Cyber Security Risk Assessment
Process flowchart

START

- **Initial system architecture diagrams and inventory**

1 Identify the System Under Consideration (SUC)

- **Updated system architecture diagrams and inventory with IACS external services & support identified**

- **Existing PHAs and other relevant risk assessments and corporate risk matrix**

2 Perform a high-level cybersecurity risk assessment

- **Initial security level target for SUC and evaluation of risk**

- **Standards and best practices, policies, supplier guidelines, criticality assessments, data flows, functional specifications, etc.**

3 Partition the SUC into zones and conduits

- **Initial or revised zone and conduit diagram**

YES ⚠ **NO**

4 High-level risk exceeds tolerable risk?

- **Company policies, regulations, tolerable risk guidelines**

5 Perform a detailed cybersecurity risk assessment

6 Document requirements for additional security countermeasures

- **Residual cybersecurity and SL-Ts for each zone and conduit**

- **Cybersecurity requirements specification (CRS)**

7 Asset Owner Approval

→ Process

→ Documents

ID: 9AKK107778