• NERC Antitrust Guidelines
  ▪ It is NERC’s policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

• Notice of Open Meeting
  ▪ Participants are reminded that this webinar is public. The access number was widely distributed. Speakers on the call should keep in mind that the listening audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.
• Agenda Breaks
• Emergency exits
• Ask questions anytime
• Ground rules
• Parking lot
• Feedback Survey
Opening Remarks & RAI Overview
Introduction on Compliance and Enforcement Activities

Lane Lanford, President & CEO, Texas RE
RAI Overview - Introduction on Compliance Activities

- Registered Entity Functions
- ERO & Regional Characteristics
- Events
- RISC

Risk Elements

Inherent Risk Assessment

Internal Controls Evaluation

Oversight Tool Selection

Scope and Focus for Entities not participating in ICE
Questions and Answers
CMEP Implementation Plan and Risk Elements

Adina Mineo, Compliance Assurance Manager, NERC
• Guide posted in September 2014 describes annual process for identification and prioritization of enterprise-wide risks
  - Potential impact to the reliability of the bulk power system (BPS)
• Risk Elements map to Reliability Standards
  - Replace prior actively monitored lists
  - Regional Entities also consider region-specific risks
• Annual operating plan for ERO Enterprise CMEP activities
  ▪ Posted in September 2014
  ▪ Regional Entity appendices in development; to be posted in early November
  ▪ May be updated as needed throughout the implementation year

• Risk Elements map to Reliability Standards
  ▪ Not “AML” and not a baseline for audit scope

• Preliminary Oversight Plan
  ▪ Scheduled audits include 3-year cycle

• 2015 ERO CMEP Implementation Plan can be found here:
Questions and Answers
Inherent Risk Assessment Process and Application

Tom Tierney, Director of Compliance, MRO
Framework

- Registered Entity Functions
- ERO & Regional Characteristics
- Events
- RISC

Risk Elements

Inherent Risk Assessment

Internal Controls Evaluation

Oversight Tool Selection

Entity Compliance Oversight Plan
Figure 2. IRA Module Flow Chart

Information Gathering
- Gather Risk Elements Module Output
- Determine Entity Specific Information Needs to Perform IRA
- Develop Targeted Information Request List

Assessment
- Risk Factor and Standards and Requirements Applicability Review
- Risk Factor Analysis
- Review of IRA Conclusions

Results
- Results Documentation
- Draft Compliance Oversight Plan for Registered Entity
• Scalability and impact on varying size entities
• Implementation in 2015
• Entity expectations during the Inherent Risk Assessment (IRA) process
• IRA outputs and impact on compliance oversight plan (including no ICE election)
• IRA updates
• For 2015, Regional Entities will perform IRAs for most scheduled audits. Regional Entities may perform IRAs for other registered entities as determined necessary
• NERC and the Regional Entities will continue to identify tools and templates to promote consistency in IRA implementation
• NERC and the Regional Entities will provide outreach and training to industry and Regional staff
IRA Example – Operations & Planning

- IRAs conducted for three wind farms with similar registrations (GO/GOP)
  - 131 applicable Requirements
  - 28 Requirements on 2014 AML
- Inherent risk assessment captured unique aspects of each and allowed for tailored monitoring scope
- Wind Farm #1
  - “Vanilla” example
  - 20 requirements in scope for audit (only 5 on AML)
- Wind Farm #2
  - Also responsible for interconnection of nuclear facility
  - 25 requirements in scope for audit (only 5 on AML)
- Wind Farm #3
  - Doesn’t own collector bus
  - Two requirements in scope (neither on AML)
  - Guided Self-Certifications instead of Compliance Audit
• IRAs conducted for three entities subject to CIP V3 Standards
• Inherent risk assessment captured unique aspects of each and allowed for tailored monitoring scope
• Entity #1
  ▪ TOP’s transmission substations not V3 Critical Assets, but will be V5 High/Medium assets
  ▪ Data gathered from entity reflected heavy use of virtualization for networking & servers
  ▪ Oversight plan emphasized current RBAM’s treatment of substations and focused on treatment of virtualized assets under CIP-005-3 and CIP-007-3
• Entity #2
  ▪ Vertically-integrated entity has several V3 Critical Assets, but control centers will be its only V5 High/Medium assets
  ▪ Data gathered from entity indicated use of DNP over TCP/IP from EMS to substations
  ▪ Oversight plan emphasized control centers, as well as CIP-005-3 due to routable connections
• Entity #3
  ▪ GO/GOP with no V3 CCAs declared, and no V5 High/Medium assets based on known information
  ▪ CIP Standards removed from monitoring scope
Questions and Answers
Internal Control Evaluation
Process and Application

Keshav Sarin, Manager Compliance Risk Analysis, WECC
Tom Tierney, Director of Compliance, MRO
Internal Control Evaluation Process

- **Scope of ICE** is a collaborative effort between Region and Entity
- **Entity** determines final ICE scope

- **Entity creates nothing new**
- **Examples:** management practices, policies, procedures, systems, tools, people, etc.

- **Region evaluates what Entity already does in the way that Entity already does it**

- **Feedback includes maturity levels**
- **ICE report can help identify areas for improvement in controls that could increase reliability and mitigate risks**
ICE Basics

• Scalability and impact on varying size entities
• Timing of Internal Control Evaluation (ICE)
• Implementation in 2015
• Entity expectations during the ICE process
   Flexible, scalable, focus on existing management practices, business decision to participate
• ICE outputs and impact on compliance oversight plan
   ICE can only further limit or have no impact upon audit scope/frequency
   ICE can provide roadmap to controls improvements
   ICE cannot increase audit scope/frequency (defaults to scope via IRA)
   ICE cannot result in a Possible Violation
• Impact on CIP Version 5 transition
   ICE will help Regions better understand how entity manages or mitigates risks to further tailor monitoring activities
• Evaluate internal controls related to the risks from the IRA outcomes
• Documentation for steps and ICE conclusions
• ICE results shared with the registered entity
• A deficient internal control does not necessarily indicate possible noncompliance with a Reliability Standard or Requirement
• ICE may inform CEAs on selection of appropriate CMEP tools and scope focus
ICE Next Steps

- NERC and the Regional Entities will continue to identify tools and templates to promote consistency in ICE implementation
- NERC and the Regional Entities will provide outreach and training to industry and Regional staff
• Internal controls related to COM-002
  ▪ Preventive control involves random review of operator communications, followed by feedback and corrective actions
  ▪ Registered Entity uses three-part communication for routine communications
  ▪ Detective control involves complete review of any situation in which a directive may be issued

• Conclusion was that registered entity will identify and address issues timely

• Based on results of internal control testing, Standard was not tested directly
• Internal controls related to PRC family of Standards
  - Preventive control involves use of work order management system to track testing activities and alert on upcoming or missing tests
  - Detective control involves random monthly management review of 10% of maintenance and testing records
• Conclusion was that registered entity will meet all requirements related to maintenance and testing intervals
  - Criteria for management review not clearly documented
• Resulted in reduced sampling for related Standards
  - While intervals will likely be met, not sure whether management review is consistent with Region’s application of standards
• Entity has internal control for “maintenance”

• Maintenance internal control covers multiple NERC Reliability Standards
  - PRC-005
  - PRC-008
  - PRC-011
  - FAC-003
  - EOP-005
  - CIP-003 R6
  - CIP-006 R8

• Regional Entity tests design and effectiveness of one internal control to gain reasonable assurance of compliance with seven NERC Reliability Standards
• Professional auditing standards allow Regional staff to rely on the work of others (independent organization)

• Regional staff may rely on work related to testing of internal controls or testing of compliance with Standards and Requirements
  ▪ Oversight scaled by utilizing the work of others

• Entity conducts independent evaluations of individual standards/requirements (entity-level control – governance)

• Conclusion: Entity effectively implements and independently tests NERC reliability standards/requirements

• Based on results of internal control testing and independent testing, audit significantly scaled
  ▪ 34 potential requirements in AML for the audit
  ▪ 15 requirements - use work of independent auditor
  ▪ Four requirements- review work of independent auditor to confirm adequacy of work
• Considerations
  - Levels of risk and depth needed to obtain reasonable assurance for each area of focus
  - Monitoring methods to be employed and which standards/requirements are in scope for each
  - Timing of compliance monitoring activities
  - Available resources
• Reflect how ICE impacts monitoring activity from example
• Compliance monitoring activities may become more frequent, but less intrusive
  ▪ Shift from large, infrequent audits to “continuous” monitoring
• Focused scope for monitoring places emphasis on areas that present highest risk to reliability of the BES
• Regions to make better use of all the tools provided by the CMEP, not just audits
<table>
<thead>
<tr>
<th>Milestone</th>
<th>Estimated Timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk elements Identified (ERO and Regional)</td>
<td>Oct &amp; Nov of Previous year</td>
</tr>
<tr>
<td>IRA Complete</td>
<td>120-180 days before start of audit</td>
</tr>
<tr>
<td>CIP v5 RFI Due</td>
<td>135 days before start of audit</td>
</tr>
<tr>
<td>ICE Complete</td>
<td>90-150 days before start of audit</td>
</tr>
<tr>
<td>Audit Scoping</td>
<td>90 days before start of audit**</td>
</tr>
<tr>
<td>Audit starts</td>
<td></td>
</tr>
</tbody>
</table>

*Timing is estimated and may fluctuate among Regional Entities.  
**CMEP Section 3.1.1
Questions and Answers
IRA & ICE Industry Panel Discussion

Moderator:  
Keshav Sarin, Manager Compliance Risk Analysis, WECC

Participants:  
Doug Johnson, Manager of Operational Compliance, American Transmission Company LLC  
Greg Froehling, NERC Compliance Officer, Rayburn Country Electric Cooperative  
Dick Garlish, Director of Regulatory Compliance & Senior Counsel, Idaho Power Company
Rayburn Country Electric Cooperative (RCEC) Example

Risk-based Compliance Oversight Framework (Framework)

- Registered Entity Functions
- ERO & Regional Characteristics
- Events
- RISC

Risk Elements

Initial Scope

IRA

Scope

ICE

Focus

CMEP Tools

Scope and Focus for Entities not participating in ICE

Inherent Risk Assessment

Internal Controls Evaluation

Oversight Tool Selection

Entity Compliance Oversight Plan
Step 1 - RCEC Example

1. General Information (13 Questions)
2. Risk based questionnaire.

RCEC known profile:
- DP/LSE
- 5 Member Cooperatives
- 700MW 2013 Peak Load
- All radial connections
- No BES assets
3. Focused RSAW responses.
4. Round 1 Risk Based questions.
Step 3 - RCEC Example

5. Round 2 Risk Based questions.
6. Round 3 Internal Controls questions.

Internal Controls Evaluation

The RCEC experience
7. Offsite Audit call / review.
8. Future Monitoring methods decision.
Final Outcome

Entity Compliance Oversight Plan
Unique to entity determined by risk.
Self-logging and Compliance Exceptions Program Concepts

Chris Luras, Director of Compliance Risk Analysis & Enforcement, WECC

Teresina Stasko, Senior Counsel & Manager of Enforcement Actions, NERC
What is a compliance exception?
- Noncompliance that is not pursued through the enforcement process described in CMEP § 5.0

Who is eligible for a compliance exception?
- Implemented on a limited basis in 2014
- Available to all registered entities in 2015

What can be treated as a compliance exception?
- Minimal risk noncompliance
- Any discovery method
- Mitigated within 12 months of compliance exception notification

Who determines compliance exceptions?
- Regional Entity staff
  - Usually Risk and Mitigation or Enforcement teams

When are compliance exceptions determined?
- After review by applicable Regional Entity staff
- 60 day triage goal
• Accumulation of compliance exceptions may inform the ERO enterprise of increased risk
  ▪ For the registered entity
  ▪ For the continent or a specific region

• Compliance exceptions are not part of an entity's violation history for penalty purposes

• Regional Entity decides how to treat a recurrence of compliance exceptions
• Compliance exception program is not meant to eliminate or reduce oversight or visibility
• All noncompliance is tracked and recorded
• Compliance exceptions are shared with NERC and FERC on a monthly basis through non-public means
Benefits of Compliance Exceptions

- Matches risk with regulatory burden through expanded discretion
- Improves resource allocation
- Promotes differentiation of risk
- Encourages self-identification of noncompliance by registered entity
Status of Compliance Exceptions

- Through September 30, 2014, Regional Entities have treated 54 minimal risk issues as compliance exceptions.
- All Regional Entities will implement compliance exception process in 2015.
Scenario:

An entity discovers that an employee failed to complete CIP cyber security training annually.
• Examples of Factors Supporting **Compliance Exception:**
  - Employee was on leave and did not receive automated reminder emails
  - Entity self-identified issue through regular training log reviews
  - Limited number of employees completing training late
  - Unforeseeable technical issue with email reminder messages
  - Issue with employee was addressed promptly
  - Employee completed CIP training in previous years
  - Employees are generally aware of CIP obligations
• Examples of Factors Supporting Enforcement:
  ▪ No effective control, practice, or system in place to ensure training is completed in a timely manner
  ▪ Employees generally not aware of CIP obligations
  ▪ Multiple employees completing training late (or not at all)
  ▪ Entity did not discover issue promptly
  ▪ Entity did not mitigate issue promptly
  ▪ Underlying cause was foreseeable and could easily happen again
Scenario:

Entity staff discovers that, after a group of five visitors leaves its facility, the security guard only noted four of the visitors in the visitor log.
• Examples of Factors Supporting **Compliance Exception:**
  - Issue was promptly discovered
  - Logs are regularly reviewed according to a process or procedure
  - Other protections were in place at the time of the issue:
    - Video monitoring
    - Continuous escort with authorized staff
    - Visitor access proximate card were used
  - Issue promptly mitigated:
    - Technical or procedural error resolved and backup solution implemented
    - Second security guard added at entrance to assist at busy times
Examples of Factors Supporting Enforcement:

- Security guard at entrance is regularly overwhelmed with visitors and badged employees – and no guard is added to assist
- Missing visitors/logs not discovered promptly (or at all)
- Issue not mitigated promptly or properly
- Escort has frequent visitors and is responsible for ensuring all visitors were logged and failed to do so
- Other protections were not in place or failed:
  - Continuous escort not maintained
  - Access controls or video monitoring not present or non-operational
**Examples of Factors Supporting Enforcement:**

- Security guard at entrance is regularly overwhelmed with visitors and badged employees – and no guard is added to assist
- Missing visitors/logs not discovered promptly (or at all)
- Issue not mitigated promptly or properly
- Escort has frequent visitors and is responsible for ensuring all visitors were logged and failed to do so
- Other protections were not in place or failed:
  - Continuous escort not maintained
  - Access controls or video monitoring not present or non-operational
Self-logging Program

- Two avenues to achieve compliance exception treatment:
  - Case-by-case
  - Self-logging

- Self-Logging
  - Formerly known as aggregation of self-reports
  - Registered entity logs minimal risk noncompliance
    - Log contains detailed description of issue, risk assessment, and mitigation (more detail than self-report)
    - Submitted to Regional Entity for review and approval every three months
    - Once approved, noncompliance on log processed as compliance exception
Self-Logging Program

- Only applies to minimal risk issues
- Replaces individual Self-Reports
- Does not affect audit scope
  - Treated the same as OEAs
  - Noted as logged issues
  - Reviewed by auditors in advance of the audit
Basis for Entry into Self-logging Program

- Compliance history and level of cooperation in prior compliance and enforcement matters
- History of self-assessment, self-reporting, and timely and thorough mitigation
- Quality, comprehensiveness, and execution of internal compliance program
- May be informed by results of IRA and ICE
Review of Logged Noncompliance

- Occurs every three months
- Reviewed by Regional Entity Staff
  - Is noncompliance sufficiently described?
  - Is minimal risk determination justified and reasonable?
  - Is mitigation appropriate/adequate?
- Regional Entity gives feedback to registered entity
Once Region Approves Log

- Logged items are tracked by Regional Entity
- Logged items are sent to NERC as compliance exceptions
- NERC submits items to FERC
  - No public posting
Benefits of Self-logging Program

- Presumed compliance exception
- Efficiency gains
- Facilitates trend-spotting by Regional Entities and NERC
Currently, there are 14 registered entities participating in the Self-Logging Program.

Participants include Multi-Region registered entities.

Regional Entities are currently considering additional registered entities for participation.

Regional Entities will continue to consider additional opportunities for Self-Logging.
Scenario:

Entity identifies possible noncompliance

Entity conducts risk/harm assessment → identifies issue as posing a **minimal risk** to reliability
Self-logging Participant

- Entity logs noncompliance in tracking spreadsheet
- Send spreadsheet to Region

Triage Process

Outcomes:
- Compliance exception
- More information needed
- Enforce

Compliance Exception

- Minimal risk confirmed
- Presumption of compliance exception
- Processed as compliance exception
Self-Logging Process Example

**Entity Not Participating in Self-logging**

- Entity self-reports noncompliance to Regional Entity

**Triage Process**

**Outcomes:**
- Compliance exception
- More information needed
- Enforce

**Compliance Exception**

- Minimal risk confirmed
- Self-identified issue
- Eligible for compliance exception treatment
Questions and Answers
Self-logging and Compliance Exception Industry Panel Discussion

Moderator:
Chris Luras, Director of Compliance Risk Analysis & Enforcement, WECC

Participants:
Randy Crissman, Vice President-Technical Compliance, New York Power Authority
Doug Johnson, Manager of Operational Compliance, ATC
Rick Terrill, Director Regulatory & Market Support, Luminant Power
CCC Involvement in the ERO’s Implementation of Risk-based CMEP Activities

Patti Metro, Manager, Transmission & Reliability Standards, NRECA and CCC Chair
Background and Role of CCC

- NERC’s Compliance and Certification Committee (CCC) is an independent body reporting to the NERC Board of Trustees (Board)
- Work with NERC staff on Compliance, Registration, and Certification Programs
- Provide comments and recommendations from stakeholders to NERC Board and NERC staff
- CCC roles include:
  - Establish and implement programs to monitor NERC’s compliance
  - Serve as a hearing body
  - Serve as a mediator
  - Monitor Compliance Administration
  - Monitor organization registration and certification
- Board assignments as directed
- Membership filled by sector and industry personnel
Subcommittees of CCC

• CCC has three subcommittees
  ▪ ERO Monitoring Subcommittee (EROMS)
  ▪ Organization Registration and Certification Subcommittee (ORCS)
  ▪ Compliance Processes and Procedures Subcommittee (CPPS)

NOTE: Non CCC members can participate in the subcommittees of the CCC.
CCC has a subcommittee specifically focused on RAI and Risk-based Compliance Monitoring Activities. For 2015, the Subcommittee has two main projects:

- Support the Risk-based Compliance Monitoring and Enforcement Program
- Update criteria for the ERO to assess the effectiveness of Regional Entity CMEP Programs
  - Develop criteria that appropriately reflects expected program improvements resulting from RAI and the transition in 2015

Subcommittee is completely open to observers and happy to receive input from and work with any Stakeholder, Regional Entity representative, or ERO Personnel
• Subcommittee has discussed range of topics around CMEP administration that may change with risk-based compliance monitoring. For example:
  ▪ Whitepaper proposing changes to NERC standard Data Retention Requirements
    o Promote consistency
    o Recordkeeping requirements commensurate with reliability risks
  ▪ RAI Design Principles: Advise on Program Modules and develop Frequently Asked Questions Document
  ▪ NERC Standards Audit Report Conclusions/Structure
    o Ways to reinforce the objective of achieving reasonable assurance of compliance
• CCC Executive Committee
  - Patti Metro, National Rural Electric Cooperative Association – Chair [Tx Dependent Utility]
  - Jennifer Flandermeyer, Kansas City Power & Light – Vice Chair [RE-SPPRE]
  - Matthew Goldberg, ISO-NE – CPPS Chair [ISO/RTO]
  - Martin Huang, British Columbia Hydro – Nominating Subcommittee Chair [Federal/Provincial]
  - Keith Comeaux, NRG Energy – ORCS Chair [Electricity Marketer]
  - Ted Hobson, JEA – EROMS Chair [RE-FRCC]
  - Charlie Berardesco – NERC Management Sponsor
  - Steve Noess – NERC Management Sponsor
  - Adina Mineo – Secretary, NERC Staff

• CCC CPPS Subcommittee Members
  - Matthew Goldberg, ISO-NE [ISO/RTO]
  - Jim Stanton, Quanta Technology [Sm End Use Customer]
  - Helen Nalley, Southern Company [IOU]
  - Silvia Prada-Mitchell, Florida Power & Light [Merchant Electricity]
  - Jason Marshall, ACES Power Marketing
  - Martin Huang, British Columbia Hydro [Federal/Provincial]
  - Rick Terrill, Luminant Mining Company [Lg End Use Customer]
  - Martyn Turner, Lower Colorado River Authority [State/Municipal]
• CCC information (agenda, minutes, details) can be found at the following:  http://www.nerc.com/comm/CCC/Pages/default.aspx

• Full 2014 Roster

• CCC work products can be found on NERC’s RAI Tab:
Questions and Answers
Path Forward and Success in Implementation of Risk-based Approach to CMEP

Steven Noess, Director of Compliance Assurance, NERC
Path Forward and Implementation

- Transformation and shift to the risk-based approach to CMEP activities and the end-state of RAI
- Training for NERC and Regional Entity Staff
  - Phased approach during remainder of 2015 and Q1, 2015
- Outreach
  - Continued outreach through workshops and webinars
  - Q1, 2015 hold outreach and education on lessons learned from implementations
  - NERC oversight - Compliance & Enforcement
  - Activities in Q1, 2015: Review conceptual consistency in the application of the ERO Enterprise's risk-based approach to CMEP
  - Observe use of risk-based enforcement tools by measuring utilization on a Region-by-Region basis
• NEW RAI website

• Guidance documents on ERO Enterprise’s Risk-based CMEP

• Informational Filing on Implementation of RAI with FERC,
  http://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/FinalFiled_RAI_Informational_Filing_20141103.pdf

• Weekly Standards and Compliance Bulletin
Questions and Answers