NERC – Power System Risks and New Cyber Security Regulations

vermont electric power company

VELCO

Chris Root, COO
Vermont System Planning Committee
Middlebury College
April 24, 2019

Topics

1. NERC's 9 risks to the bulk system
2. Overall Critical Infrastructure Protection (CIP) Standards
3. New Supply Chain Cyber Rules (CIP13)

NERC Risk Profiles

High: Emerging risks that are not generally understood by industry, regulators and policy makers. The reliability risks are known to exist, but more recently identified and the extent of the risk and impacts not clearly understood. More analysis and experience are required to further define the risks and to develop mitigation actions.

1. **Cybersecurity Vulnerabilities**
2. **Changing Resource Mix**
3. **BPS Planning**
4. **Resource Adequacy and Performance**

Moderate: Evolving risks with impacts that are somewhat understood by industry, regulators and policy makers. The reliability risks have been identified but have attributes that are different from risks dealt with by the industry in the past. New or additional mitigating actions or methods need to be developed and implemented.

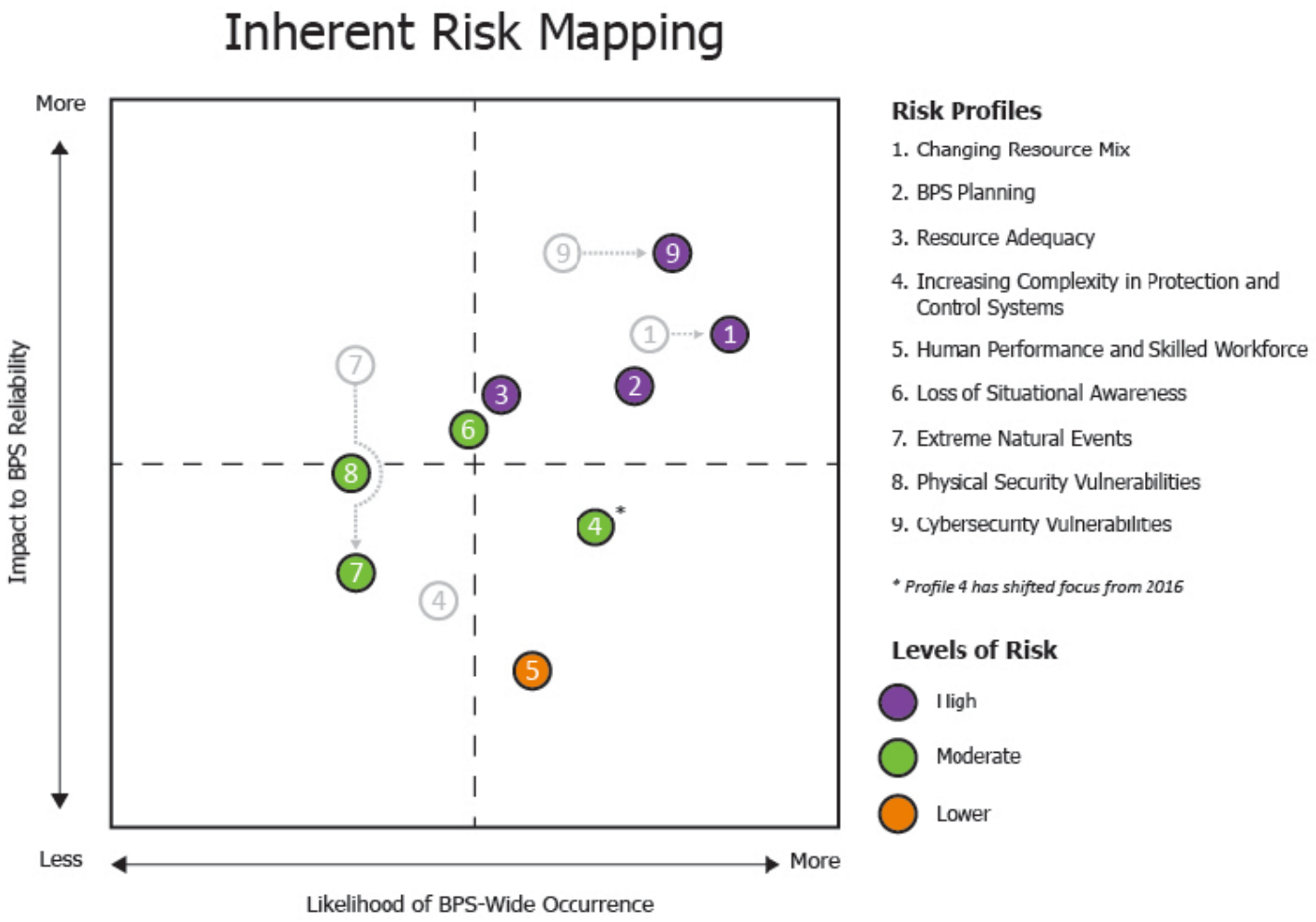
5. **Increasingly Complex Protection/Control Systems**
6. **Loss of Situational Awareness**
7. **Extreme Natural Events**
8. **Physical Security Vulnerabilities**

Low risks do not mean that possible reliability impact is small, but rather the profiles are known or existing risks that are universally understood and have been accepted by regulators and policy makers. The reliability risks have been identified, analyzed and should continue to be mitigated by known methods and approaches. The risks are predictable, well defined, and at least similar to reliability issues that have been dealt with by the industry in the past.

9. **Human Performance and Skilled Workforce**

Source: NERC ERO Reliability Risk Priorities – RISC Recommendations to the NERC Board of Trustees - October 2017

Prioritization of Reliability Risks

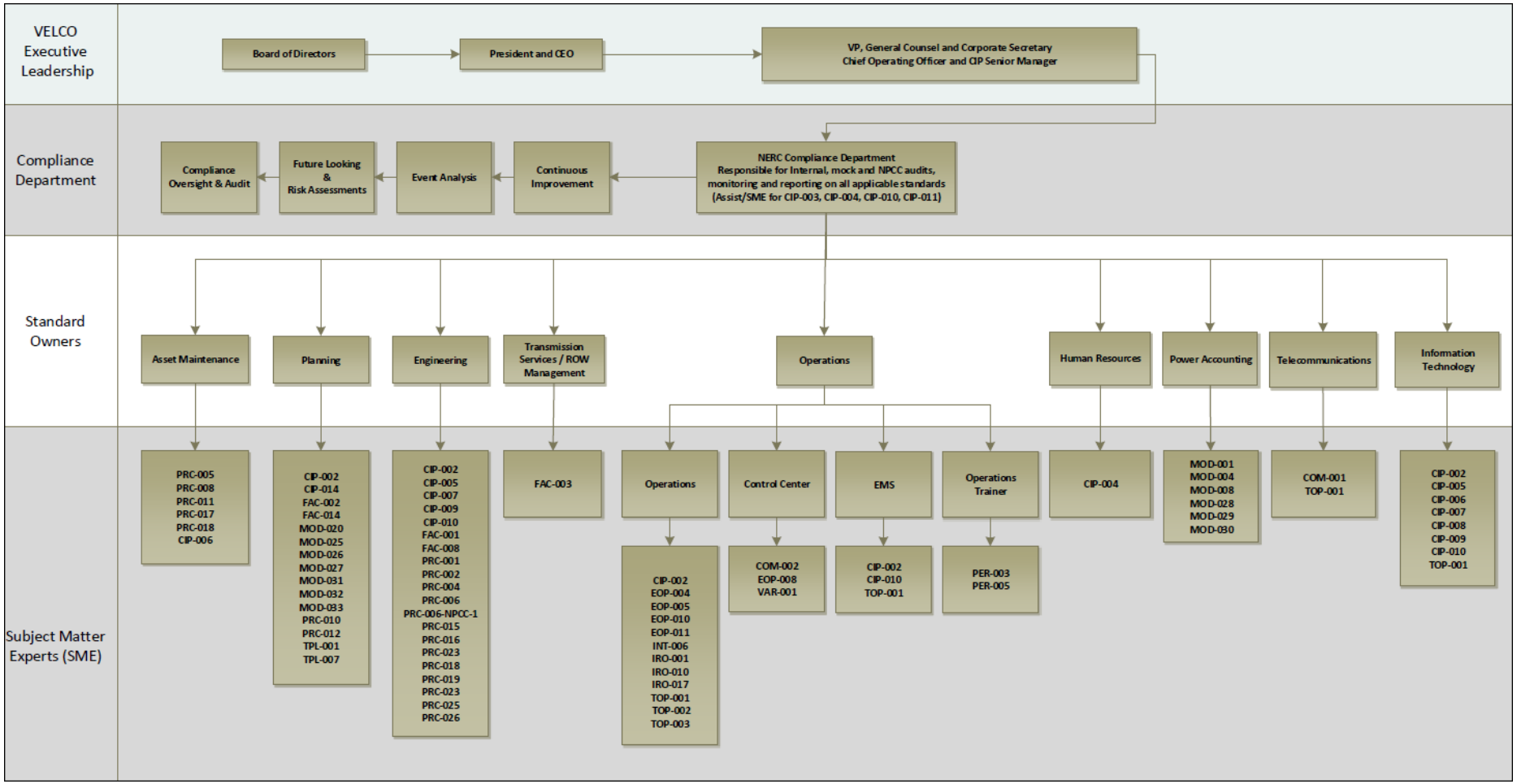


Source: NERC ERO Reliability Risk Priorities – RISC Recommendations to the NERC Board of Trustees - October 2017

Summary of Risks

- As resource mix changes, there are new risks and challenges
  - Fuel security – NE
  - Lack of fault current
  - Intermittency
  - Inertia
  - Inverter issues

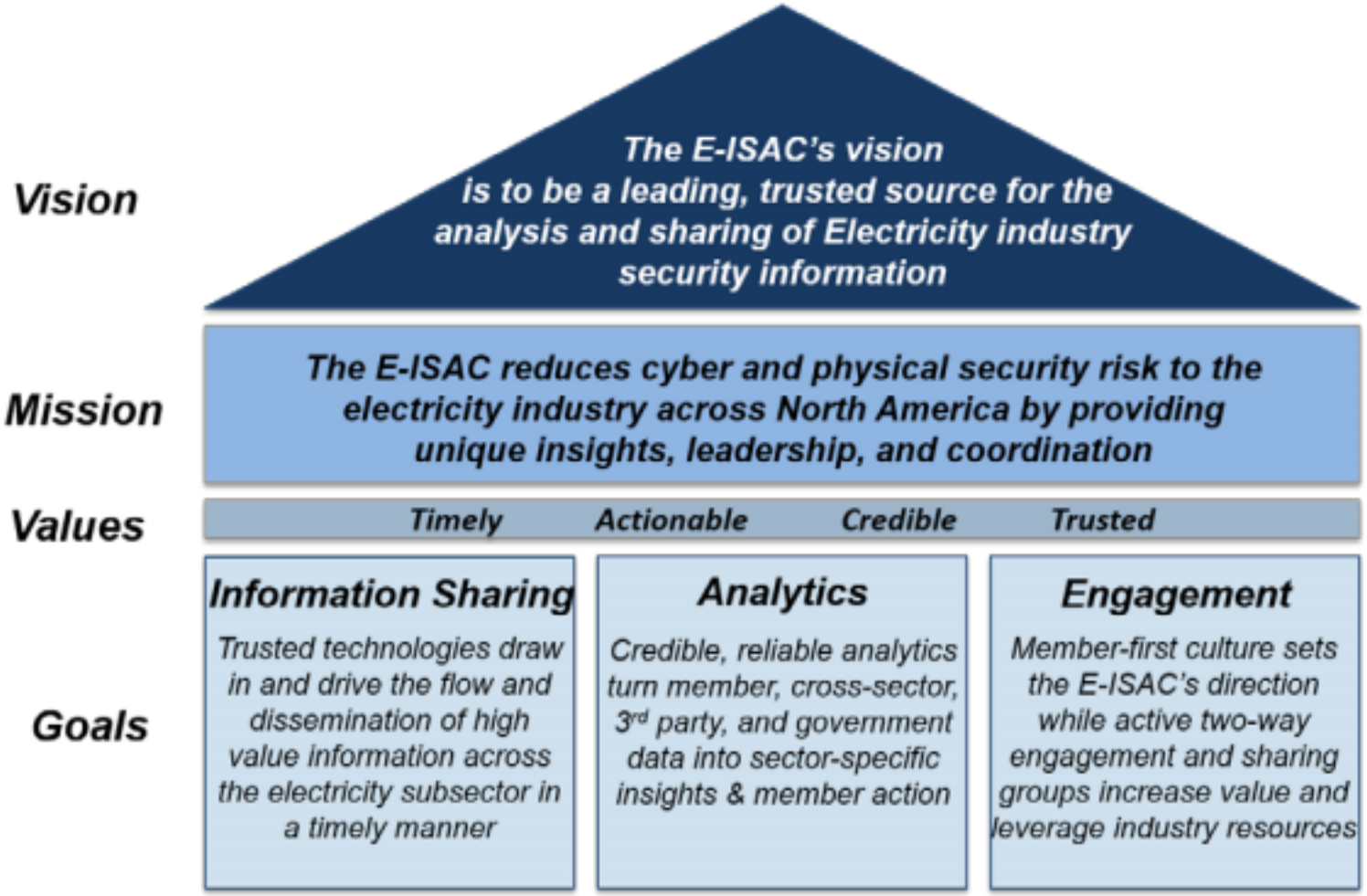
NERC Compliance Program Hierarchy



VELCO

- Must meet all standards
- Gets audited periodically by NERC's regional compliance group – Northeast Power Coordinating Council (NPCC)
- Significant fines for violations since 2008

E-ISAC


Vision
The E-ISAC's vision is to be a leading, trusted source for the analysis and sharing of Electricity industry security information
Mission
The E-ISAC reduces cyber and physical security risk to the electricity industry across North America by providing unique insights, leadership, and coordination
Values
Timely
Actionable
Credible
Trusted
Goals
Information Sharing
Trusted technologies draw in and drive the flow and dissemination of high value information across the electricity subsector in a timely manner
Analytics
Credible, reliable analytics turn member, cross-sector, 3rd party, and government data into sector-specific insights & member action
Engagement
Member-first culture sets the E-ISAC's direction while active two-way engagement and sharing groups increase value and leverage industry resources

High level requirements of CIP-013

- Develop a supply chain cyber security risk management plan to follow in the planning and procurement of vendor equipment and software to be installed in high and medium impact BES Cyber Systems
- Approve & Implement the Plan
- Review the plan and update as needed with approval by CIP Senior Manager no longer than every fifteen calendar months

Next steps:

- Define BES cyber system impact using industry definitions:

Identify applicable assets (CIP-002) as defined by NERC:

BES Cyber Asset- A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

BES Cyber Systems- One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

- Develop program/plan documenting overall approach to protecting assets
  - Identify approach taken to assess risks
  - Identify how defined BES cyber system impact
  - Identify overall process
    - Forward looking: sourcing of products & services through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer

Next steps continued

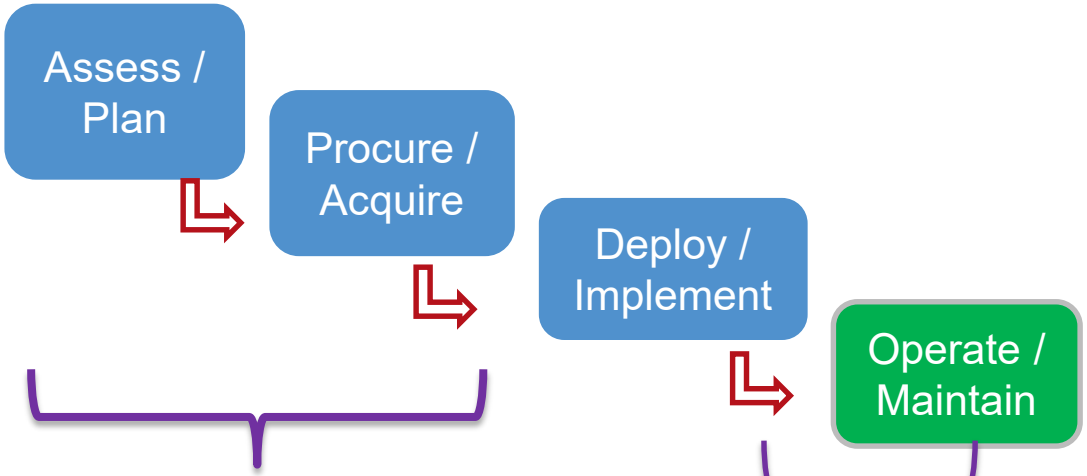
- ID vendors used to purchase applicable assets
- Modify current procurement process to include security controls (particularly those with MSAs)
- Modify current onboarding process to include security controls where necessary
- Create and populate Risk Register
- Train employees on new process
- Approve & Implement the plan
  - Create new procurement MSA / vendor agreements with language around cyber security
  - Create new scorecard to be used when purchasing equipment
- Continuously review/update the plan with a minimum of at least once every 15 calendar months
- CIP Senior Manager or delegator approval for any changes

New procurement process ideas

For purchases identified as having a BES Cyber Impact

- Vendor worksheet / scorecard will rate the security aspects of the vendor in addition to current filters (based on VELCO agreed upon criteria & requirements of CIP-013)
- The scorecard will be reviewed and approved by SMEs
- Purchase request made
- MSA, PO, work-confirmation w/new wording needed
- Did the vendor sign?
  - Yes – contract granted – continue work
  - No – is this a high facility?
    - Yes – don't use the vendor
    - No – if medium assess risks associated. If low and vendor is trusted the PM can justify the risks and continue to use the vendor if so desired

National BES Cyber System Life Cycle



R1 and R2 are meant to address "procurement" activities performed during these phases of the life cycle

R3, R4, and R5 are meant to address "operational" activities performed during this phase of the life cycle

*Note: Plans developed in R1 should "identify and assess risk(s) during the procurement and deployment of vendor products and services" (R1 1.1.1) thus addressing risks during the 1st three life cycle phases

Slide source: NATF CIP-013 Supply Chain Slides for 02142017

Cyber Security Supply Chain Risk Management

- NERC CIP-013-1 strategy
  - Enterprise
  - Supplier
  - Asset type
  - Hybrid (hardware/software)
- Vendor risk management

  (questionnaire ⟶ full audit)
- Need to know where your chips come from

Summary

- Generation mix is rapidly changing across US
- Cyber issues are very “REAL”
- Distributed Energy Resources (DER) at high levels can impact the bulk electric system
- Most inverters of DER are connected to internet with little or no cyber fire walls
- No cyber regulations for DER “FOR NOW!”