EPRI Cyber Security Assessments

TOGETHER...SHAPING THE FUTURE OF ENERGY™

CYBER SECURITY ASSESSMENTS ACROSS SECTORS

1 Level 1: Enterprise Level Assessment
Cross-Sector EPRI Team assess a utility's cyber security programmatic maturity and organization across the entire enterprise.

2 Level 2: Business Unit Assessment
Sector focused OT assessments, led by the home sector, using cross-sector resources for exposure.

3 Level 3: Technical Assessment
Assessment of a utility's specific systems using risk-informed methodologies, metrics, or other standards.

Different Assessment Types for Different Focused Outcomes

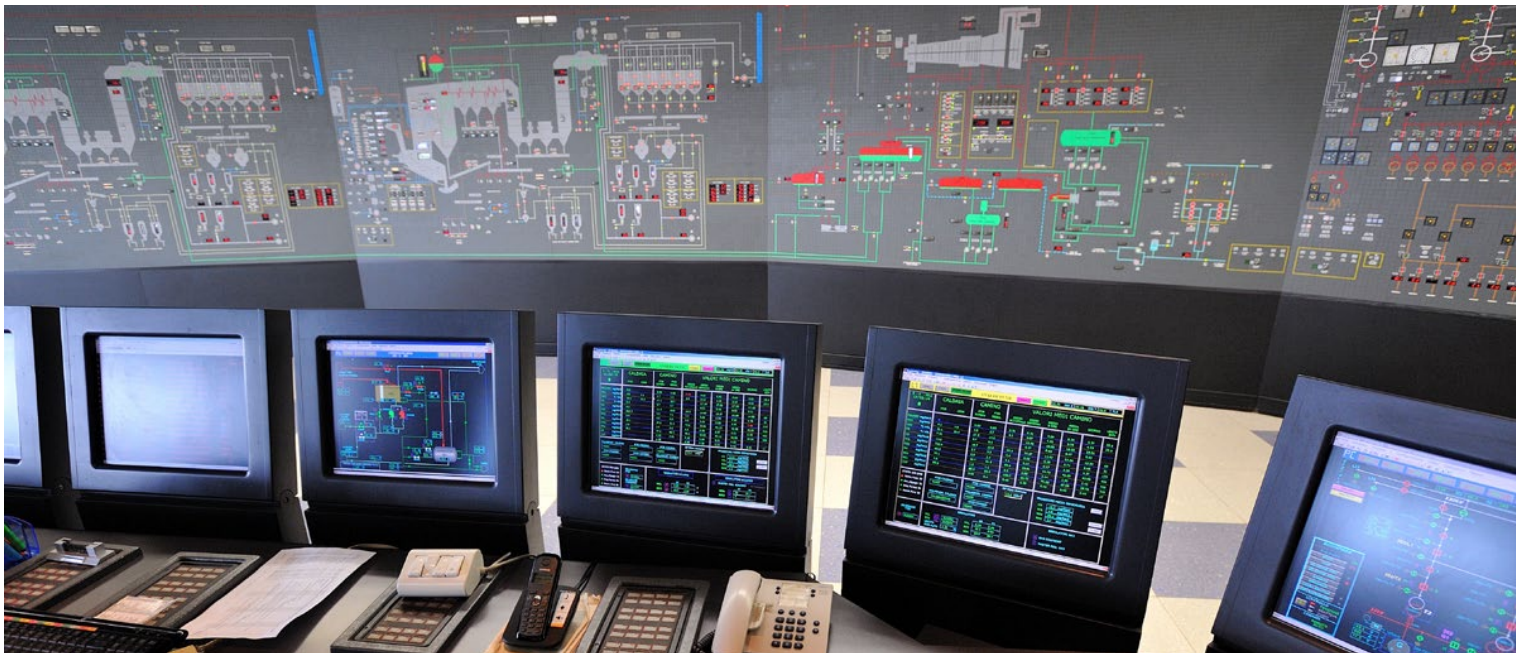
ENTERPRISE LEVEL ASSESSMENT

Objective: Providing insight and best practices for an enterprise-level cyber security strategy across all business units

- Assess the utility's cyber security programmatic maturity
- Align with corporate objectives and performance indicators and senior leadership vision
- Develop near and long-term performance goals in accordance with industry best practices and standards
- Driving efficiencies through alignment and coordination of IT/OT across all business units

Expected Outcomes

- Report detailing goals, benchmarking, quick wins, and an implementation roadmap
- Utility is able to develop an action plan based on results
- Leadership presentations and stakeholder communications
- Opportunities for inreased efficiency and less sensitivity to change through alignment across business units



BUSINESS UNIT ASSESSMENT

- Generation OT Cyber Security Programmatic Assessment
  - Focusing on programmatic implementation areas, IT/OT integration, and interdependencies
- Customized assessment criteria based on EPRI research methodologies, industry best practices, standards, and regulatory guidance
- Developing recommendations for capability and maturity improvement by providing:
  - Implementation roadmap prioritizing quick wins
  - Project plan to understand time, resource, and funding commitments
  - Shared lessons learned and anonymized observations for all members

Additional Materials SPN: 3002014441

- Delivers objective readiness review of overall or specific OT cyber security program aspects to help utilities prioritize actions that improve postures
- General assessments examine overall OT cyber security program based on NIST Cybersecurity Framework or DOE's C2M2
- Tailored assessments examine specific OT cyber security concerns like remote access or transient cyber assets
- Risk assessments focus on the highest priority OT risks for baseline plans and ongoing mitigations
- Recommendations address gaps in technologies, processes, and skills with actionable information
- Leverages EPRI's expertise in utility OT environments and applies research results to recommendations

Additional Materials SPNs:
3002020210 (General)
3002022419 (Tailored)

- Assessment offering based upon the EPRI Nuclear Cyber Security Program Guide that focuses on:
  - Developing a risk-informed implementation
  - Measuring against performance-based, objective criteria
  - Either new program setups or ongoing program maintenance
  - Review existing process on how best to incorporate methodologies based upon EPRI research
  - Recommendations for incorporating cyber security throughout the entire design lifecycle

TECHNICAL ASSESSMENT

EPRI's Cyber Security Technical Assessment Methodology (TAM) offers a risk-informed methodology for utilities to assess digital components, determine the actual vulnerabilities, and allocate appropriate mitigations.

Security standards and tools typically focus on company-level risk and may apply the same controls to every component from a control catalog. EPRI's risk-informed guidance advances the traditional vulnerability assessment and mitigation process through a systems engineering approach that enables users to assess specific cyber security risks at the component or system level.

TAM Interest Group

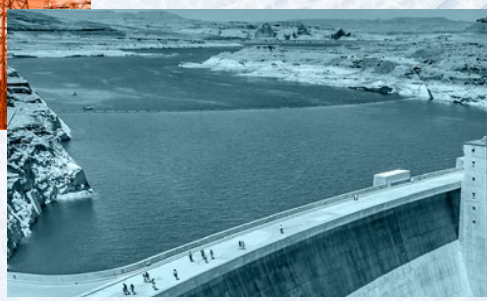
The TAM Interest Group is a collaboration for users and those interested in the TAM research. Through structured collaboration, participants can enable effective implementation while also encouraging process improvement. Users will gain insight into the TAM process and risk-informed cyber security practices.

The objectives of the TAM Interest Group are the following:

1. Provide structured and ongoing technology transfer to the electric sector and vendors.
2. Provide a method for formal feedback, lessons learned capture, and process improvement.
3. Provide an opportunity for individualized implementation support.

Technical Contact: jhollern@epri.com
TAM Computer Based Technology Transfer Module: 3002016907






TOGETHER...SHAPING THE FUTURE OF ENERGY™

EPRI 3420 Hillview Avenue, Palo Alto, California, 94304-1338 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com
© 2022 Electric Power Research Institute (EPRI), Inc. All rights reserved.

3002023190