O&P Internal Controls Evaluation (ICE) Update

NPCC Compliance Workshop
November 8, 2017

Ben Eng
NPCC
Manager, Entity Risk Assessment
'Assuring BES Reliability through Risk and Controls Management'
Agenda

• Three (3) Presentations related to Internal Controls and Risk Assessments
  – This presentation is your “appetizer”
  – *Enhancing CIP Cybersecurity Through Risk Management* is the “main course”
  – *Ontario IESO ICE Program* presentation this afternoon is your sweet “dessert”
Agenda

• 2017 Results and 2018 Workplan

• Lessons Learned
ERO Risk Based Compliance Monitoring Framework
2017 Results

Change Management:

• All NPCC Entities had their Inherent Risk Assessments completed by the end of 2016. The IRA Summary Report was a snapshot in time of the Risk Factors and the (pre-ICE) audit scope at the time of the report.

• For 2017, the NPCC ERA group reviewed the IRA Summary reports and refreshed the pre-ICE scopes for all entities on the 2017 O&P audit schedule.

• ICE was offered to all entities on the O&P Audit Schedule.
All eight (8) entities shown above volunteered for ICE prior to the scheduled audit. Several entities having onsite O&P audits volunteered for ICE and benefited from NPCC’s free controls analysis and obtained a better understanding of their internal controls.
# 2018 Audit Schedule


<table>
<thead>
<tr>
<th>Type*</th>
<th>Entity Name</th>
<th>NCR</th>
<th>Region</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-Site</td>
<td>Vermont Transco, LLC</td>
<td>NCR07228</td>
<td>NE</td>
<td>4/9/2018</td>
</tr>
<tr>
<td>On-Site</td>
<td>ISO-NE</td>
<td>NCR07124</td>
<td>NE</td>
<td>6/4/2018</td>
</tr>
<tr>
<td>On-Site</td>
<td>Central Maine Power Company</td>
<td>NCR07029</td>
<td>NE</td>
<td>9/10/2018</td>
</tr>
<tr>
<td>On-Site</td>
<td>NSTAR Electric Company</td>
<td>NCR07180</td>
<td>NE</td>
<td>10/22/2018</td>
</tr>
<tr>
<td>Off-Site</td>
<td>Norwood Municipal Light Department</td>
<td>NCR00415</td>
<td>NE</td>
<td>3/14/2018</td>
</tr>
<tr>
<td>Off-Site</td>
<td>Wheelabrator Bridgeport, L.P.</td>
<td>NCR02923</td>
<td>NE</td>
<td>3/14/2018</td>
</tr>
<tr>
<td>Off-Site</td>
<td>Mohegan Tribal Utility Authority</td>
<td>NCR07037</td>
<td>NE</td>
<td>3/14/2018</td>
</tr>
<tr>
<td>Off-Site</td>
<td>Norwich Public Utilities</td>
<td>NCR07038</td>
<td>NE</td>
<td>3/14/2018</td>
</tr>
<tr>
<td>Off-Site</td>
<td>Town of Wallingford Dept of Utilities</td>
<td>NCR07041</td>
<td>NE</td>
<td>3/14/2018</td>
</tr>
<tr>
<td>Off-Site</td>
<td>QB 1</td>
<td></td>
<td>QB</td>
<td>3/14/2018</td>
</tr>
<tr>
<td>Off-Site</td>
<td>Materials Innovation and Recycling Authority (MIRA)</td>
<td>NCR07045</td>
<td>NE</td>
<td>4/18/2018</td>
</tr>
<tr>
<td>Off-Site</td>
<td>Hudson Light and Power Department</td>
<td>NCR07107</td>
<td>NE</td>
<td>4/18/2018</td>
</tr>
<tr>
<td>Off-Site</td>
<td>Reading Municipal Light Department</td>
<td>NCR07206</td>
<td>NE</td>
<td>4/18/2018</td>
</tr>
</tbody>
</table>
Blast email to Primary Compliance Contacts

Subject: FW: 2018 O&P Compliance Monitoring - vote requested

Please Vote:

In order to finalize the proposed 2018 offsite O&P Audit Schedule, NPCC would like to know whether or not you intend to volunteer for Internal Controls Evaluation (ICE) by NPCC prior to your scheduled monitoring.

Please respond to this email by choosing one of the choices shown under the “Vote” button at the top of this email. A “No” vote will allow the Compliance Monitoring Group to refine their 2018 O&P Audit Schedule.
COSO* Model for Internal Controls

The COSO* Cube

- Control Environment – setting the tone at the top. Governance, Policies, Procedures
- Risk Assessment – identification and analysis of relevant risks. What are the things that keep you up at night?
- Control Activities – activities to address the identified risks. They are reciprocals to risks. Reconciliations, segregation of duties, approvals
- Monitoring – review and manage control designs. Can degrade, be overridden or bypassed. Is it working?

* Committee of Sponsoring Organizations of the Treadway Commission
Why do bad things happen to good people?

Has this ever happened to you?
• Lost/misplaced your keys, wallet, purse, smartphone?
• Lock yourself out of the house or car?
• Forget to pack something for a trip?
• Forget the reason you walked into a room in your home?
• Allow an important document to expire (driver’s license, passport, car inspection)
• Forget to pay or mail a bill or letter?

Hopefully, the above did not result in any serious consequences.
What were the causes for these mishaps?

- Distraction; not paying attention to what you’re doing
- Multitasking
- Forgot to write it down
- Not a routine activity; off normal; new responsibility
- First time doing something or not done in a long time
- Complacency – “I’ve done it a million times. I can do it in my sleep”
- Overconfidence - Willing to accept risks/consequences (at the time)
- Laziness; taking a short cut; cutting corners
- Not exercising your internal controls
Lessons Learned

“Those who cannot remember the past are condemned to repeat it.” – George Santayana

• Do you have internal controls that could have prevented the bad things from happening? Absolutely!
• Do we take our Internal Controls for granted?
• When we get lazy and use them inconsistently or only when convenient, bad things can happen.
• Consistent and disciplined use of internal controls increase our chances of successfully achieving our goals.
Personal Internal Control Tools

• Mnemonics (letters, words, expressions, rhymes)
  – HOMES or Super Man Helps Every One
  – ROY G BIV
  – “I before E except after C....”
  – My Very Excited Mother Just Served Us Nine Pies
  – “Thirty Days hath September, April, June, and....”
  – R-I-C-E (Rest Ice Compression Elevation)
  – Spell Mississippi (M-I-S-S-I-S-S-I-P-P-I)
  – I Value Xylophones Like Cows Dig Milk
  – ELI the ICE man (Voltage leads Current in inductive circuit)
  – FUNKY WALL GLASS (= phone, keys, wallet, glasses)

[copyright pending by Ben Eng]
Personal Internal Control Tools

• Lists
  – Grocery List
  – Back to School List
  – Packing List
  – Honeydew ("Honey, do this") List
  – Work Priority List, Schedules
  – Bucket List
  – Christmas wish List
  – Best restaurants in the area
  – Wines/Beer to try
Personal Internal Control Tools

- Training & Skills
  - Education
    - Grade, intermediate, high school
  - College
    - Bachelors, Masters, Doctorate
  - Licenses/Certifications/Permits
    - Drivers, Pilots, Professional Engineer, CPA, Law
    - Chiropractic, Reflexology, Acupuncture, Nutritional
    - Theological, Veterinary
    - Law Enforcement, Fire, EMT
    - Rifle/Pistol
  - Hobbies
    - Sports, Athletics, Recreational, Culinary, Intellectual, Health, Dancing
    - Self taught, instructional videos, YouTube, practice
    - Instructors, classes, trainers, tutors
Internal Controls Venn Diagram

Internal Control Designs generally consist of a combination of the three “Control Silos” shown below

- Document, review and assess Internal Controls that are volunteered for evaluation by the Registered Entity.
- “Tease out” and document controls that are taken for granted, or not formalized.
- Ask the 5 “W” and 1 “H” questions pertaining to the control silos that are preventative, detective and/or corrective to “drift from compliance”.
- Interview Subject Matter Experts and task performers to determine whether controls have been implemented.
- Obtain reasonable assurance that entity’s internal controls mitigate risks to BES reliability so that NPCC ICE team can make informed decisions regarding appropriate compliance monitoring tools.
Lessons Learned

“I have policies and procedures for (activity). Aren’t those my internal controls?”

- Procedures and Policies do not make up the entirety of your internal controls. They are one component of the Control Silos.
- The procedures/policies cannot implement the actions, expectations, criteria, decisions, reviews, approvals described within them.
- Generally you need the support of the other two control silos – tools and skilled human capital. Their overlap generally indicates key controls.
Lessons Learned

“I developed my Internal Controls designs and you “ICE’d” them. I’m done, right?”

• Internal Controls designs and their evaluations are not a one time occurrence. They are “living” and need to be maintained.
• They need to be tested initially and periodically.
• They can degrade over time, overwritten or bypassed.
  – The control objectives may change
  – The automation or technology may change
  – The skilled human capital needs may change
  – Oversight, approvals, checks and balances may change due to organization changes (consolidation with other units or companies)
• Change management must be applied.
Lessons Learned

“Process Flow Diagrams? We don’t need no stinking Process Flow Diagrams!”

• NPCC has done many ICE and promote the use of annotated process flow diagrams accompanied with narrative description. The Institute of Internal Auditors recommends flowcharts for process mapping.
• A picture is worth a thousand words
• Beneficial because it promotes and documents internal and inter-departmental communications, handoffs, feedback; provides a sense of ownership and value added to the process. Useful as a training tool and reference for succession planning.
• Refer to the Internal Controls Silos diagram for self/peer check and independent reviews to confirm process flows and control designs. Ask the 5W and 1H questions.
Attributes of Better Internal Controls

• Repeatable results
  – Automated tools generally provide consistent results
  – SCADA, EMS, Work Management, Software (Databases, Queries, Reports)

• Monitoring/Early warning
  – Periodic or Real Time monitoring of planned work.
  – Reminders well in advance of deadline. Provides “margin” to meet compliance and avoid need to Self Report

• Feedback/Closure
  – Process to ensure completion of work before approving closeout of work package/ticket/report
  – Maintain records (e.g. maintenance/test records) supporting the closeout of work tickets.
QUESTIONS?
Thank You
Enhancing CIP Cybersecurity Through Risk Management

Lee Budd
Duong Le
Ben Eng
The Imposing Cyber Risk Landscape

- Hacking – many complex activities to gain access to a computer system’s servers, databases and files; can be applied to all layers of the environment, networks, OS, web applications, databases & mobile devices, etc.
- Advanced Persistent Threat – a network attack by an unauthorized entity to steal data and that goes undetected for a period of time (often nation states)
- State Sponsored Terrorism
- Organized Crime
- Industrial Espionage
- Extortion – a cybersecurity crime involving an attack or threat with a demand for money
- Intellectual Property Theft
- Identity Theft
- Data Breach, Data Corruption & Data Loss
- Social Engineering/Phishing- involves tricking people into breaking normal security procedures
- Distributed Denial of Service – an interruption in an authorized user’s access to a computer network (caused by malicious intent)
- Malware – Malicious code that is intended to damage or disable computers and systems
The Imposing Cyber Risk Landscape

- Social Media (aka “that Hot Stinking Mess”)
- Changes arising from Smart Grid Dynamics vs. the more conventional Generation, Transmission, and Distribution model
Targeting Risk Thru Controls Resiliency

- NERC RAI was conceived (at least in part) to address risk based compliance monitoring
- Progressive compliance monitoring and control functions are now evolving to consider risk management techniques to inform their assessments
- Current compliance monitoring efforts have also been re-focused to address not only standards/requirements, but also risk mitigation thru internal controls (aka the risk response)
- Of note, internal controls also share a reciprocal relationship to risk (weak or missing controls = poor risk mitigation and may compromise reliability)
Targeting Risk Thru Controls Resiliency

- Current day CIP Cybersecurity resiliency (risk mitigation) has progressed from:
  - Traditional monolithic (boundary / perimeter protections)
  - Augmented boundary protection with detection and response measures
  - Agile (resilient) dual protection (layered) strategies relying on both the ‘depth and breadth of defenses’
  - Today’s progression in cyber risk mitigation and resiliency is a direct result of the level of persistent cyber threats and attacks
The Breach Quadrilateral

• Infiltration
  - The point at which the attacker gets into an organization.

• Propagation
  - Where the bad guys pivot, as the initial point of entry isn’t always where they want to be.

• Aggregation
  - When the attacker finds and collects all the data that is being sought.

• Exfiltration
  - About getting out without being detected.
Targeting Risk Thru Controls Resiliency

• Cybersecurity risk frameworks & tools can be overlaid to link standards & requirements with corresponding risk types and mitigating internal controls

• Managing / mitigating risks through robust-resilient internal controls & designs strengthens BES Reliability

• NPCC ERA Group Moniker (Tag Line): “Assuring Reliability through Risk and Controls Management”
Risk Primer

• Enterprise Risk Management (ERM) Strategy:
  – Managing Risks & Internal Controls
• ERM Control Objectives:
  – Strategic
  – Operations
  – Reporting & Compliance
• ERM (Components / Dimensions):
  – Internal Environment
  – Objectives Setting
  – ID Internal & External Risk Events
  – Assess Risk
  – Risk Response
  – Control Activities
  – Information & Communications
  – Monitoring
Risk Primer

• Dimensions to ERM (managing the response):
  – Risk Acceptance
  – Risk Avoidance
  – Risk Mitigation / Reduction
  – Risk Sharing
  – Risk Transference
  – Combination
• Risk Appetite = amount of risk an Entity accepts
• Risk Tolerance = acceptable level of variation relative to achieving business objectives
• Controls = response to risk (ERM)
• Examples of some ERM resource tools include the use of risk register, risk dashboards, quantitative models, heat maps, etc.
• ERM also integrates with COSO component principles and requirements encompassing both CIP and O&P
Risk Primer

- Basic risk types/categories when assessing risk mitigation, internal controls, and reliability:
  - Operations Risk
  - Systems & Technology Risk
  - Legal & Compliance Risk
  - Fraud & Theft Loss Risk
  - Third Party & Supply Chain Risk
  - Market Risk
  - Data Breach / Loss Risk
  - Insurance Coverage Risk (through Delinquency)
  - Name and Reputation
  - Fines and Censure
Governance Risk Compliance

BOD’s, Business Objectives, Organizational Structure, ERM Strategy, Risk & Audit Committees, Profitability, ROE, KPI’s, KRI’s

Compliance Audit, Standards & Requirements, Control Activities, ICE, Information & Communications, Monitoring & Reporting, SOC1 & SOC2, SSAE16/SAS70, SARBOX

Risk Mgmt. Frameworks Methods & Tools: ERM, NIST, ES C2M2, NARUC, Standards & Requirements, ICE, etc.
ES C2M2 - Profile

• Electricity Subsector - Cybersecurity Capability Maturity Model
• Based on Maturity & Implementation Levels (MIL1, MIL2, MIL3)
• Framework used to assess & manage cybersecurity risk
• Consists of RM principles & practices
• Includes RM processes to inform cybersecurity decision making based on business needs
• Framework can be sized to fit all organizations (i.e., flexible / scalable) or used in a targeted fashion
• Meant to be compatible with or augment existing Entity RM and cybersecurity programs (including the NERC Standards)
• Developed by DOE in partnership with DHS and in collaboration with private and public-sectors
ES C2M2 - Profile

• Tailored to energy sector risk environment, and related RM tools and processes:
  – Allows for profiling of current & target CS postures
  – Enables comparison of CS RM practices to overall ERM strategy
  – ID’s CS RM program gaps
  – ID’s ES C2M2 framework areas exceeded
  – ID’s existing sector tools, standards and guidelines supporting the framework
  – Provides for a tangible demo of the Entity RM approach and its application to stakeholders
  – Enables assessment of organizational cybersecurity practices for consistency
  – Guides reviews of threats, vulnerability & asset management practices for information and operations technologies
ES C2M2 - Profile

- C2M2 Domains or Practices (aka NIST Framework Category / Subcategory)
  - Asset, Change, and Configuration Management (ACM)
  - Cybersecurity Program Management (CPM)
  - Supply Chain and External Dependencies Management (EDM)
  - Identity and Access Management (IAM)
  - Event and Incident Response, Operations Continuity (IR)
  - Information Sharing and Communications (ISC)
  - Risk Management (RM)
  - Situational Awareness (SA)
  - Threat and Vulnerability Management (TVM)
  - Workforce Management (WM)
# ES-C2M2 Maturity Indicator Levels (MILs)

<table>
<thead>
<tr>
<th>Level</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIL0</td>
<td>Practices are not performed</td>
</tr>
<tr>
<td>MIL1</td>
<td>Initial practices are performed but may be ad hoc</td>
</tr>
</tbody>
</table>
| MIL2  | Institutionalization characteristics:  
\- Practices are documented  
\- Stakeholders are identified and involved  
\- Adequate resources are provided to support the process  
\- Standards or guidelines are used to guide practice implementation  

Approach characteristic:  
\- Practices are more complete or advanced than at MIL1 |
| MIL3  | Institutionalization characteristics:  
\- Activities are guided by policy (or other directives) and governance  
\- Policies include compliance requirements for specified standards or guidelines  
\- Activities are periodically reviewed for conformance to policy  
\- Responsibility and authority for practices are assigned to personnel  
\- Personnel performing the practice have adequate skills and knowledge  

Approach characteristic:  
\- Practices are more complete or advanced than at MIL2 |

Source: Electricity Subsector Cybersecurity Capability Maturity Model Version 1.1
Domains Graphical Summary of the C2M2 Survey
Objectives Graphical Summary of 4 of the 10 Domains on the C2M2
Steps in a Typical Process Improvement Activity

• The C2M2 evaluates maturity across 10 domains of cybersecurity and identifies specific gaps as a means to initiate a process improvement project
# Recommended Process for Using Results

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Activities</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform Evaluation</td>
<td>Conduct C2M2 Self-Evaluation Workshop with appropriate attendees</td>
<td>C2M2 Self-Evaluation Report</td>
</tr>
<tr>
<td>1. C2M2 Self-Evaluation</td>
<td>1. Analyze gaps in organization’s context</td>
<td>List of gaps and potential consequences</td>
</tr>
<tr>
<td>2. Policies and procedures</td>
<td>2. Evaluate potential consequences from gaps</td>
<td></td>
</tr>
<tr>
<td>3. Understanding of cybersecurity program</td>
<td>3. Determine which gaps need attention</td>
<td></td>
</tr>
<tr>
<td>Analyze Identified Gaps</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. C2M2 Self-Evaluation Report</td>
<td>1. Identify actions to address gaps</td>
<td>Prioritized implementation plan</td>
</tr>
<tr>
<td>2. Organizational objectives</td>
<td>2. Cost-benefit analysis (CBA) on actions</td>
<td></td>
</tr>
<tr>
<td>3. Impact to critical infrastructure</td>
<td>3. Prioritize actions (CBA and consequences)</td>
<td></td>
</tr>
<tr>
<td>Prioritize and Plan</td>
<td>4. Plan to implement prioritize actions</td>
<td></td>
</tr>
<tr>
<td>1. List of gaps and potential consequences</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Organizational constraints</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implement Plans</td>
<td>1. Track progress to plan</td>
<td>Project tracking data</td>
</tr>
<tr>
<td>1. Prioritized implementation plan</td>
<td>2. Reevaluate periodically or in response to major change</td>
<td></td>
</tr>
</tbody>
</table>

19
NIST – National Institute of Standards & Technology

• The electricity subsector RMP guide is a collaborative development by the DOE, with assistance from NIST & NERC
• Members of industry & utility trade groups provided input and authorizing guidance to the RMP
• NIST Interagency Report (NISTR 7628) addresses Guidelines for SMART Grid Cyber Security
• NERC Critical Infrastructure Cybersecurity Standards define / refine effective Cyber Security for Electricity Subsector Org’s.
• For Entities subject to compliance with NERC CIP Cybersecurity Standards, Entities are expected to use this guideline, although it does not alter NERC compliance requirements for these Entities
NIST – National Institute of Standards & Technology

• The Program Core: consists of cyber activities / practices, desired outcomes, and informing references

• High Level Function(s) depicting the strategic view of Entity cyber security management
  ▪ Identify (ID) Protect (PR) Detect (DE) Respond (RS) Recover (RC)
    ▪ Categories – cyber program outcomes / activities
    ▪ Sub categories – technical / mgmt. activity outcomes
    ▪ Informative References – cross sector standards, guidelines and practices supporting outcomes
# NIST Cybersecurity Risk Framework

## Functions and Categories

<table>
<thead>
<tr>
<th>Function Unique Identifier</th>
<th>Function</th>
<th>Category Unique Identifier</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>IDENTIFY</td>
<td>ID.AM</td>
<td>Asset Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.BE</td>
<td>Business Environment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.GV</td>
<td>Governance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RM</td>
<td>Risk Management Strategy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.SC</td>
<td>Supply Chain Risk Management</td>
</tr>
<tr>
<td>PR</td>
<td>PROTECT</td>
<td>PR.AC</td>
<td>Access Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.AT</td>
<td>Awareness and Training</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.DS</td>
<td>Data Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.IP</td>
<td>Information Protection Processes and Procedures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.MA</td>
<td>Maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.PT</td>
<td>Protective Technology</td>
</tr>
<tr>
<td>DE</td>
<td>DETECT</td>
<td>DE.AE</td>
<td>Anomalies and Events</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.CM</td>
<td>Security Continuous Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.DP</td>
<td>Detection Processes</td>
</tr>
<tr>
<td>RS</td>
<td>RESPOND</td>
<td>RS.RP</td>
<td>Response Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.CO</td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.AN</td>
<td>Analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.MI</td>
<td>Mitigation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td>RC</td>
<td>RECOVER</td>
<td>RC.RP</td>
<td>Recovery Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.CO</td>
<td>Communications</td>
</tr>
</tbody>
</table>

Source: Framework for Improving Critical Infrastructure Cybersecurity Draft Version 1.1
**NIST CSF Functions, Categories, Subcategories and Controls**

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDENTIFY (ID)</td>
<td>Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization’s risk strategy.</td>
<td>ID.AM-1: Physical devices and systems within the organization are inventoried</td>
<td>• CCS CSC 1  • COBIT 5 BA109.01, BA109.02  • ISA 62443-2-1:2009 4.2.3.4  • ISA 62443-3-3:2013 SR 7.8  • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2  • NIST SP 800-53 Rev. 4 CM-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.AM-2: Software platforms and applications within the organization are inventoried</td>
<td>• CCS CSC 2  • COBIT 5 BA109.01, BA109.02, BA109.05  • ISA 62443-2-1:2009 4.2.3.4  • ISA 62443-3-3:2013 SR 7.8  • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2  • NIST SP 800-53 Rev. 4 CM-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.AM-3: Organizational communication and data flows are mapped</td>
<td>• CCS CSC 1  • COBIT 5 DS05.02  • ISA 62443-2-1:2009 4.2.3.4  • ISO/IEC 27001:2013 A.13.2.1  • NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.AM-4: External information systems are catalogued</td>
<td>• COBIT 5 APO02.02  • ISO/IEC 27001:2013 A.11.2.6  • NIST SP 800-53 Rev. 4 AC-20, SA-9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.AM-5: Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value</td>
<td>• COBIT 5 APO03.03, APO03.04, BA109.02  • ISA 62443-2-1:2009 4.2.3.6  • ISO/IEC 27001:2013 A.8.2.1  • NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established</td>
<td>• COBIT 5 APO01.02, DS06.03  • ISA 62443-2-1:2009 4.3.2.3  • ISO/IEC 27001:2013 A.6.1.1</td>
</tr>
</tbody>
</table>
NIST RISK MANAGEMENT PROCESS
NIST - MULTITIERED ORGANIZATION-WIDE RISK MANAGEMENT

- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness

- Inter-Tier and Intra-Tier Communications
- Feedback Loop for Continuous Improvement
Implementing the NIST Cybersecurity Risk Framework

- Prioritize & Scope
  - Identify business/mission objectives, organizational priorities, systems and assets supporting the business.

- Orient
  - Identify threats and vulnerabilities applicable to systems and assets.

- Create a Current Profile
  - Assess current state of the organization’s cybersecurity program.

- Conduct a Risk Assessment
  - What is the likelihood of a cybersecurity event and the impact/consequence it has on the organization?

- Create a Target Profile
  - Desired cybersecurity outcome the organization would like to achieve.

- Determine, Analyze, and Prioritize Gaps
  - Analyze gaps between the current state and your Target Profile; Evaluate the potential consequences from these gaps, determine which gaps need attention; Identify actions to address gaps; Perform cost-benefit analysis on those actions; Prioritize actions (based on Cost Benefit Analyses and consequences)

- Implement Action Plan
  - Create a plan to implement the prioritized actions
NARUC Risk Management

1. Identify issues to manage
2. Establish risk tolerance / criteria
3. Analyze, evaluate and prioritize risks
4. Develop risk management options
5. Perform cost / benefit analysis
6. Take action in a cycle that include improvement
NARUC Risk Management

- Prioritize & Scope
- Orient
- Develop a current profile
- Conduct a risk assessment
- Create a target profile
- Determine, Analyze, and Prioritize Gaps
- Implement your action plan

Audience Polling

- Does your Company have a documented cybersecurity risk management strategy?
  a) Yes
  b) No

- What cybersecurity framework does your organization use?
  a) NIST
  b) ES-C2M2
  c) DOE RMP
  d) NARUC
  e) Other (Home-grown)
  f) None

- Does your organization’s cybersecurity risk assessment integrate with the organization’s overall risk management program?
  a) Yes
  b) No
CS RM Takeaways

- Info Systems Technology & Operations have all converged around being able to effectively manage risk
- Where feasible, leverage your organizations ERM strategy & resources
- Bolster your ERM strategy by utilizing the various cyber security RM frameworks, methods and tools available
- Commit to identifying, assessing & implementing an action plan for your cyber security risk program
- Resiliency in cyber systems is achieved thru Identifying and assessing risk(s) and deploying agile (resilient) dual protection (layered) strategies
- CIP cyber security compliance is more easily achieved or exceeded where risk-based assessments / tools are first applied and then mitigated through corresponding controls
CS RM Takeaways

- Your risk profile is probably bigger than you realize
- Application of R/M programs tend to skew the focus toward better practice element CIP controls and risk mitigation techniques
- Readily integrates risk identification and management oversight with corresponding CIP controls & CIP designs
- Also, considers alternative IT schemes for effective CIP asset hardening, protection and safeguarding (CIS CSC (SANS) Top 20, PCI/DSS, OWASP, etc.)
- It is possible to have both gaps in risk mitigation and controls while also conforming to the current suite of CIP standards & requirements
- Promotes the greater likelihood of attaining High Reliability Organization status (via risk identification, risk mitigation & controls integration)
- Facilitates a better understanding to address risk and controls required to harden and protect against the Breach Quadrilateral (Infiltration, Propagation, Aggregation, Exfiltration)
CS RM Takeaways

- Benefits ability to limit negative impacts from data loss, data corruption and data breach
- Better positions CIP management efforts toward pro-action and continuous process-improvement
- The integrated risk discipline and CIP-ICE better informs (i.e., qualitative & quantitative) resourcing, controls design and technological decision making
- Identifies control gaps and risks not mitigated through standards and requirements compliance
- Considers rigorous, effective and timely Incident response, remediation and reporting
- Helps to meet / fulfill Entity responsibilities required to maintain in force insurances and policy limitations / exclusions (E&O, Cyber, Data Loss, etc.)
- Aids in forestalling controls degradation, bypassing or overriding
Risk Assessment Frameworks

- NIST Framework for Improving Critical Infrastructure Cybersecurity - [https://www.nist.gov/cyberframework](https://www.nist.gov/cyberframework)
- DOE Electric Subsector Cybersecurity Capability Maturity Model (ES-C2M2) - [https://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/electricity-subsector-cybersecurity](https://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/electricity-subsector-cybersecurity)
- NARUC Risk Management in Critical Infrastructure Protection - [https://www.naruc.org/](https://www.naruc.org/)
Questions?

Lee M. Budd (lbudd@npcc-ic.org)
Duong Le (dle@npcc.org)
Ben Eng (beng@npcc.org)