

# Internal Controls – Evaluation, Testing and Issues/Trends

---

## NPCC Entity Risk Assessment (ERA) Group

NPCC 2019 Fall Compliance Workshop  
November 20-22, 2019  
Newport, RI



# Risks

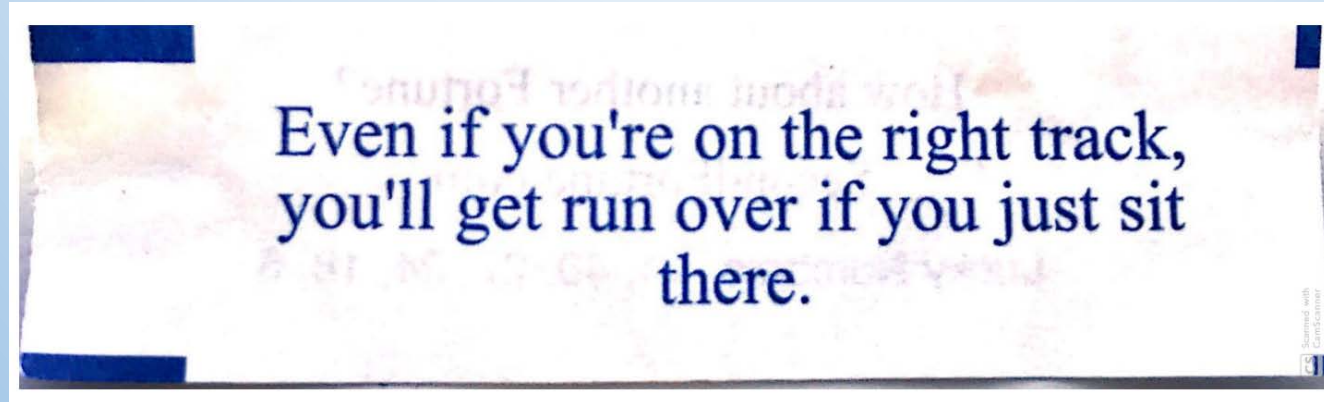
The terms “Risk”, “Risk Mitigation”, “Risk Tolerance”, “Inherent Risk”, “Residual Risk” have been appearing in our vocabulary more frequently:

- Financial Risks
- Occupational Risks
- Safety
- Health/Medical
- Reputation
- Travel/Commuting
- Legal (Liability)
- Business Continuity/Operations

# “Where there’s Risks, there should be Controls”

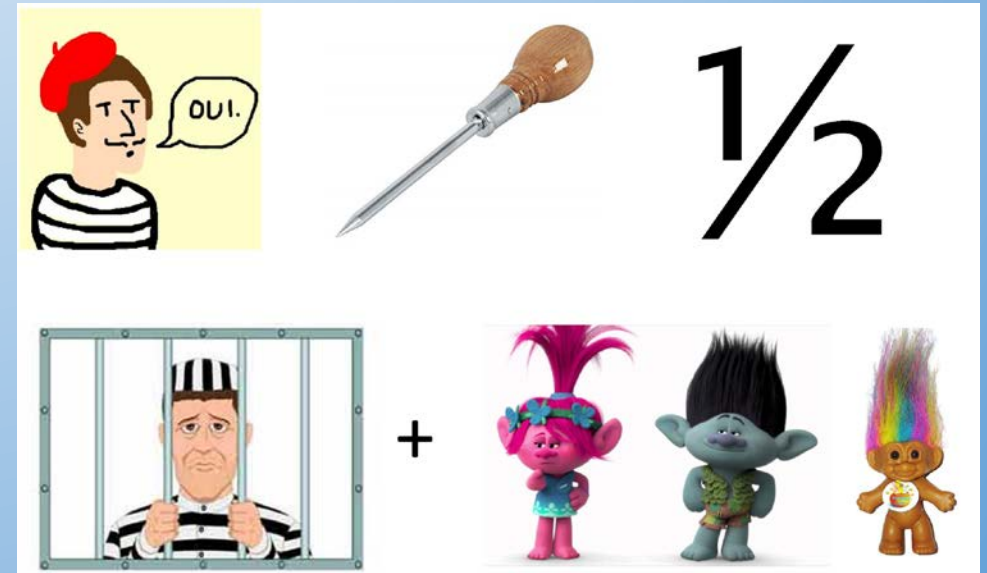
- Controls are used to mitigate the consequences of Risks
- Fully implemented controls (tested and monitored) help ensure consistent, rigorous achievement of goals in a timely manner.
- Controls are:
  - Procedures, Policies, Guides, Practices, Instructions, Studies
  - Spreadsheets, Databases, Lists, Passwords, Patches, Barriers, Work Management, Reminders
  - Staff, contractors; trained to do their jobs; certified if necessary; job description/prerequisites

# Food for Thought



# Recent Trends/Issues

- Audit Findings vs. Controls
  - Audits are focused on meeting the wording of the Requirement.
  - Lack of (or poor controls) may be noted by the Audit Team as an Area of Concern and/or Recommendations to develop/improve controls. Controls are “forward looking”.
- The ERO is expected to assess the controls that support compliance to the NERC Reliability Standards



# Recent Trends/Issues

- Many Registered Entities don't fully understand what constitutes controls (and testing of same) versus Audit evidence.
- Regional Entities are not consistent in their approach, timing, data requests for controls documentation, and deliverables.
  - NPCC provided the North American Generators Forum (NAGF) with a presentation (tutorial, clarification, personal example, specific examples for Generator Owners and Operators) at their annual 2019 meeting.

[https://www.npcc.org/Compliance/Entity%20Risk%20Assessment/ppt\\_NAGF\\_InternalControls\\_NPCC\\_BEng\\_101619a.pdf](https://www.npcc.org/Compliance/Entity%20Risk%20Assessment/ppt_NAGF_InternalControls_NPCC_BEng_101619a.pdf)

# Evaluation of Internal Controls

The *evaluation of internal controls (eic)* occurs whether or not the entity provides controls information in advance of the audit.

- If controls information is provided well in advance of the audit, NPCC will do testing and assessment of the controls and
  - Provide a table of suggestions to enhance the controls and
  - If warranted, recommend
    - Possibly reducing sampling of audit evidence or
    - Possibly deferring the audit of the requirement to Spot Check or Self-Certification at a later date
- All evaluation and testing information, including justification for deferrals/sampling reductions are documented in NPCC Workpapers.

# Evaluation of Internal Controls

The *evaluation of internal controls (eic)* occurs whether or not the entity provides controls information in advance of the audit.

- If controls information are not provided in advance of the audit, then (during the audit) NPCC will:
  - review audit submittals, ask control questions, review testing of entity controls and
  - provide suggestions to enhance the controls
  - During the Audit Team Lead's Initial Audit Briefing call, the eic auditor may introduce him/herself and provide a high level overview of what the eic process entails and types of information requested.

# Recent Trends/Issues

- Registered Entities don't realize that NPCC is testing their controls during the *evaluation of internal controls* process (whether prior to, or during the audit)

Hey, did NPCC test your controls?

Hmm...I'm not sure.



# Does NPCC Test Entity Controls?

YES. Absolutely!!!

## *Assessment Criteria*

The CEA may use a binary effective/not effective method for assessing implementation effectiveness, or it may use a measured approach to assess internal control implementation. CEAs should have a documented methodology for assessing implementation, and this methodology may include, but is not limited to, the following:

- The automation of internal controls
- Compensating and supporting internal controls
- Registered entity identification of key controls
- The level of available internal control documentation
- Peer review of key controls within the registered entity
- Feedback on control design processes
- Registered entity's internal review and testing of existing internal controls

# Controls Questions and Testing

During the eic, NPCC may ask Controls related questions:

- What procedure(s) are used to support compliance?
  - Are the procedures current? How do you know the steps in the procedure have been performed in a timely manner?
  - What (“testing”) evidence can you provide to confirm the above? Looking for Emails, work management task status/closeout, meeting minutes, checklist, lessons learned, logs, attendance, system out-put, screenshots, real time witness testing.
- What tools are used to support compliance?
  - How do you know the tools are working properly?
  - Do you have evidence that the tool has been used when required?
  - What “testing” evidence can you provide?
- Who is applying the tools and procedures listed above?
  - Are the people using the tools and applying the procedure qualified, trained, authorized?
  - What (“testing”) evidence can you provide (qualifications, training records, job description)

# Controls Questions and Testing



- Answers to NPCC's Control related questions and evidence of testing are documented in NPCC eic Workpapers
- Suggestions to enhance controls will be provided in the entity's Compliance Oversight Plan (COP) and Audit Report

# Controls for Cyber Security Risks

NPCC Entity Risk Assessment (ERA) Group



NPCC 2019 Fall Compliance Workshop  
November 20-21, 2019  
Newport, RI

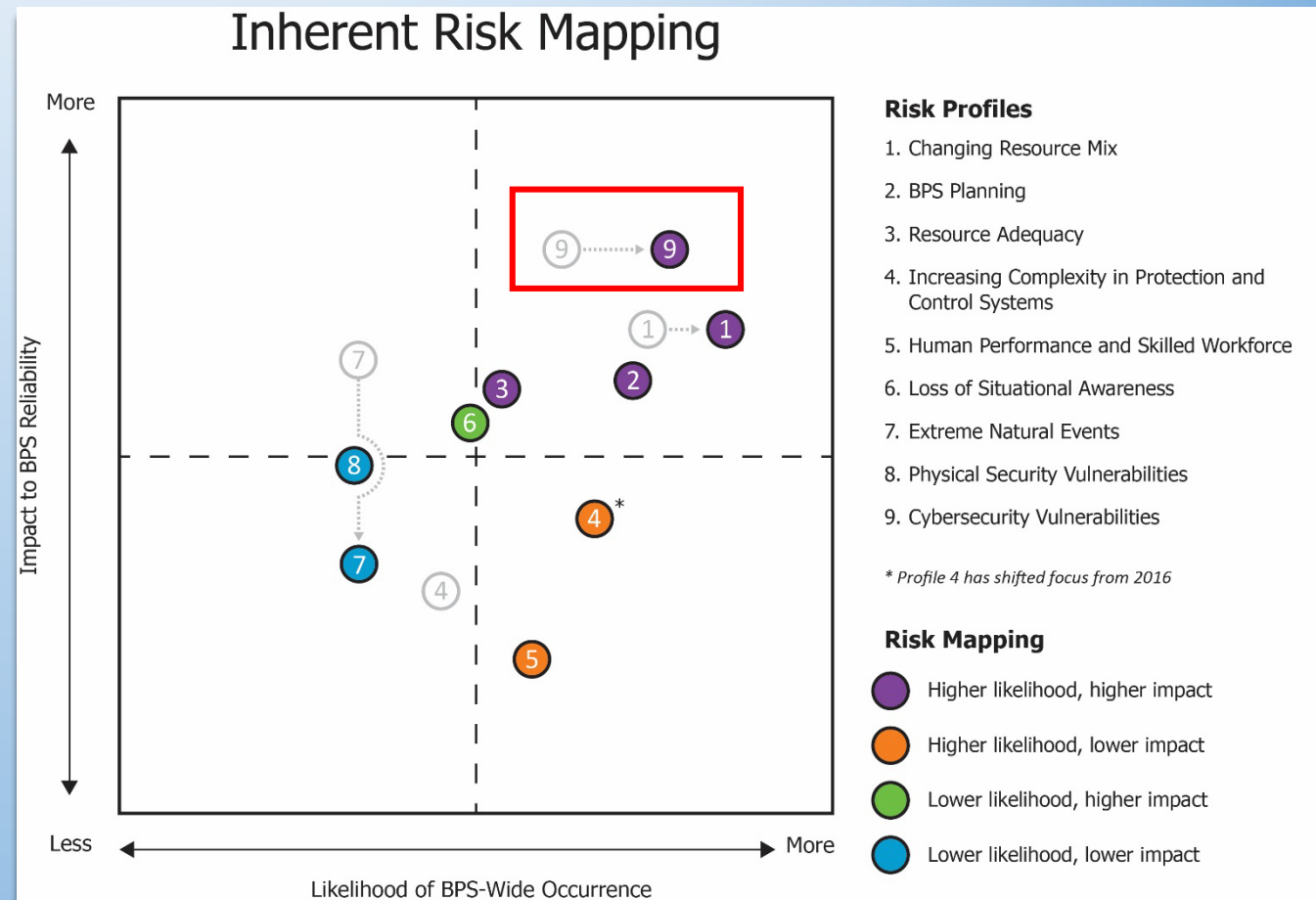
# ERO Reliability Risk Priorities, February 2018

## 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)



# Identified Risks – Presentation Focus

- ERO Reliability Risk Priorities, February 2018
  - **Report Risk Profile #9: Cybersecurity Vulnerabilities (CV)**
    - **CV Risk #1** - Cybersecurity threats result from exploitation of both external and internal vulnerabilities:
      - a) Exploitation of employee and insider access.
      - b) Weak security practices of host utilities, third-party service providers and vendors, and other organizations.
      - c) Unknown, undisclosed, or unaddressed vulnerabilities and exposures in cyber systems.
      - d) Growing sophistication of bad actors, nation states, malicious actors and collaboration between these groups.
    - **CV Risk #4** -Technologies and Services
      - a) Increased reliance on third party service providers and cloud-based services for BPS operations and support.
      - b) Cybersecurity risks in the supply chain: software integrity and authenticity; vendor remote access; information system planning; and vendor risk management and procurement controls.

Source: <https://www.nerc.com/comm/risc/related%20files%20dl/ero-reliability- risk priorities-report board accepted february 2018.pdf>

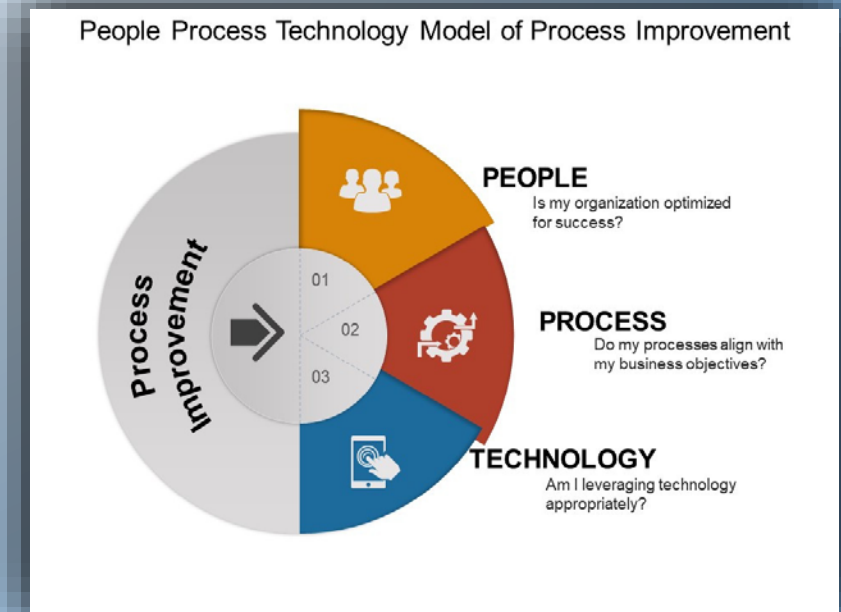
# 2018 RISC Report – Controls

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.

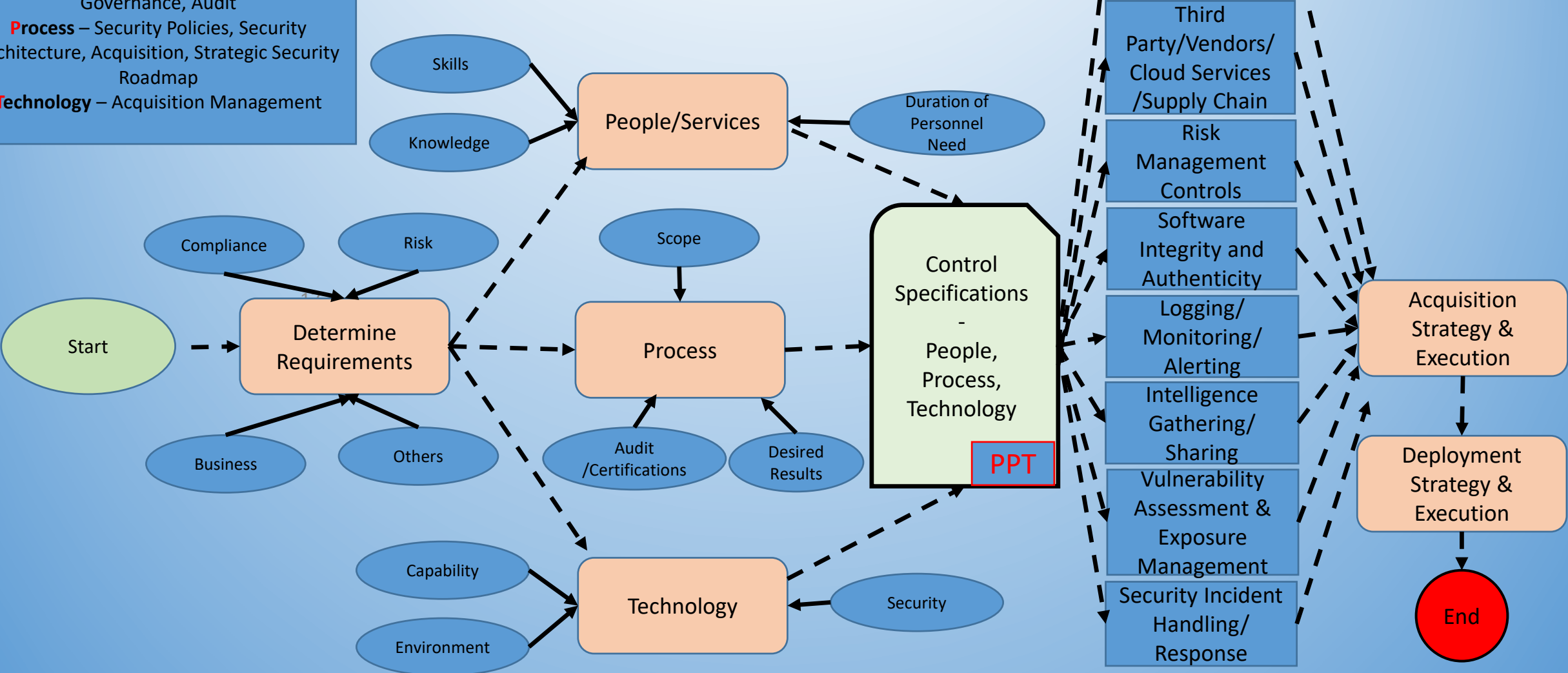
# 2018 RISC Report – Control Flow: Development (Overview)



## 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 – Cyber Risk #1

Cybersecurity threats result from exploitation of both external and internal vulnerabilities:

### Exploitation of Employee and Insider Access

- Know who is accessing your systems.
- Systems should be restricted to only personnel who need access.
- Identify user ability to cause harm and Potential to cause harm.
- **Third Parties, Manage Services and Contractors.**

### Weak Security Practices

#### Source of Security Practices:

- Internal Entity Security Practices
- Third-Party Providers/Suppliers
- Other Organization ( e.g. Government, RCs,).

#### Practices:

- E.g.: Vulnerability / Patch Management, Policy /Procedures, Deployed Encryption, Information security, Remote Access, Exposure Management, Procurement.

### Key Inputs for Control Design:

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

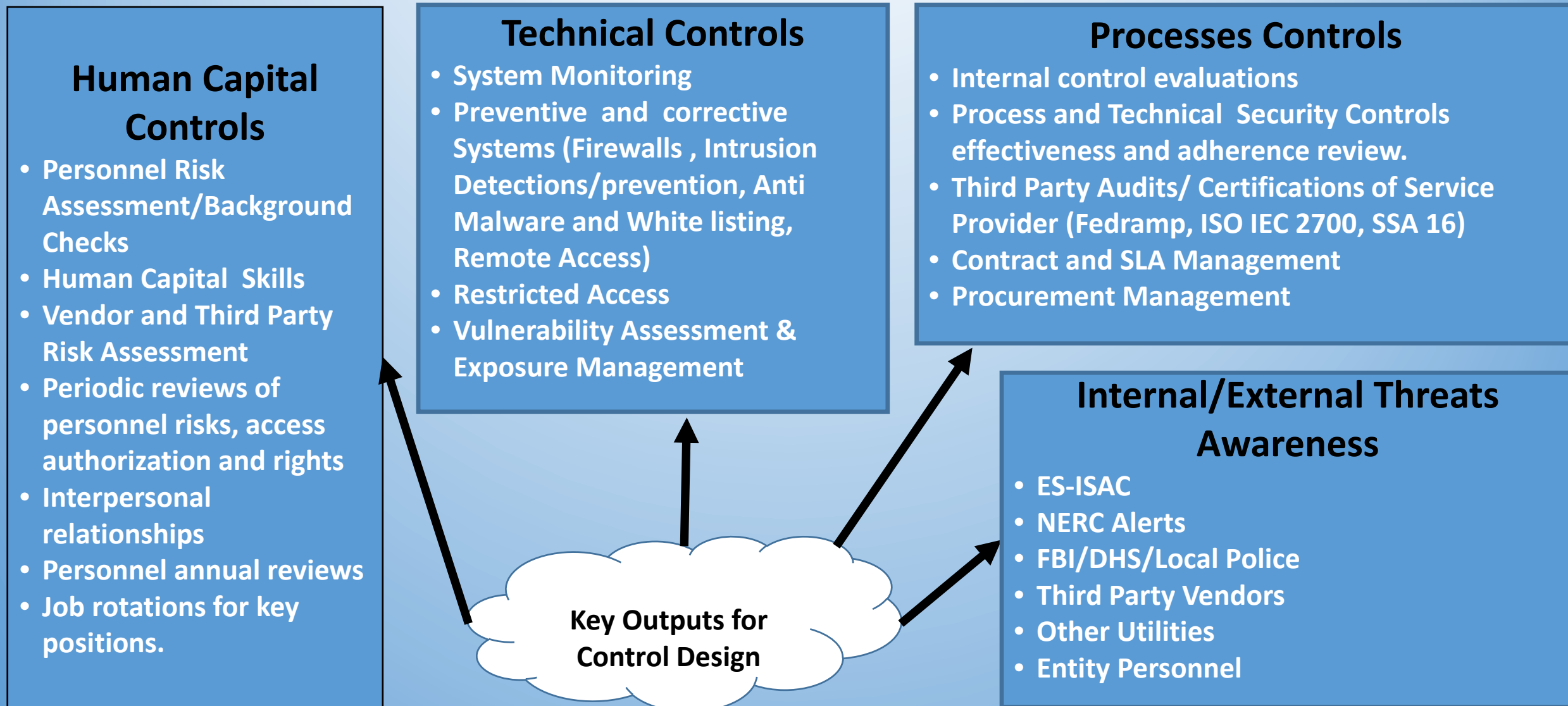
### Growing Sophistication of External Threats

- Bad/Malicious Actors (disruptive, Hacktivist or financial gain attacks).
- Nation States.
- Threat vectors cyber/physical/ combination.
- Intelligence Gathering Sources.
- Widely Available Tools.

### Unknown, Undisclosed, or Unaddressed Vulnerabilities and Exposures

- Vulnerability and Exposure Management.
- Entity Risks.
- Defense in Depth.
- Intelligence Gathering.

# 2018 RISC Report – Risk #1: External and Internal Vulnerabilities Controls



# 2018 RISC Report Risk #1 – Control Flow: Implementation/Maintenance

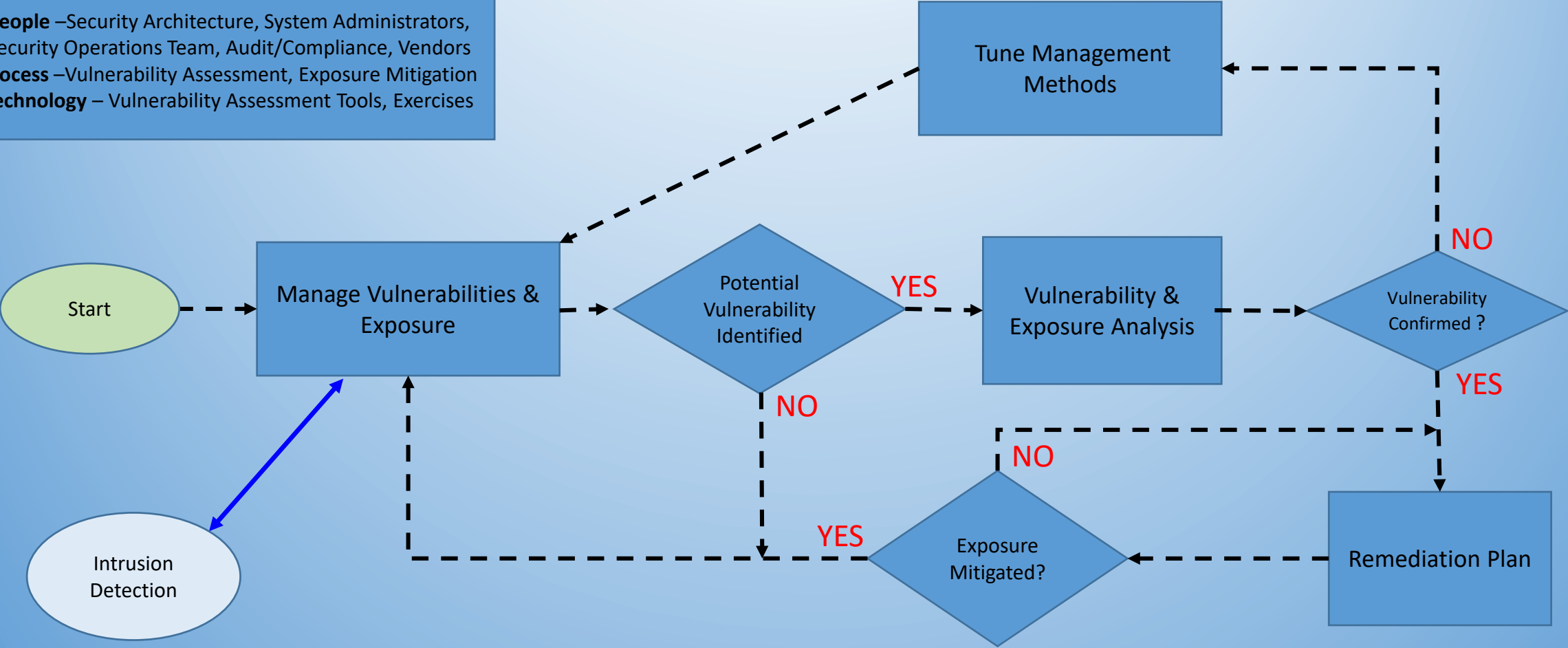


**Vulnerability Assessment & Exposure Management**

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

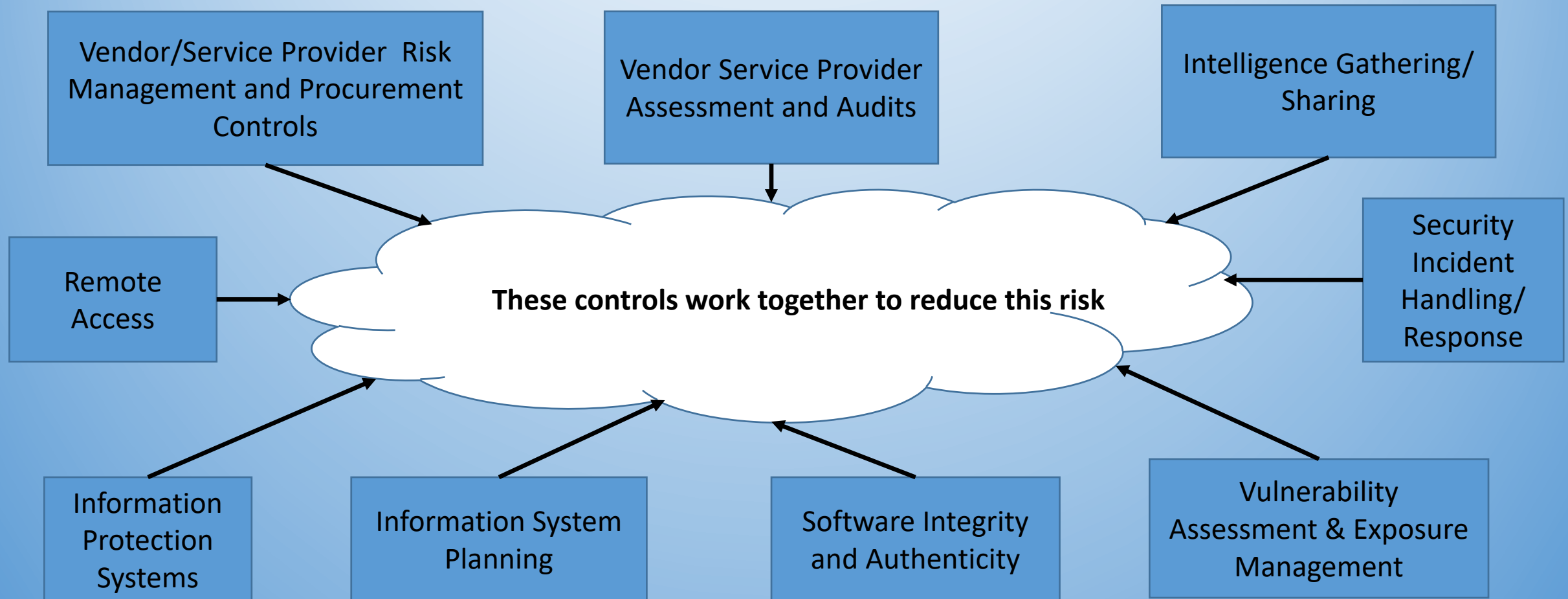
**Process** –Vulnerability Assessment, Exposure Mitigation

**Technology** – Vulnerability Assessment Tools, Exercises



# 2018 RISC Report – Cyber Risk #4: Technologies and Services:

## Key Controls/Control Areas for this Risk:



# 2018 RISC Report – Risk #4: People, Process, Technology



## Vendor/Service Provider Risk Management and Procurement Controls

**People** –Procurement, Security Architecture, Security Operations Team, Audit/Compliance, Vendor/Supplier Resources/ System Administrators

**Process** – Corporate Supply Chain Process, Contracts, RFPs, NDA's,

**Technology** – Remote Access Process, Cloud Service Provider Technical Protections, NIDS, HIDS

## Vendor Service Provider Assessment and Audits

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

**Process** –Vulnerability Assessment, Exposure Mitigation, Vendor Assessments,, Certification(s), Audits, FedRAMP (Cloud Services)

**Technology** – Vulnerability Assessment Tools, Exercises, IDS, Electronic Architecture.

## Software Integrity and Authenticity

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

**Process** – Software Validity Verification, Software Monitoring, Software Assessment, Software Deployment, Vulnerability Assessment

**Technology** – Software Monitoring, Software Deployment, Vulnerability Assessment

## Intelligence Gathering/Sharing

**People** –, Security Operations Team, Audit/Compliance, Vendors/Government

**Process** – Intelligence Gathering/Evaluation/Sharing

**Technology** – Intelligence Sharing Platforms/Services

## 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

## Remote Access

**People** –Security Architecture, System Administrators, End User, Security Operations Team,

**Process** – Monitoring, Detection, Remote Access Procedures

**Technology** – Remote access servers, Jump Host, Firewall rules

## Information System Planning

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

**Process** –Corporate Requirements/policies, vendor polices and services

**Technology** – Security, Tool/Service Workflow, Technology Knowledge

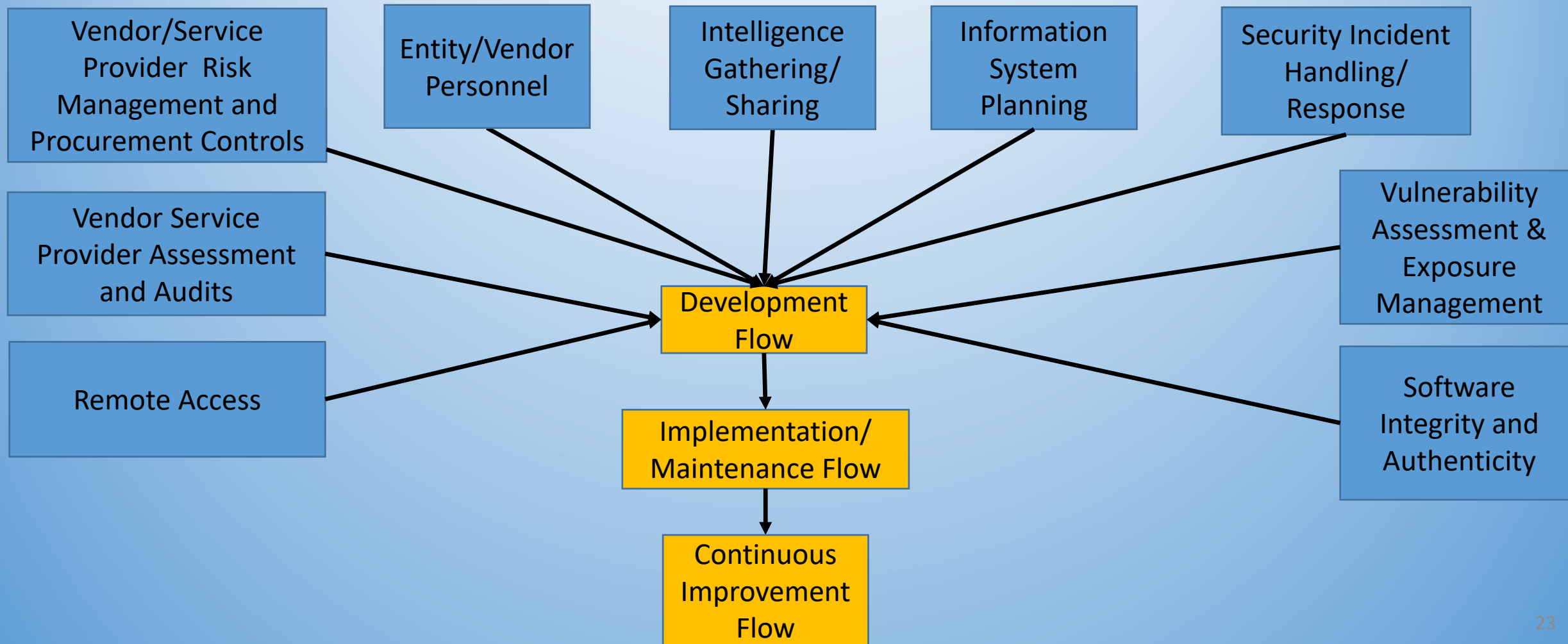
## Entity/Vendor Personnel

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

**Process** – Hiring/contracting Process, Contracts/NDAs, Skills/Knowledge, Employee Training Plan

**Technology** – Background checks, Employee/Vendor Reviews, Employee training

## Control Flow Development, Implementation/Maintenance, Continuous Improvement:

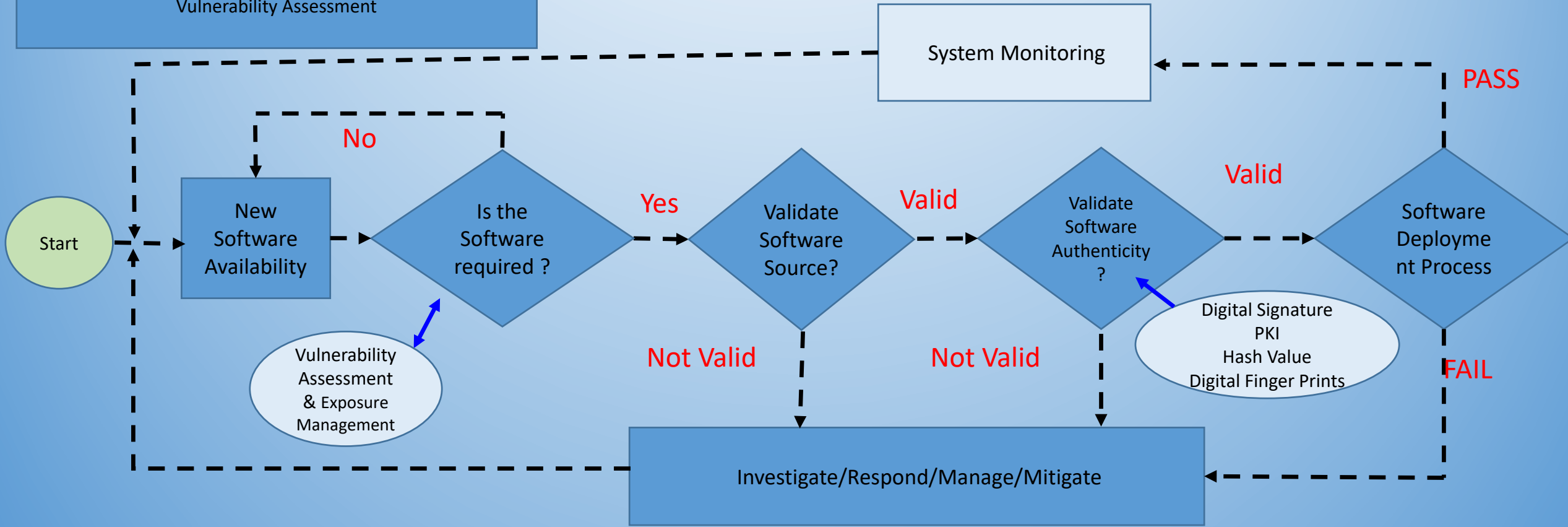


# 2018 RISC Report Risk #4 – Control Flow: Implementation/Maintenance

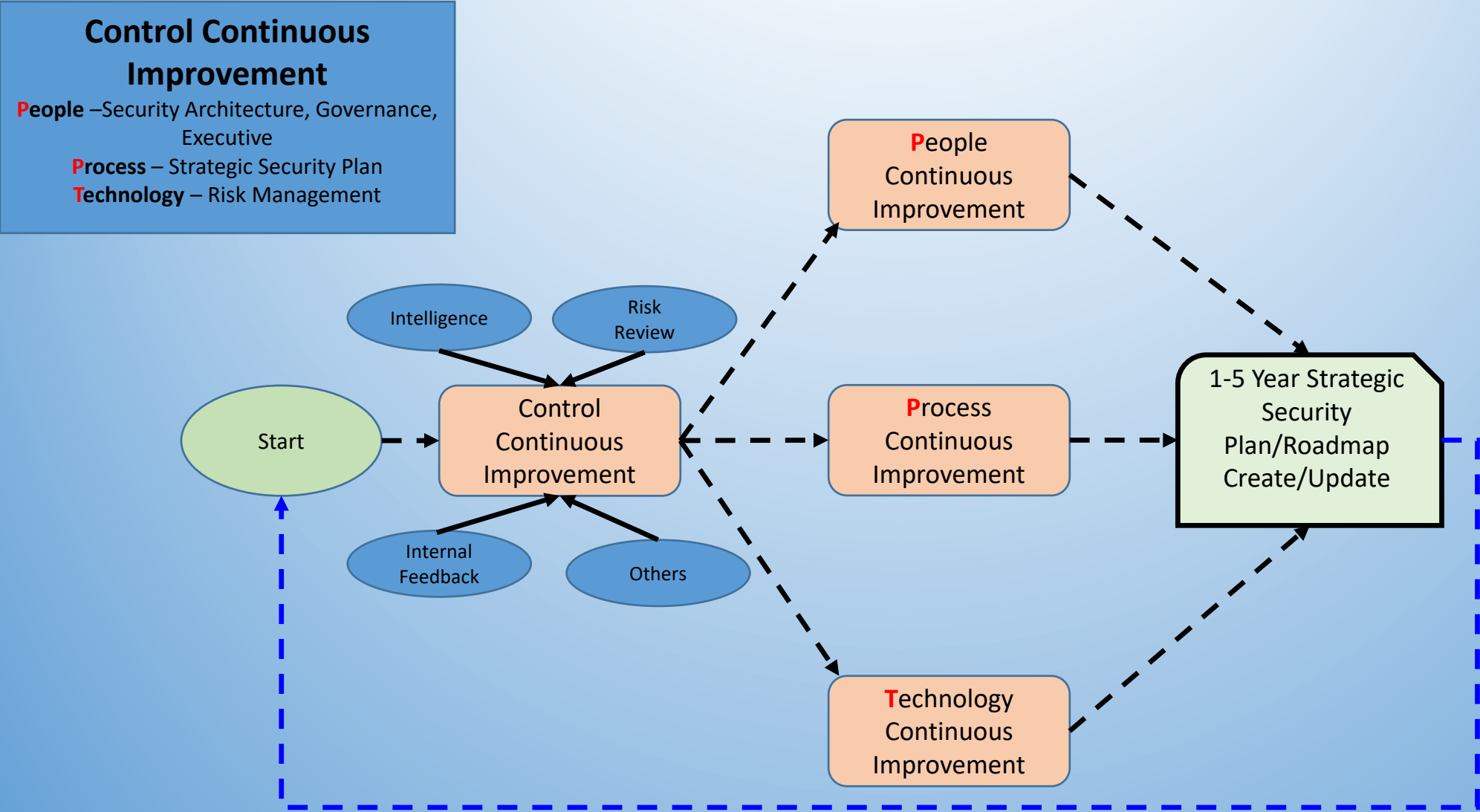


## Software Integrity and Authenticity

- People** –Security Architecture, Security Operations Team, System Administrators, Vendors
- Process** – Patch Validity Verification Patch Monitoring, Patch Assessment, Patch Deployment, Vulnerability Assessment
- Technology** – Patch Monitoring, Patch Deployment, Vulnerability Assessment



# 2018 RISC Report – Control Flow: Continuous Improvement



# 2018 RISC Report – Best Practices Sources

- **CIPC SCWG-** <https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx>
- **NATF –** <http://www.natf.net/documents>
- **EEI Cyber & Physical Security -**  
<https://www.eei.org/issuesandpolicy/cybersecurity/Pages/default.aspx>
  - **Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk**  
- <https://www.eei.org/issuesandpolicy/cybersecurity/Documents/EEI%20Law%20-%20Model%20Procurement%20Contract%20Language%20%28Version%202%29%20031919.pdf>
- **US-CERT -**  
[https://www.energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems\\_040714\\_fin.pdf](https://www.energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf)
- **IIA Bulleting:** Cloud Security, Insider Threats, and Third-Party Risk, August 2019  
(Member Ship Required)

# Summary

## Key points to consider:

- Identify and document **P**eople, **P**rocess, **T**echnology 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](mailto:ERA@NPCC.org)*