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

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.
“...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
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

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.
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

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

- **Hiring Requirements**
  - Position Required Skill Sets
  - Contractor Vs Employee
2018 RISC Report – Human Capital Knowledge and Experience

Security Incident Handling/Response
- Internal Incident Response Drills
- GridEX

Specialized/Specific Training
- Certifications (CISSP, CISA)
- System/Device Training
- Idaho Labs
- GridEx
- SANS GIAC

Key Inputs for Control Design

Working Group Participation and Professional Membership
- NPCC Task Forces and Working Groups, NERC Standard Development, E-ISAC
- Industry Trade Groups
- GridSecCon
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:

- Anti-Malware
- Logging/Monitoring/Alerting
- Intelligence Gathering/Sharing
- Intrusion Detection
- Patch Management
- Specialized/Specific Training
- Security Incident Handling/Response
- Vulnerability Assessment & Exposure Management

These controls work together to reduce this risk.
Control Flow Development, Implementation/Maintenance, Continuous Improvement:

- Intrusion Detection
- Anti-Malware
- Logging/Monitoring/Alerting
- Intelligence Gathering/Sharing
- Specialized/Specific Training
- Security Incident Handling/Response
- Patch Management
- Vulnerability Assessment & Exposure Management

Development Flow

Implementation/Maintenance Flow

Continuous Improvement Flow
Control Development

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


Technology – Acquisition Management

Control Flow: Development

Start

Determine Requirements
- Business
- Compliance
- Risk
- Others
- Capability
- Environment

People
- Skills
- Knowledge

Process
- Scope
- Desired Results

Technology
- Control Specifications - People, Process, Technology

Control Flow: Development

End

PPT

Patch Management
- Vulnerability Assessment & Exposure Management
- Intrusion Detection
- Anti-Malware
- Logging/Monitoring/Alerting
- Intelligence Gathering/Sharing
- Specialized/Specific Training
- Security Incident Handling/Response

Acquisition Strategy & Execution
- Deployment Strategy & Execution
Intrusion Detection

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

**Process** – Monitoring, Update, Detection, Response

**Technology** – NIDS, HIDS, Network/Host/Application

Firewalls, Exercises

---

Start

Monitor/Detect Intrusions

Known or Suspected Intrusion Detected? (YES/NO)

Initial Investigation

Tune Detection Methods

Invoke Cyber Security Incident Management Plan

Actual Event/Incident? (YES/NO)

Vulnerability Assessment & Exposure Management
2018 RISC Report Risk #7 – Control Flow: Implementation/Maintenance

Vulnerability Assessment & Exposure Management

Process – Vulnerability Assessment, Exposure Mitigation
Technology – Vulnerability Assessment Tools, Exercises

Start

Manage Vulnerabilities & Exposure

Potential Vulnerability Identified

Vulnerability & Exposure Analysis

Vulnerability Confirmed?

Remediation Plan

Tune Management Methods

Exposure Mitigated?

Intrusion Detection

YES

NO

YES

NO

YES

NO

YES

NO
2018 RISC Report – Control Flow: Continuous Improvement

Control Continuous Improvement
- People – Security Architecture, Governance, Executive
- Process – Strategic Security Plan
- Technology – Risk Management

Start → Control Continuous Improvement → Process Continuous Improvement
         /          /
        /            /
   Intelligence     Risk   Technology Continuous Improvement

   Internal Feedback   Others

   1-5 Year Strategic Security Plan/Roadmap Create/Update
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