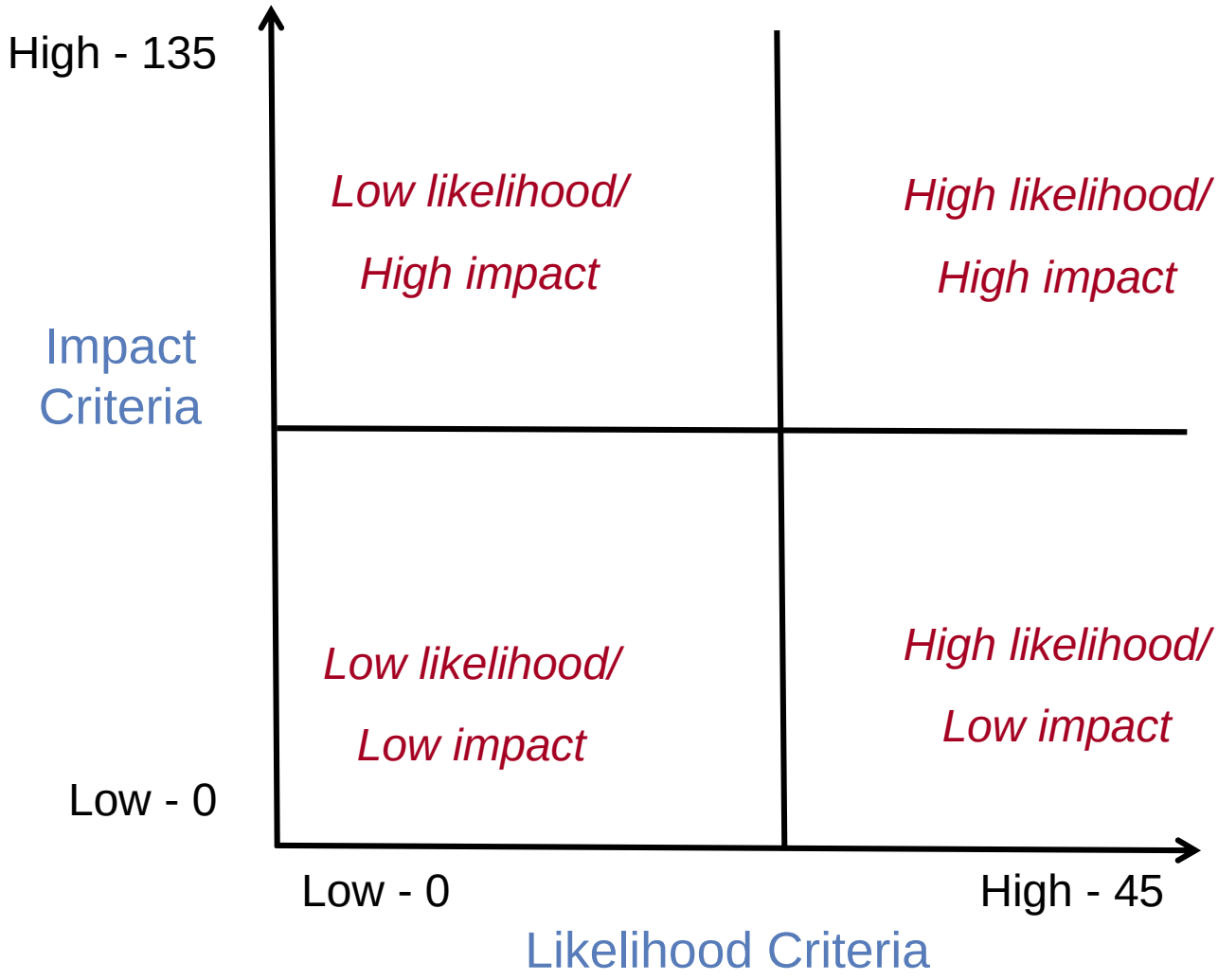
EPRI ELECTRIC POWER RESEARCH INSTITUTE

Security Posture Assessment

Annabelle Lee
Senior Technical Executive

ICCS – European Engagement Summit
April 28, 2015

NESCOR Failure Scenarios Risk Ranking Graph



NESCOR Failure Scenarios Impact Criteria - Examples

Criterion	How to score
System scale	0: single utility customer, 1: neighborhood, 3: town or city, 9: potentially full utility service area and beyond
Public safety concern	0: none, 1:10-20 injuries possible, 3: 100 injured possible, 9: one death possible
Financial impact of compromise on utility	0: Petty cash or less, 1: up to 2% of utility revenue, 3: up to 5%, 9: Greater than 5%

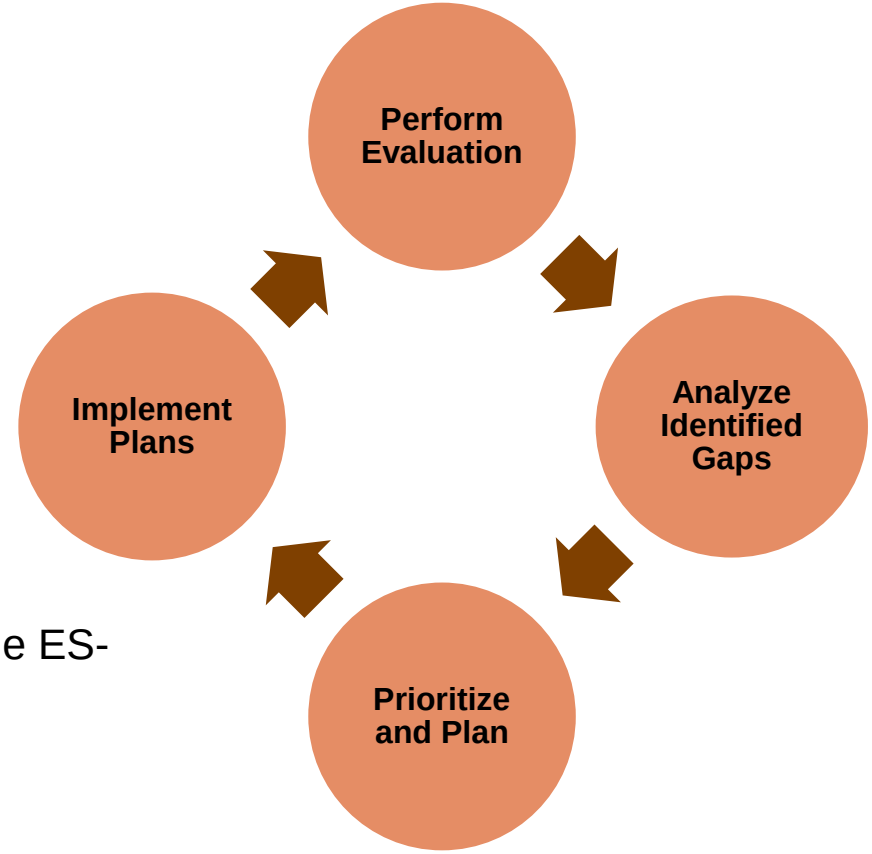
NESCOR Failure Scenarios Likelihood and Opportunity - Examples

Criterion	How to score
Skill required	0: Deep domain/insider knowledge and ability to build custom attack tools, 1: Domain knowledge and cyber attack techniques, 3: Special insider knowledge needed, 9: Basic domain understanding and computer skills
Common vulnerability among others	0: Isolated occurrence, 1: More than one utility, 3: Half or more of power infrastructure, 9: Nearly all utilities
Accessibility (logical, assume have physical access)	0: common knowledge or none needed, 1: publicly accessible but not common knowledge, 3: not readily accessible, 9: high expertise to gain access

Security Posture using the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2):

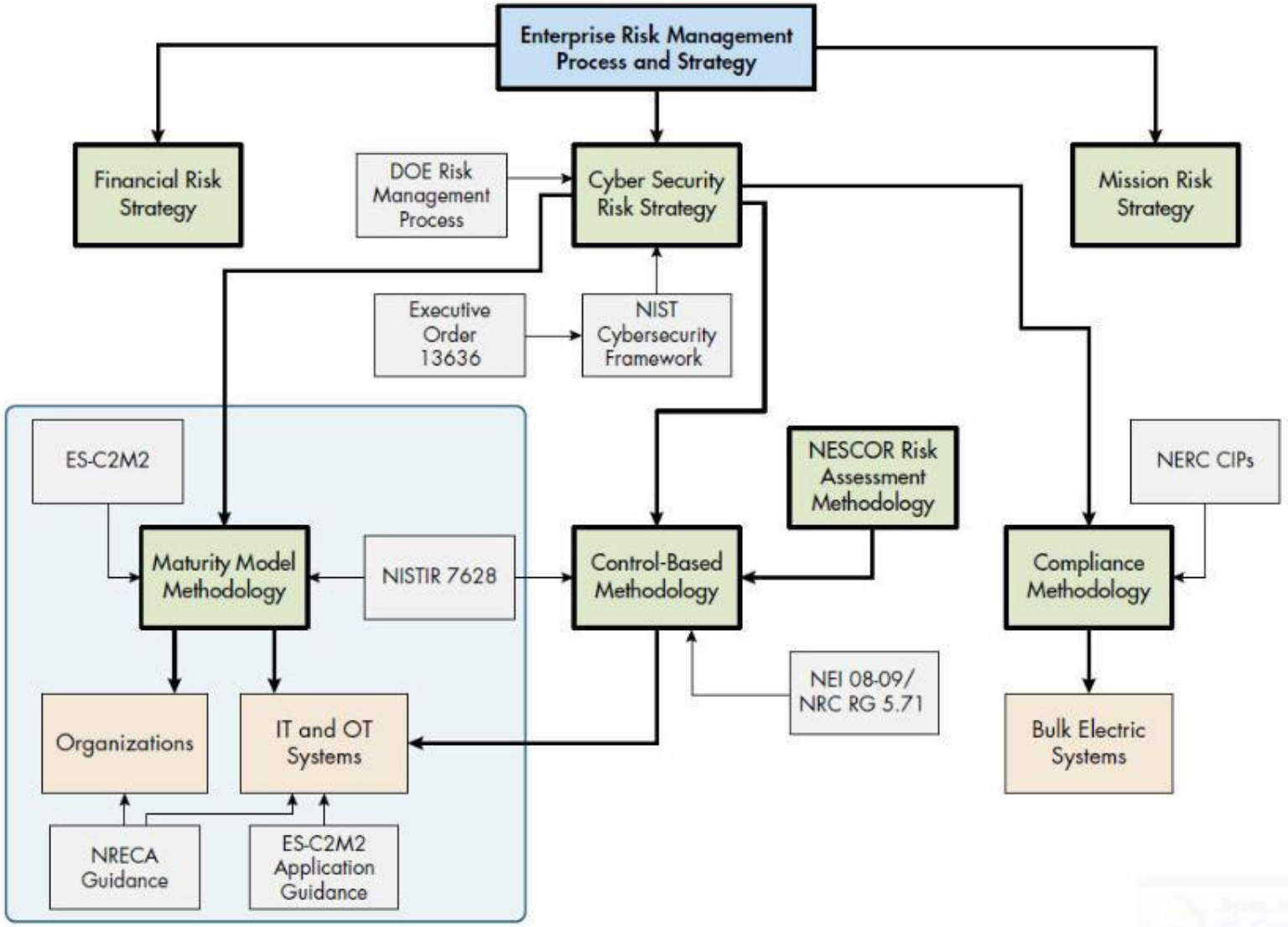
EPRI Technical Update 3002003332

Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)



- Recommended Approach for Using the ES-C2M2
- The process is repeated based on:
  - Implemented plans
  - Changing business objectives
  - Evolving risk environment

Security Posture Assessment



Security Metrics for Energy Delivery Systems

Issue

- The current ES-C2M2 focuses on *organizations*, rather than *systems*

Approach

- Develop *application guidance* for the ES-C2M2 practices
  - Focus on systems
  - Alternative to revising the ES-C2M2 practices
  - Consider the logical interface categories in the NISTIR 7628
- Coordinated with the risk assessment project
  - Build on the mapping documents

Value

- Provide an approach to baseline security posture of systems

- *Work performed in collaboration with DOE, trade associations, members, and volunteers*

Background….

- Companion document to:
  - Risk Management in Practice – *A Guide for the Electric Sector* EPRI Technical Update: 3002003333
- Traces NISTIR 7628 security requirements to ES-C2M2 security practices
  - Identifies assessment methods based on *Guide for Assessing the High-Level Security Requirements in NISTIR 7628, Guidelines for Smart Grid Cyber Security*, SGIP CSWG, 2012-004_1, Version 1.0, August 24, 2012
  - Includes *application guidance* for ES-C2M2 assessments against systems

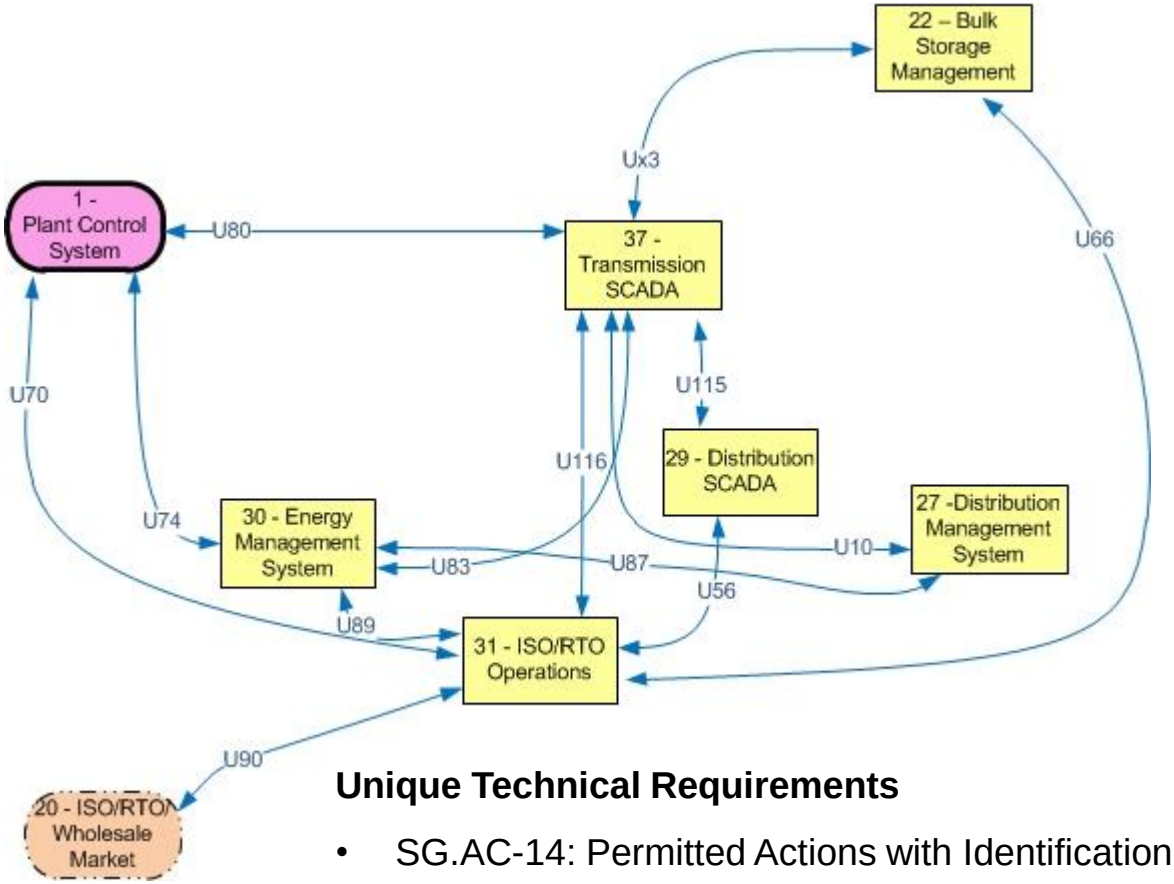
Security Posture Assessment

- NISTIR 7628 assessment methods
  - **Examine -** review, inspect, observe, study, or analyze one or more assessment objects e.g., specifications, mechanisms, or activities).
  - **Interview** - conduct discussions with individuals or groups of individuals
  - **Test -** exercise one or more assessment objects under specified conditions to compare actual with expected behavior
- ES-C2M2 Determination
  - Not Implemented
  - Partially Implemented
  - Largely Implemented
  - Fully Implemented

Application Guidance Example

- Manage Asset Configuration
  - **MIL3**
  - *Configuration Management:* The organization should develop and maintain baseline configurations for the groups of control systems. The ES-C2M2 process should include an assessment to ensure the baselines are reviewed and updated and that the configurations are monitored. The GRC requirements should be developed and applied at the system level, and not at the organization level.
  - SG.CM-2: Baseline Configuration

Logical Interface Category 6: Interface Between Control Systems in Different Organizations



Unique Technical Requirements

- SG.AC-14: Permitted Actions with Identification or Authentication
  - The associated ES-C2M2 practice is IAM-2a
- SG.IA-4: User Identification and Authentication
  - The associated ES-C2M2 practices are IAM-1a and IAM-1b
- SG.SI-7: Software and Information Integrity
  - The associated ES-C2M2 practices are SA-2e and SA-2i

ES-C2M2 and Failure Scenarios Common Mitigations

2. Manage Asset Configuration		
MIL1	b. Configuration baselines are used to configure assets at deployment	• Verify
MIL2	c. The design of configuration baselines includes cybersecurity objectives	• Secure design and implementation • Secure operations
3. Manage Changes to Assets		
MIL2	d. Change management practices address the full life cycle of assets (i.e., acquisition, deployment, operation, retirement)	• Track, implement configuration management • Secure operations
MIL3	f. Change logs include information about modifications that impact the cybersecurity requirements of assets (availability, integrity, confidentiality)	• Track, implement configuration management
4. Management Activities		
MIL2	a. Documented practices are followed for asset inventory, configuration, and change management activities	• Track, implement configuration management • Track • Plan • Profile • Secure design and implementation

Cyber Security Metrics Framework – What's Next….

Cyber Security Metrics Framework

Issue

- Lack of a standard way to show the value of cyber security to the organization – current focus is operational metrics

Approach

- Need to show the real risk to the organization
- Meaningful metrics and data displays for leadership/management

Value

- How used to make risk decisions across the organization and prioritize risk

Cyber Security Metrics Framework (2)

- Current status
  - Show vulnerabilities addressed and patches deployed
  - Don’t understand the real risk to the organization
- Goals
  - How show as value added at the business unit level?
    - Example: comparison of impact cost and mitigation
  - Need more predictive metrics
  - Beyond signatures to behavior analysis
  - Want monitoring tools across the operational organizations
  - Would like to know how compare with peers
  - Meaningful metrics and data displays for leadership/management
    - Status related to ES-C2M2, NIST Cybersecurity Framework, NISTIR 7628, etc.

alee@epri.com

202.293.6345

Discussion

Together…Shaping the Future of Electricity