Security Operations Team, Audit/Compliance
Process – Monitoring, Update, Detection, Response
Technology – NIDS, HIDS, Network/Host/Application Firewalls, Exercises



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



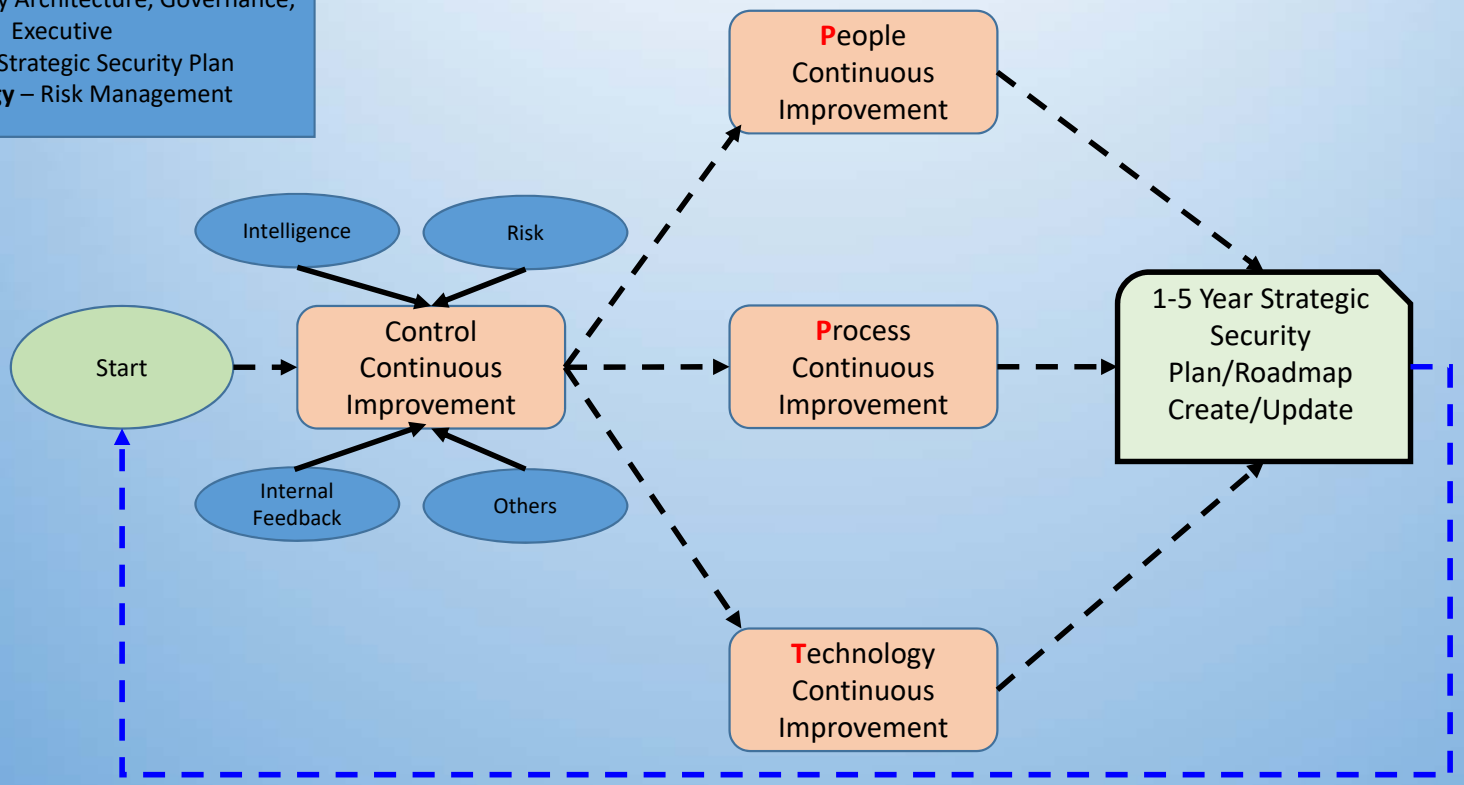
2018 RISC Report – Control Flow: Continuous Improvement

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