

Controls for Cyber Security Risks

NPCC Entity Risk Assessment (ERA) Group



NPCC 2019 Webinar
December 11, 2019

NPCC Entity Risk Assessment Group

- Risk Assessments
- Evaluation of Internal Controls
- Outreach – training, internal controls frameworks to mitigate risks, documentation and testing, workshop presentations, webinars, onsite visits
- Ben Eng – Manager, ERA
- Duong Le – Senior Compliance Engr
- Mike Bilheimer – Senior CIP Analyst



“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

ERO Reliability Risk Priorities, February 2018

RISC's Recommendations to the NERC Board of Trustees

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

Reliability Issues Steering Committee (RISC):

- is an advisory committee to the NERC Board of Trustees (Board).
- provides key insights, priorities, and high-level leadership for issues of strategic importance to BPS reliability.
- advises the Board, NERC standing committees, NERC staff, regulators, REs, and industry stakeholders of key risks to reliable operation of the BPS and recommendations to mitigate those risks
- provides guidance to the ERO Enterprise and industry to effectively focus resources on the critical issues to improve the reliability of the BPS.

ERO Reliability Risk Priorities, February 2018

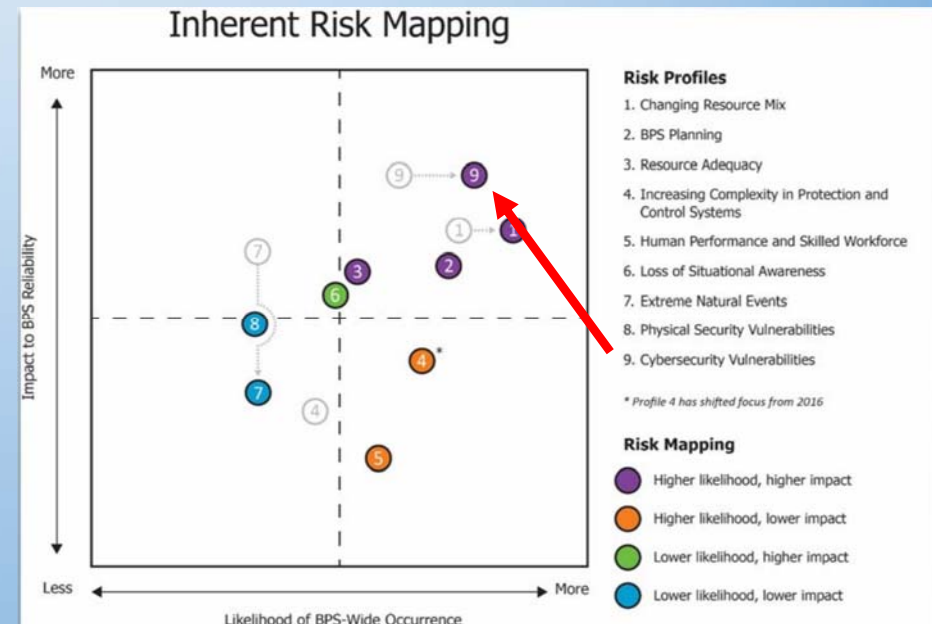
(Presented at NPCC 2019 Spring Workshop)

- Heat map identified CyberSecurity Vulnerabilities Risk Profile as Highest *Impact to BES Reliability* and 2nd highest *Likelihood of BPS Wide Occurrence*

“...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)



Outreach



2018 Reliability Issues Steering Committee (RISC) Report 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.

NPCC 2019 Spring Workshop Presentation – Controls to address the above

https://www.npcc.org/Compliance/Entity%20Risk%20Assessment/pptNPCC_2019Spring_Controls_RISC_BEng_051919.pdf

Controls for Cyber Security Risks



- 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.

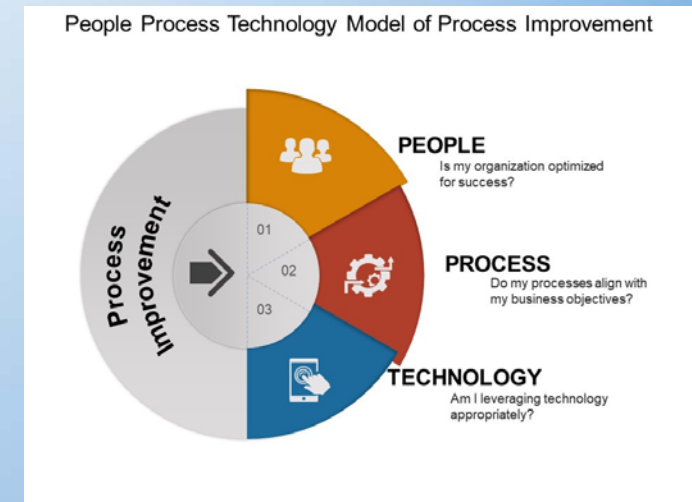
2018 RISC Report – Controls

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)

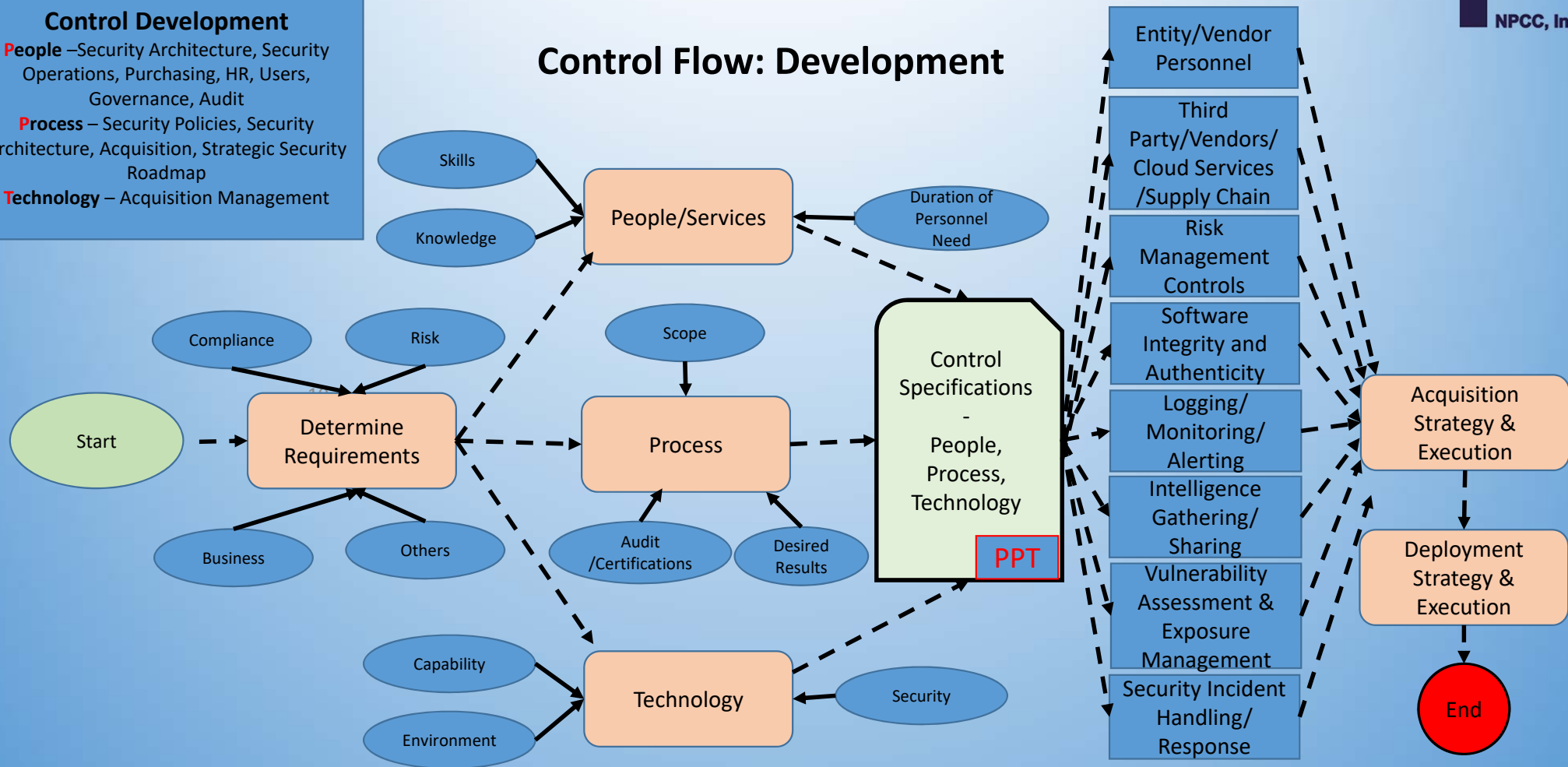
Control Development

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



Human Capital Controls

- Personnel Risk Assessment/Background Checks
- Human Capital Skills
- Vendor and Third Party Risk Assessment
- Periodic reviews of personnel risks, access authorization and rights
- Interpersonal relationships
- Personnel annual reviews
- Job rotations for key positions.

Technical Controls

- System Monitoring
- Preventive and corrective Systems (Firewalls , Intrusion Detections/prevention, Anti Malware and White listing, Remote Access)
- Restricted Access
- Vulnerability Assessment & Exposure Management

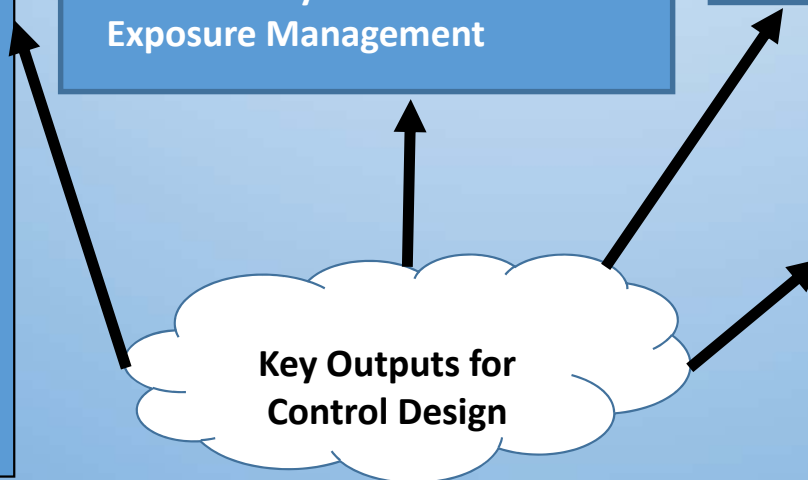
Processes Controls

- Internal control evaluations
- Process and Technical Security Controls effectiveness and adherence review.
- Third Party Audits/ Certifications of Service Provider (Fedramp, ISO IEC 2700, SSA 16)
- Contract and SLA Management
- Procurement Management

Internal/External Threats Awareness

- ES-ISAC
- NERC Alerts
- FBI/DHS/Local Police
- Third Party Vendors
- Other Utilities
- Entity Personnel

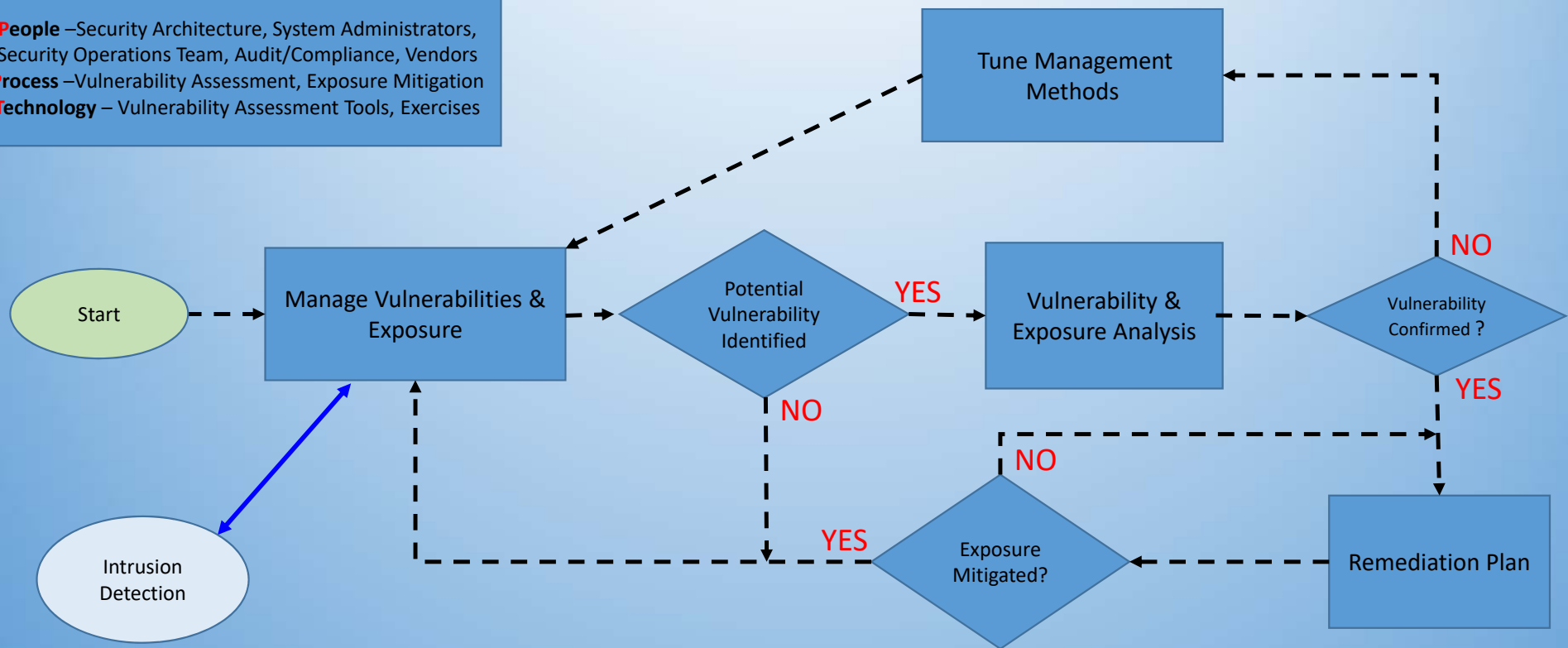
Key Outputs for Control Design



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

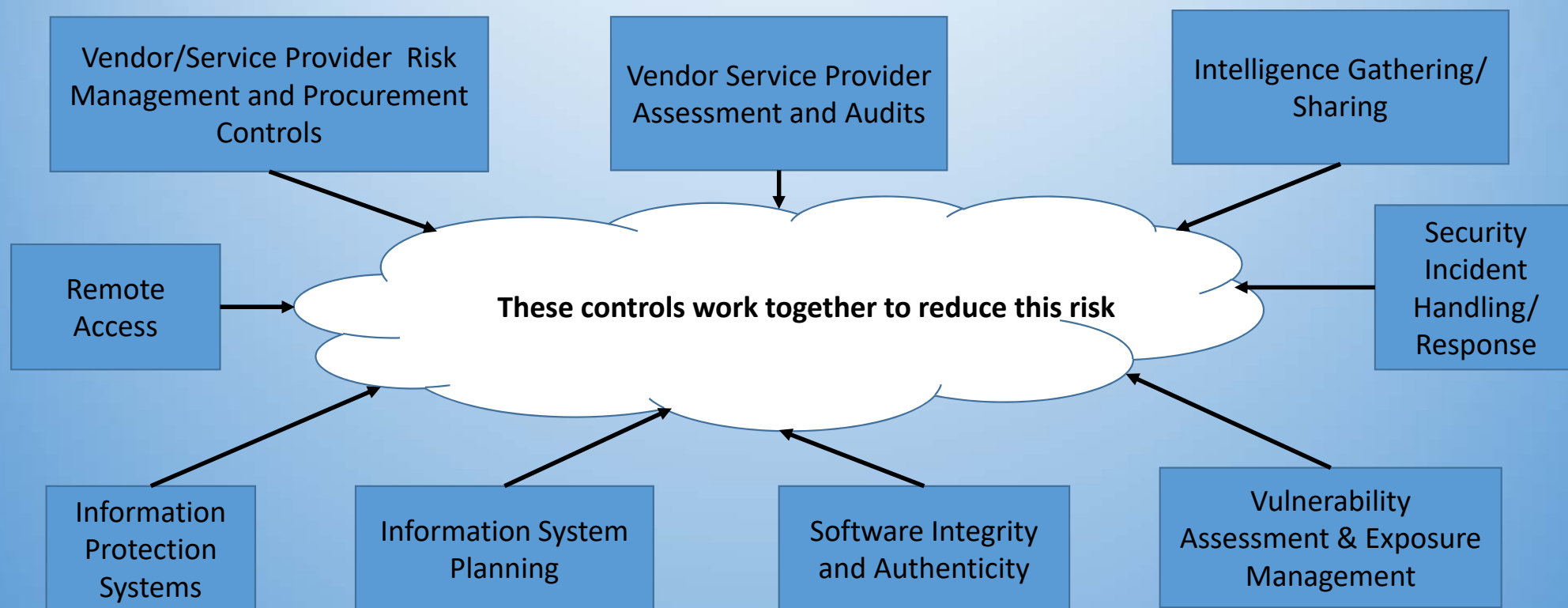
Vulnerability Assessment & Exposure Management

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 policies and services

Technology – Security, Tool/Service Workflow, Technology Knowledge

Entity/Vendor Personnel

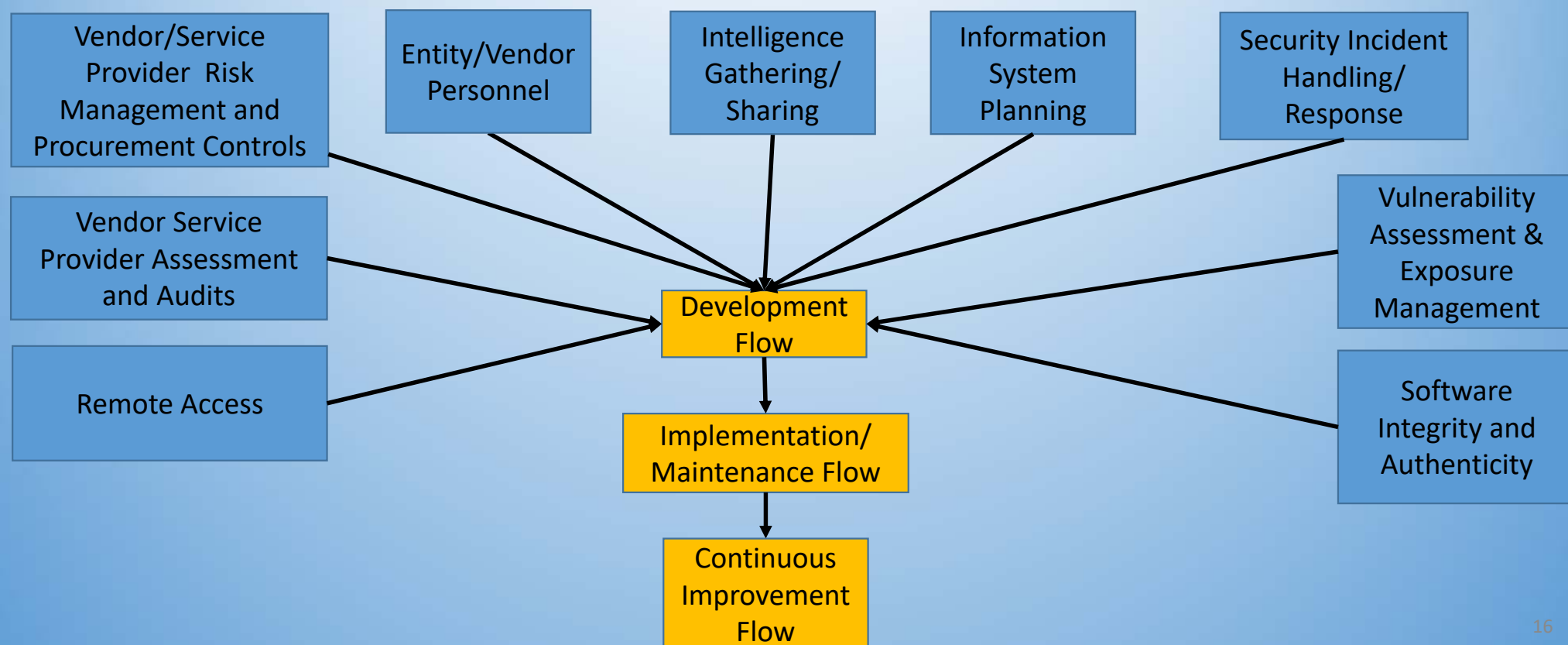
People –Security Operations Team, Human Resources, System Administrators, Users

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

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

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

Control Flow Development, Implementation/Maintenance, Continuous Improvement:



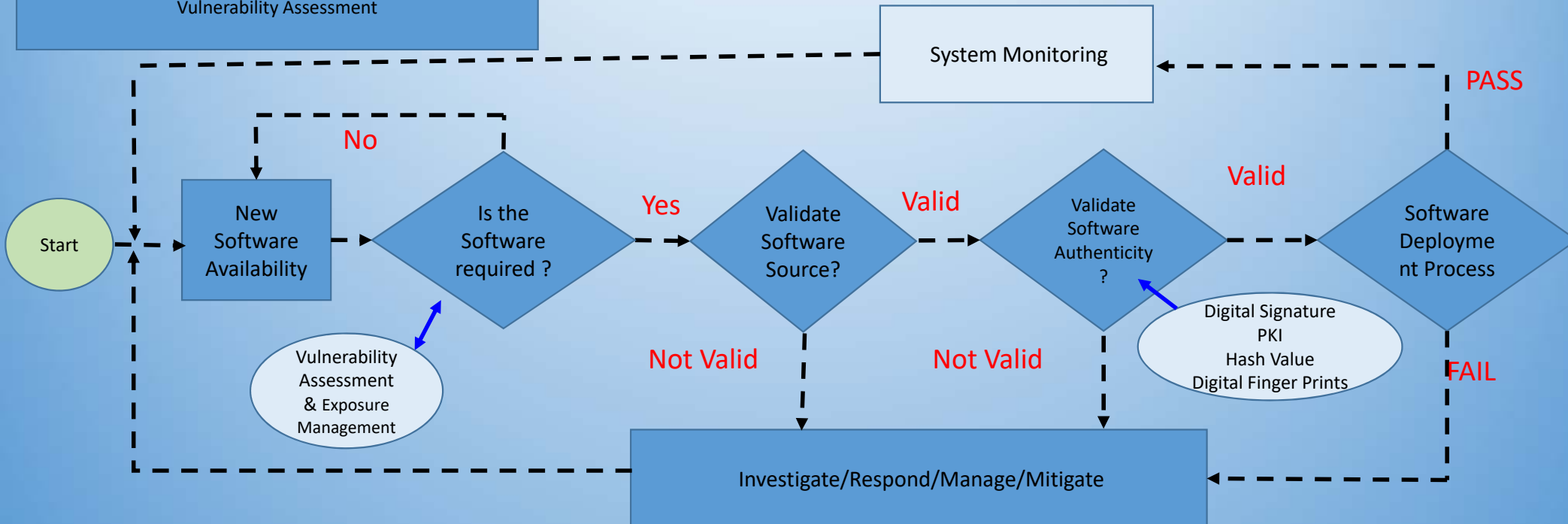
2018 RISC Report Risk #4 – Control Flow: Implementation/Maintenance

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



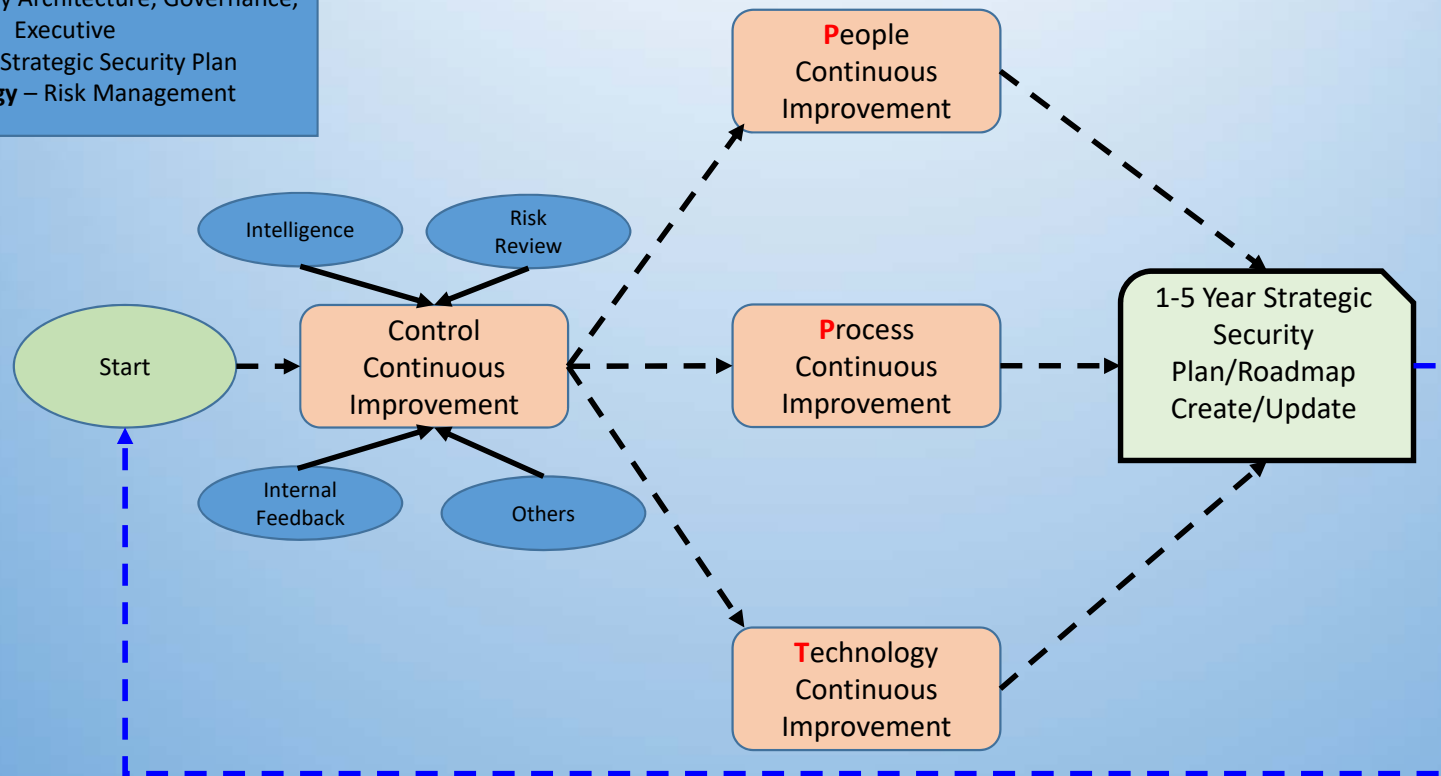
2018 RISC Report – Control Flow: Continuous Improvement

Control Continuous Improvement

People – Security Architecture, Governance, Executive

Process – Strategic Security Plan

Technology – Risk Management



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_031919.pdf
- **US-CERT -**
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 **D**evelopment, **I**mplementation/**M**aintenance and **C**ontinuous Improvement
- One size doesn't fit all



A photograph of a dark asphalt surface with several large, light-colored question marks painted on it. The word 'Questions?' is overlaid in a large, red, italicized serif font.

Questions?

Email: ERA@NPCC.org