Internal Controls Evaluation (ICE) Update
Equal Time for Other Sports

• Where are the Hall of Fames for these 10 sports
  – Football (Pro)
  – Basketball
  – NASCAR
  – Hockey
  – Golf
  – Soccer
  – Tennis
  – Swimming
  – Track and Field
  – Sailing
Equal Time for Other Sports

• Where are the Hall of Fames for
  – Football (Canton Ohio)
  – Basketball (Springfield MA)
  – NASCAR (Charlotte NC)
  – Hockey (Toronto Ontario; Eveleth MN – USA)
  – Golf (St. Augustine FL)
  – Soccer (Pachuca, Hidalgo, Mexico; Oneonta NY*)
  – Tennis (Newport RI)
  – Swimming (Ft. Lauderdale FL)
  – Track and Field (Washington Heights NY)
  – Sailing (Annapolis MD)
* closed
Is Baseball the most watched sport in the US?

- What are the rankings for most popular watched sports? Pick the top 5 in order
  - Soccer
  - Basketball
  - Football
  - Baseball
  - NASCAR
  - Hockey
  - Golf
  - Tennis
  - Swimming
  - Track and Field
  - Sailing
Is Baseball the most watched sport in the US?

- What are the rankings for most popular watched sports? Pick the top 5 in order
  - Soccer
  - Basketball (5 – 6%)
  - Football (1 – 35%) (3 – 11% College)
  - Baseball (2 – 14%)
  - NASCAR (4 – 7%)
  - Hockey
  - Golf
  - Tennis
  - Swimming
  - Track and Field
  - Sailing

**football**

In 2014, 35 percent of fans call the NFL their favorite sport, followed by Major League Baseball (14 percent), college football (11 percent), auto racing (7 percent), the NBA (6 percent), the NHL (5 percent) and college basketball (3 percent). Jan 26, 2014

[Harris Poll -- NFL still most popular; MLB 2nd - ESPN.com](espn.go.com/nfl/story/_/id/10354114/harris-poll-nfl-most-popular-mlb-2nd)
Topics

• Status of Internal Controls Evaluations
• Benefits of ICE
• Lessons Learned
• Appendix – references, examples
Intro and Background

NERC Risk-based Compliance Oversight Framework
• Allows each Registered Entity optional participation in ICE assessment by Regional Entity (NPCC).

Internal Controls Evaluation (ICE)
• refines scope, monitoring methods and frequency based on assessment of the organization’s Internal Controls and Internal Control Designs (ICD) implementation
• used to support and inform
  – ERO CMEP Implementation Plan
  – NPCC CMEP Implementation Plan (Appendix A3)
IRA results and Scoping are provided in the IRA Summary Report to the entity. Section 4 describes the pre-ICE audit scope.

If entity participates in ICE, then post-ICE proposed scope of audit and alternate monitoring methods are provided in the ICE Summary Report to the entity.
Compliance Monitoring Lifecycle

1. Inherent Risks of Entity
   - IRA Process

2. Risks to BER Reliability
   - NERC/Regional Risks
     - Risk Elements
     - Focus Areas
   - Other Risks
     - Operational
     - Emergent

3. Scoping Hopper

Risk Assessment

1. IRA Process
   - Initial & Periodic Refresh
   - Derivative of Registration
   - Risk Factors & Ratings

2. Risks to Reliability
   - Mapping to NERC Standards

3. "Scoping Hopper"
   - Criteria & Matrix
   - Determine Intensity & Frequency of Monitoring Based on Risk

4. Change Management
   - Applies to All Components and Processes Shown on This Sheet

Method/Intensity/Frequency of Compliance Monitoring

Results of Compliance and Self-Monitoring

Self Reports, Investigations, Violations, Mitigation

Audits

Spot Check/Self Certs

Not Monitored

Compliance History

Systemic or Common to > N Entities?
<table>
<thead>
<tr>
<th>Registered Entity</th>
<th>Entity Name</th>
<th>Number of Standards Provided for ICE review</th>
<th># of Reqs. (Pre-ICE)</th>
<th># of Reqs. Deferred to Alternate Monitoring Method(s) due to ICE</th>
<th># of Reqs. Remaining in Scope of Compliance Engagement (Post-ICE)</th>
<th>% Reqs. Deferred to Alternate Monitoring Method(s) due to ICE</th>
<th>% Reqs. Deferred to Alternate Monitoring Method(s) based on # of Applicable Reqs.</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>ENTITY A</td>
<td>26</td>
<td>57</td>
<td>32</td>
<td>25</td>
<td>56.1%</td>
<td>9.3%</td>
<td>DP, TO, TOP, TP, TSP</td>
</tr>
<tr>
<td>4</td>
<td>ENTITY B</td>
<td>6</td>
<td>26</td>
<td>13</td>
<td>13</td>
<td>50.0%</td>
<td>5.5%</td>
<td>TO, TP, TSP</td>
</tr>
<tr>
<td>5</td>
<td>ENTITY C</td>
<td>24</td>
<td>88</td>
<td>59</td>
<td>29</td>
<td>67.0%</td>
<td>13.8%</td>
<td>BA, RC, TOP, TP, TSP (more)</td>
</tr>
<tr>
<td>6</td>
<td>ENTITY D</td>
<td>42</td>
<td>146</td>
<td>69</td>
<td>77</td>
<td>47.3%</td>
<td>15.6%</td>
<td>BA, RC, TOP, TP, TSP (more)</td>
</tr>
<tr>
<td>7</td>
<td>ENTITY E</td>
<td>15</td>
<td>46</td>
<td>35</td>
<td>11</td>
<td>76.1%</td>
<td>16.8%</td>
<td>GO, GOP, TO</td>
</tr>
<tr>
<td>8</td>
<td>ENTITY F</td>
<td>6</td>
<td>11</td>
<td>9</td>
<td>2</td>
<td>81.8%</td>
<td>5.7%</td>
<td>TOP</td>
</tr>
<tr>
<td>9</td>
<td>ENTITY G</td>
<td>18</td>
<td>39</td>
<td>14</td>
<td>25</td>
<td>35.9%</td>
<td>4.1%</td>
<td>DP, TO, TOP, TP, TSP</td>
</tr>
<tr>
<td>10</td>
<td>ENTITY H</td>
<td>9</td>
<td>19</td>
<td>6</td>
<td>13</td>
<td>31.6%</td>
<td>1.3%</td>
<td>DP, GO, GOP, TO, TOP</td>
</tr>
<tr>
<td>11</td>
<td>ENTITY I</td>
<td>15</td>
<td>75</td>
<td>58</td>
<td>17</td>
<td>77.3%</td>
<td>15.7%</td>
<td>TO, TOP, TP, TSP</td>
</tr>
<tr>
<td>12</td>
<td>ENTITY K</td>
<td>24</td>
<td>96</td>
<td>56</td>
<td>40</td>
<td>58.3%</td>
<td>10.8%</td>
<td>BA, GO, GOP, TO, TOP, TP, TSP (more)</td>
</tr>
<tr>
<td>13</td>
<td>TOTALS</td>
<td>185</td>
<td>603</td>
<td>351</td>
<td>252</td>
<td>58.1%</td>
<td>9.9%</td>
<td></td>
</tr>
</tbody>
</table>

5/11/2016
ICE Objectives

• Primary objective:
  – Recognize internal controls utilized by the Entity to manage and mitigate reliability risks.

• Other objectives of the ICE review:
  – Leverage ERO Enterprise Inherent Risk Assessment Framework;
  – Align Regional Entity & registered entity compliance resources with BES reliability risk-focus areas;
  – Identify and assess entity’s risk mitigation and internal controls design;
  – Obtain reasonable assurance that the entity internal controls and internal control designs are in place and operating effectively
  – Develop Entity Compliance Oversight Plan including Compliance monitoring methods, scope & frequency.
Benefits of ICE

Expected benefits derived from ICE review participation typically include the following:

– Attainment of BES reliability, Corporate Goals and Objectives;
– Alignment of staff performance to Key Performance Indicators;
– Improved operational performance (i.e., exceeding standards and requirements);
– Enhanced entity communication and interaction across organizational business functions;
– Targeted BES reliability risk-focused scoping;
– Reduction in audit duration;
– Improved risk and control awareness;

• Internal Control Design evaluation including:
  – Functional and Business Process Assessment;
  – Risk Identification, Mitigation & Remediation;
  – Design and Gap Analysis
  – Non-binding Recommendations for Internal Control Design Enhancement.

• ICE Training and Outreach.
Methodology

- ICE review process to assess Entity ICD’s and related risk mitigation
- Developed multiple worksheet types to facilitate Entity preferences and review flexibility
  - Type 1 ICE Worksheet:
    - Depicts internal controls on a requirement-by-requirement basis.
  - Type 3 ICE Worksheet:
    - Depicts internal controls based upon Functional Businesses and/or Control Processes.
    - Covers multitude of standards and requirements.
    - Aligns with organizational business functions and processes.
    - NPCC’s preferred approach
    - See Appendix for examples
- Pre-ICE WebEx for every ICE participant
- Frequent communication encouraged
Lessons Learned

All key Internal Controls have not been identified and documented.

– Automation tools often overlooked, taken for granted (hence not taking credit for them)
  • Work management systems
  • Document management tools
  • Compliance management tools
  • Inventory/Maintenance/Vegetation Management tools
  • Checklists, logs
– Tribal knowledge ("oh everybody knows that. I didn’t think I had to list it")
– Existing processes (documented or undocumented) are not identified in ICE and therefore not credited.
Lessons Learned

Flowcharts really really help. Really!

– Flowcharts are recognized as a best practice
– Facilitates comprehensive gap analysis of internal controls design
– Functional Responsibilities/Departments
  • inputs/outputs/handoffs/feedback loops.
  • two way “traffic” documentation (e.g. emails, meeting agendas/notes/lessons learned, regular meetings, logs
  • Identify “control silo” components
  • “map” to the ICE worksheets
NPCC Control Design Assessment and Comments

Annual Blackstart Restoration Plan

- Distribution Loads → UFLS stages → Update Blackstart Restoration Plan → Prepare Blackstart Training Package → Present Mandatory training to Operators → Review training evaluation forms
- Update in Blackstart Restoration plan and Training
- Email to RC
- Update
- Approval
- Print and place in ECC
- Print and place at BCC
- Beginning of the next year (Q1)

Please indicate/annotate Procedure No./Name if applicable. If procedure no. or names are too long, create short abbreviations and provide the legends for these. Briefly describe what each procedure does on a separate page if needed.

Please indicate/annotate Who, What, When, Where, and How associated with the Internal Control Design as applicable. Use another page to describe if necessary.

Indicate tools used. Is this tool Automatic, Manual, or Hybrid? Briefly describe in detail each tool on a separate page as needed.

Does this process and here or is in an input to another process/control within your organization?

This looks like it’s a Key Control. What if the email is not sent to the RC? If this is a Key Control, please so indicate. How do you ensure this Key Control doesn’t fail and cause the part of whole Internal Control Design to fail?
Lessons Learned

Submittals not always quality checked prior to submittal to NPCC ICE Team

- Mapping of flow diagrams to ICE worksheets
- Additional undocumented controls (discovered during ICE evaluation walkthrough)

- Conduct a peer check of your SME’s flow diagram.
- Conduct Independent check of flow diagram to ICE worksheet
- Crosscheck the “who, what, when, where, why, how” an Internal Control is implemented
- Identify and verify all feedback loops, inter-departmental inputs, outputs and handoffs
- Perform a mock walkthrough of ICE before NPCC ICE team review
- If you’ve been “ICE’d” before, use that experience for future ICE.
Lessons Learned

Audit evidence is not the same as Internal Controls evidence. SMEs need to understand the difference.

– Requirements ask for processes, procedures or programs, proof of actions, studies, calculations, communications, logs, test results to demonstrate compliance. (Maintenance, Testing, Restoration, Training, Operations, Misops, etc.)

– “Aren’t the above my internal control design? Isn’t the ICE evidence the same as the audit evidence?”

– Internal Control Silos
– Key Internal control?
  – Postulate failure mechanisms
  – Redundancy to avoid single points of failure
Audit

• Audit interested in pass/fail, No Finding or Possible Violation
• Once pass/fail, NF/PV is determined, there may be additional items provided to improve reliability (e.g. Areas of Concern, Recommendations, Suggestions)
• Backward looking (Audit Period)
“Please move along once you have received your inspection sticker”
Internal Controls Evaluation

• Preventative controls in place to
  – pass audits
  – exceed the requirements to improve reliability

• Detective controls to indicate degradation in reliability or identify drift from compliance

• Corrective controls confirm and mitigate non-compliances

• Real time and forward looking
ICE vs Audit (continued)

Audits

- RSAW are used for Audits
  - focused on evidence showing compliance
  - Some ask for brief narrative describing how the requirement was met.
  - Narrative does not delve into Internal Controls Design.
  - No credit given for exceeding the requirements to improve reliability

ICE

- ICE Worksheets used for ICE
  - Many columns requesting entity to describe many aspects of each component of the Internal Control Design
  - Asks questions to determine who, what, when, where, why, how the internal control was implemented to ensure compliance.
  - Acknowledges systematic approaches/designs to ensure/exceed reliability
Internal Control Types

- Internal Controls - Preventative [P], Detective [D] & Corrective [C]
- Institute of Internal Auditors (IIA) – recognizes Corrective controls as Good, Detective controls as Better, and Preventative controls as Best
- IIA - suggests Preventative controls be bolstered with Detective and Corrective controls – to ensure Preventative control implementation and proper functioning
Types of Controls pertaining to Kitchen Fires

Corrective Controls = Good
Types of Controls - Kitchen Fires

Detective Controls = Better

Fire Sensor
Smoke Detector Alarm

Protect life and property
Types of Controls - Kitchen Fires

Preventative Controls = Best

(Procedures, signage, training, monitoring/situational awareness, access)
“Where there’s a will, there’s a way…”
(to get around preventative controls)

Pizza-thieving Connecticut dog starts stove-top kitchen fire
"Where there’s a will, there’s a way"

"As my husband and I were entertaining guests in the other room, one of our dogs decided to break into the pizza box that was sitting on top of our gas stove. Her paw turned the gas ignition knobs as she tried to put her head further into the box. Luckily we had it on video and know who to blame! Lol let this serve as a gentle reminder not to place items on your stove top and also to carefully choose the placement of your fire detectors," the uploader wrote."
“How a NYC Traffic Cop helped me improve my Internal Control Design”
Audit evidence is not the same as Internal Controls evidence – Requirement says there must be a process, procedure or program in place for compliance. (Maintenance, Testing, Restoration, Training, Operations, etc.)

– “Isn’t the above my internal control design? The compliance evidence is the same as ICE evidence isn’t it?”

Internal Control Silos – “Who, What, When, Where, Why, How” test – Key Internal control? (Failure mechanisms) – (Protection systems have redundancy, Backup Control Centers – Single point of failure for each silo (SHC uses training to the procedure to do the right thing)

Integrated Controls Design

Control Room, Engineering, Compliance, Protection & Control, Change Mgmt., Emergency Ops., etc.

Process Function / Workflow:

Policies & Procedures:

Skilled Human Capital:

SME’s
Experience Level
Training Program
Certification
Power Systems
Operations
Engineering
Maintenance/Testing

P&P’s

SAT

SHC

Systems & Automated Tools:

EMS / SCADA
Training
Change Mgmt.
Procurement
Capital Projects
Compliance / Regulatory
Maintenance/Testing

Standards & Requirements:

Control Objectives
Risk Mitigation
Appendix

• References and additional examples (more can be found in prior presentations and on the NPCC ERA website)
Analytical Tools

Type 1 Worksheet

- Navy Section from NERC Standard – filled by NPCC

- Lavender Section – filled by Entity
  – Explanation of Headings provided on separate tab
### Analytical Tools (Cont’d)

Type 3 Worksheet
- Lavender Section – filled by Entity
  - Explanation of Headings provided on separate tab

<table>
<thead>
<tr>
<th>Entity’s Functional Business/Control Process</th>
<th>Standards and Requirements Entity’s Functional Business/Control Process Relate To</th>
<th>Internal Control Objective</th>
<th>Entity IC Design &amp; IC’s</th>
<th>Key IC Indicator</th>
<th>Key IC Rationale / Description (Basis)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>IC Type [P/D/C Preventative, Detective, Corrective]</th>
<th>IC’s / IC Design Mode (A=Auto, M=Manual, H=Hybrid)</th>
<th>Discrete IC Risk Mitigation</th>
<th>Entity Evidence Submission and Policies/Procedures Cross Reference</th>
<th>Entity 3rd Party Assessment - Vendor Name (if applicable)</th>
</tr>
</thead>
</table>
Analytical Tools (Cont’d)

Power Blue Section - NPCC completes after assessment of Internal Controls Design and supporting documents

<table>
<thead>
<tr>
<th>Control Activities</th>
<th>IC’s Implementation Level (FI, LI, PI, NI, M)</th>
<th>NPCC Assessment of IC’s / IC Design</th>
<th>NPCC Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support Evidence - Information Assessment (Credibility &amp; Sufficiency)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Remove from Audit Scope (Post ICE)? (Y/N)</th>
<th>Alternate Monitoring Method Post ICE (Spot Check [SC] Guided Self-Cert [GSC], etc.)</th>
<th>Frequency of Alternate Monitoring Method</th>
<th>Review (Onsite, Offsite, or Both)</th>
</tr>
</thead>
</table>

5/11/2016
Type 1 - ICE Example (Cont’d)

- NPCC Assessment:

<table>
<thead>
<tr>
<th>Control Activities Supporting Evidence Information Assessment (Credibility &amp; Sufficiency)</th>
<th>IC’s Implementation Level (FI, LI, PI, NI, M)</th>
<th>NPCC Assessment of IC’s / IC Design</th>
<th>NPCC Recommendations</th>
<th>Remove from Audit Scope (Post ICE)? (Y/N)</th>
<th>Alternate Monitoring Method Post ICE (Spot Check [SC] Guided Self-Cert [GSC], etc.)</th>
<th>Frequency of Alternate Monitoring Method</th>
<th>Review (Onsite, Offsite, or Both)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documents O-TRA-01-007-R05 OP 7 ECC Event Notification and Reporting covers all the pieces of the requirement</td>
<td>LI</td>
<td>Show the role of ISO in oversight. Timeline of process needs to be identified. Identify Management oversight role</td>
<td>Y</td>
<td>GSC</td>
<td>3 to 6 years</td>
<td>Offsite</td>
<td></td>
</tr>
</tbody>
</table>

5/11/2016
NPCC ERA website

• More references and examples

<table>
<thead>
<tr>
<th>ENTITY RISK ASSESSMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>TYPE</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
QUESTIONS?
Thank You