North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

Large Entity Use-Case Webinar: Conducting Supply Chain Supplier Assessments

Exelon

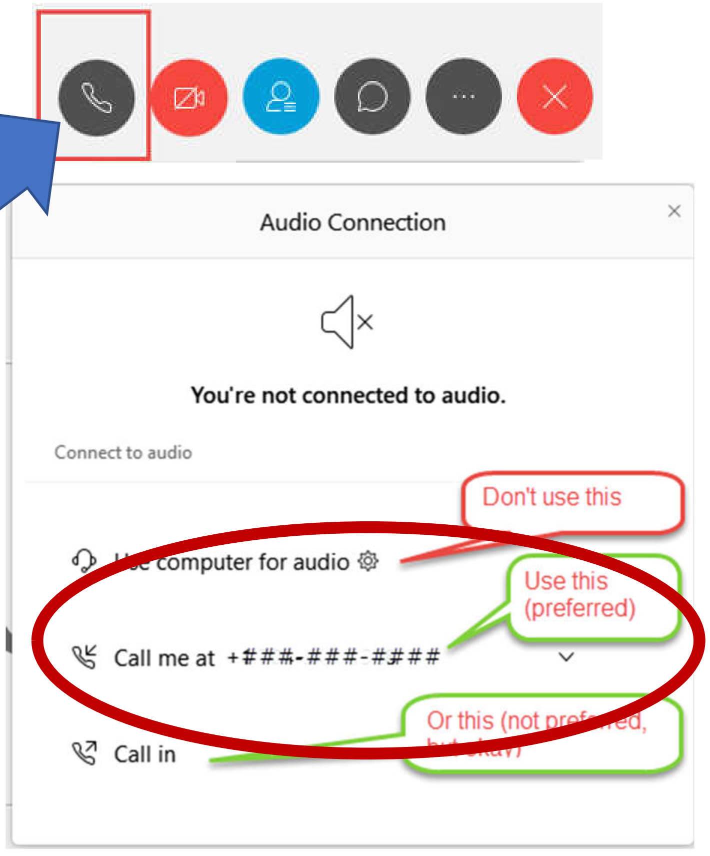
September 1, 2020

Open Distribution

Webex Audio Connection

- **Don't - dial in separately**
- **Do - have Webex CALL YOU**

- Select ☎ to connect to audio
  - Select the "Call me at…" option
  - Don't select "Use computer for audio"
  - Don't select "Call in" unless "Call me at…" does not work



Audio Connection

You're not connected to audio.

Connect to audio

Use computer for audio

Call me at +###-###-####

Call in

Don't use this

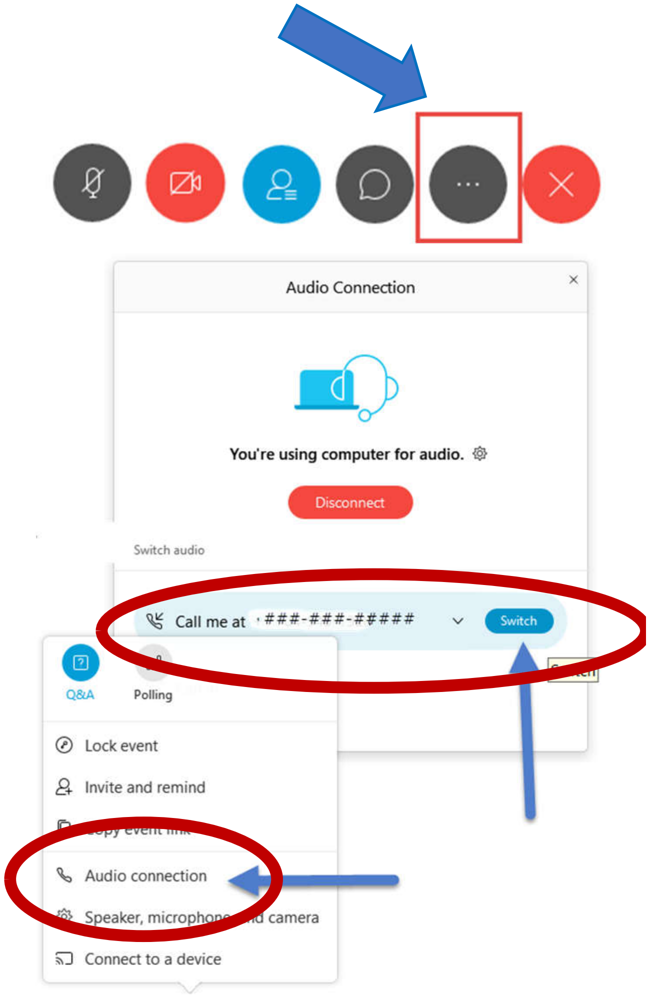
Use this (preferred)

Or this (not preferred, but okay)

If you connect to audio the wrong way,

you can change it

1. Select the “More Options” menu
2. Select “Audio connection”
3. Select “Disconnect” or select “Switch” next to “Call me at…”



You're using computer for audio.

Agenda Overview

- Introduction of NATF Supply Chain Activities
- Exelon presentation
- Q&A

Objectives

Security

- Identifying and addressing cyber security risks introduced via supply chain

Industry Convergence

- Achieve industry convergence on the approach (Model) to facilitate addressing the following objectives

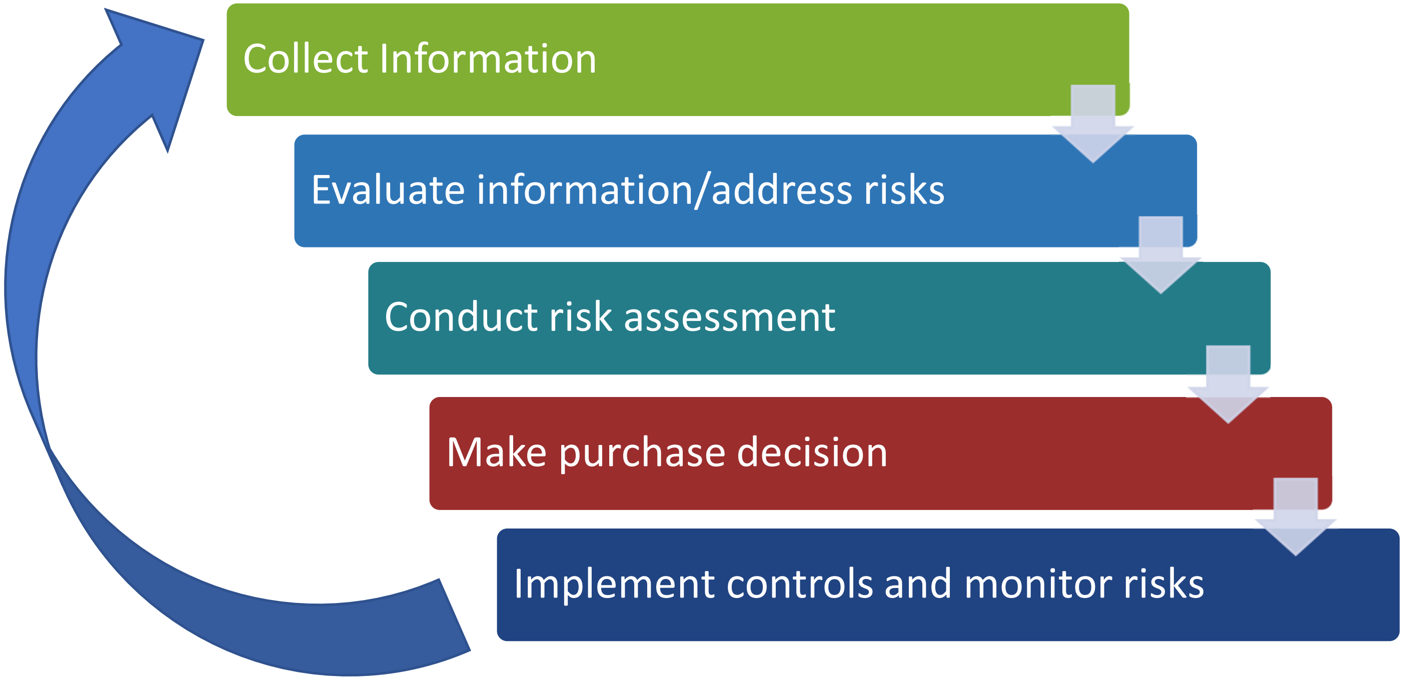
Efficiency and Effectiveness

- Convergence on common approaches to achieve reasonable assurance of suppliers’ security practices

Compliance

- Implementation guidance to meet supply chain related CIP standards (CIP-013-1; CIP-005-6 R2.4; CIP-010-3 R1.6)

Supplier Assessment Model Process Overview



Collect Information

Evaluate information/address risks

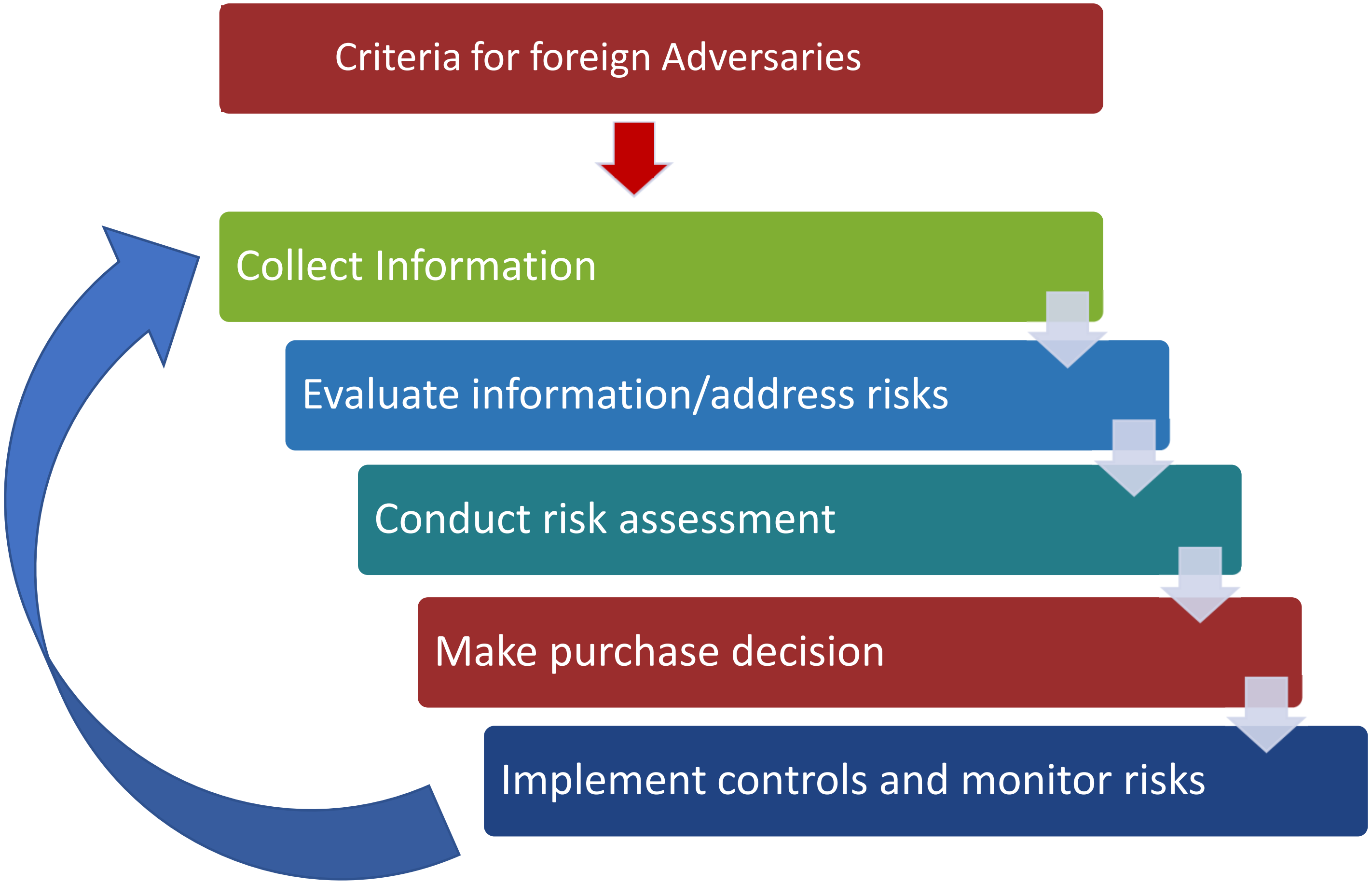
Conduct risk assessment

Make purchase decision

Implement controls and monitor risks

Open Distribution

Possible Assessment Process with EO Criteria



Criteria for foreign Adversaries

Collect Information

Evaluate information/address risks

Conduct risk assessment

Make purchase decision

Implement controls and monitor risks

North American Transmission FORUM

Open Distribution

Collect Information

- **Collect it yourself**
  - NATF Cyber Security Criteria for Suppliers
  - Energy Sector Supply Chain Questionnaire
  - Supplement with
    - Historical knowledge
    - Open source research
- **Use a solution-provider service**

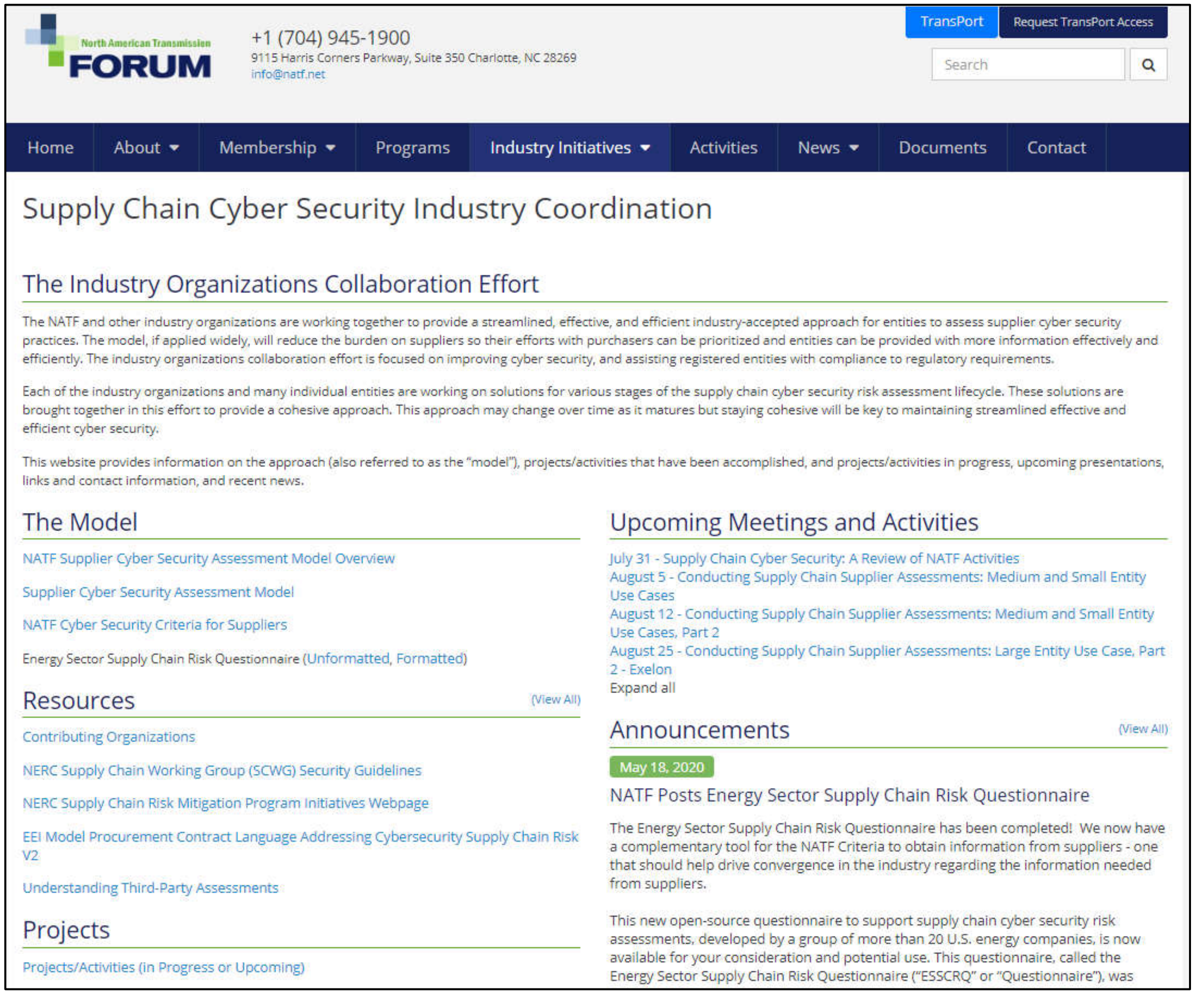
Collect Information

Methods to Obtain Assurance of Accuracy

- **Third-party Assessments**
  - *Obtain a qualified assessors' third-party assessment, certification and/or independent audit that addresses NATF Criteria and Questionnaire*
- **Obtain a validation/verification from a solution provider**
  - *Solution-provider risk assessments*
  - *Shared assessments*
- **Conduct your own validation/verification**
  - *Obtain evidence from supplier to conduct your own validation/verification*

Collect Information

NATF-hosted Industry Organizations Web Page



+1 (704) 945-1900
9115 Harris Corners Parkway, Suite 350 Charlotte, NC 28269
info@natf.net

Supply Chain Cyber Security Industry Coordination

The Industry Organizations Collaboration Effort

The NATF and other industry organizations are working together to provide a streamlined, effective, and efficient industry-accepted approach for entities to assess supplier cyber security practices. The model, if applied widely, will reduce the burden on suppliers so their efforts with purchasers can be prioritized and entities can be provided with more information effectively and efficiently. The industry organizations collaboration effort is focused on improving cyber security, and assisting registered entities with compliance to regulatory requirements.

Each of the industry organizations and many individual entities are working on solutions for various stages of the supply chain cyber security risk assessment lifecycle. These solutions are brought together in this effort to provide a cohesive approach. This approach may change over time as it matures but staying cohesive will be key to maintaining streamlined effective and efficient cyber security.

This website provides information on the approach (also referred to as the "model"), projects/activities that have been accomplished, and projects/activities in progress, upcoming presentations, links and contact information, and recent news.

The Model

NATF Supplier Cyber Security Assessment Model Overview

Supplier Cyber Security Assessment Model

NATF Cyber Security Criteria for Suppliers

Energy Sector Supply Chain Risk Questionnaire (Unformatted, Formatted)

Resources

(View All)

Contributing Organizations

NERC Supply Chain Working Group (SCWG) Security Guidelines

NERC Supply Chain Risk Mitigation Program Initiatives Webpage

EEI Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk V2

Understanding Third-Party Assessments

Projects

Projects/Activities (in Progress or Upcoming)

Upcoming Meetings and Activities

July 31 - Supply Chain Cyber Security: A Review of NATF Activities
August 5 - Conducting Supply Chain Supplier Assessments: Medium and Small Entity Use Cases
August 12 - Conducting Supply Chain Supplier Assessments: Medium and Small Entity Use Cases, Part 2
August 25 - Conducting Supply Chain Supplier Assessments: Large Entity Use Case, Part 2 - Exelon
Expand all

Announcements

(View All)

May 18, 2020

NATF Posts Energy Sector Supply Chain Risk Questionnaire

The Energy Sector Supply Chain Risk Questionnaire has been completed! We now have a complementary tool for the NATF Criteria to obtain information from suppliers - one that should help drive convergence in the industry regarding the information needed from suppliers.

This new open-source questionnaire to support supply chain cyber security risk assessments, developed by a group of more than 20 U.S. energy companies, is now available for your consideration and potential use. This questionnaire, called the Energy Sector Supply Chain Risk Questionnaire ("ESSCRQ" or "Questionnaire"), was

Exelon – Post CIP 13 Implementation

Betsy Soehren-Jones, Director of Security Governance

Jennifer Burke, Director of IT Compliance

Erin Holloway, Senior Manager of Supply Sourcing

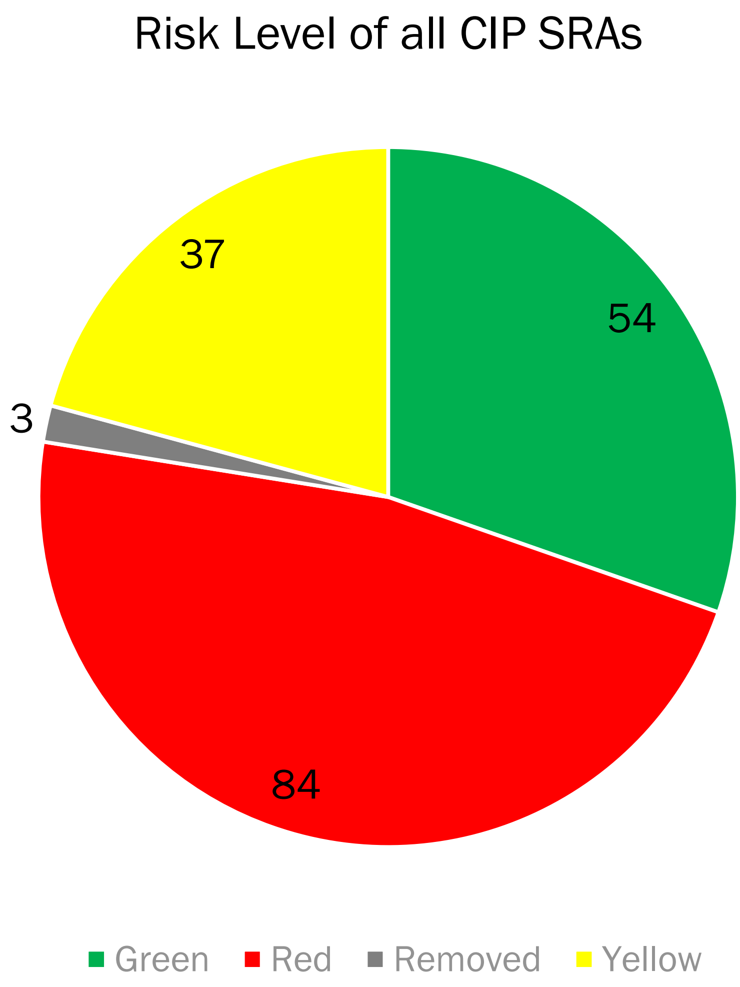
Dan Greenhalgh, 3rd Party Project Manager

Open Distribution

SRA – Top 8 “Knockout” Questions

1. Do you have an industry recognized Information Securit4y Policy published and available to all employees, including contractors and part-time employees (e.g., NIST CSF, ISO 270001)?
2. Are employees obligated as a condition of employment to adhere to the Information Security Policy?
3. Do you have written policies/procedures/guidelines for maintaining and monitoring the security of customer data?
4. Do you use anti-virus software on corporate devices or devices owned by employees that will be utilized to process Exelon information?
5. Are your anti-virus signatures updated on a defined regular basis?
6. Do you contract with subcontractors (fourth party vendors to Exelon) in the development or delivery of your application, device and/or service you are proposing to Exelon
7. Are you an affiliated entity of or do you procure products or services from the vendors listed below or their subsidiaries/affiliates?
    - ❑ Kaspersky
    - ❑ Huawei Technologies Company
    - ❑ ZTE Corporation
    - ❑ Hytera Communications
    - ❑ Hangzhou Hikivision Digital Technology Company
    - ❑ Dahua Technology Company
8. Do you conduct background checks (e.g., credit, criminal, drug, employment checks) for all employees?

SRA – Risk Levels



CIP-005 Vendor Remote Access

- Leveraged the existing controls in the Exelon NERC CIP Access Control system and Interactive Remote Access System. This includes treating all vendors with need for logical access as badged, screened and trained Exelon contractors.
- Performed sanity check of all firewall rulesets validating that no system-to-system remote access was present.
- Implemented additional controls and performed dry runs of new process in job aid. Performed sampling of data from process since August 2019 – present.

1. Updated the internal Interactive Remote Access process documents across Exelon.
2. When alerted, Security will leverage existing SEM processes to identify user live session as documented in the new job aid(s) and notify the appropriate internal team supporting IRA solution.
3. Internal IRA support team will terminate the user live session as documented in the new job aid(s)
4. Store appropriate evidence of compliance and close out the Controls Framework task for tracking.

CIP-010 Integrity and Authenticity of Software

Technology

- Leveraged existing NERC CIP Production Change Management System and Patch Tracking Tools with added indicators and tracking.
- Research performed around vendors that had built in integrity checks for patches and software downloads.

People

- Exelon Device Owners were engaged across the enterprise to validate the device type method for validating the downloaded software/patch.
- Leveraged the Prosci ADKAR change management methodology to bring stakeholders into the process early and with engagement.
- Had specific training for Exelon Device Owners who were performing new software validation and capturing the evidence.

Processes

- Updated all CIP-010 and CIP-007 R2 Exelon Process documentation and job aids
- Established controls within Controls Framework tool for evidence gathering and periodic sampling/review.

Next Steps – Maturity Advances

Background

- Exelon is benchmarking and baselining Third Party Risk Management (TPRM) and Due Diligence processes with our peers across the Utility industry, not only specifically related to NERC CIP—013 compliance, but more broadly to encompass all procurement and Third-Party activity across the lifecycle (new vendor onboarding, continuous monitoring, offboarding).

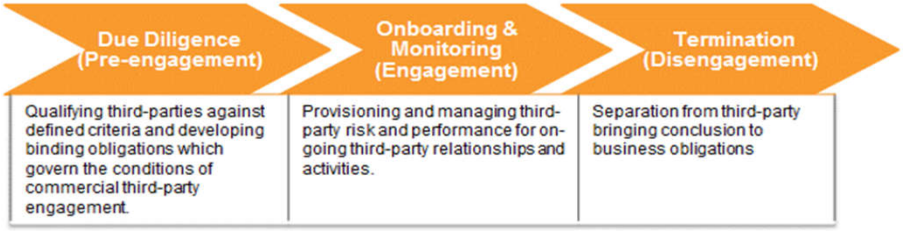
- We recognize that across the Energy Industry, there are varying levels of TPRM maturity, and that there are opportunities for efficiency gains and optimization of our Third-Party processes (e.g. scaling level of diligence to the risk posed, enterprise workflow management tools).

- The questions are intended to be fairly high-level and encapsulate feedback from individual departments who play a part in Third Party Processes (e.g. Legal, Supply, IT, Insurance, Risk, Audit) as well as a holistic look at

- Third Party Processes in general (e.g. how do you coordinate between the various internal stakeholders, who owns the process for your organization, do you have a formalized TPRM framework).

- Exelon will consolidate the responses and distribute the results and findings to all participants.

- We are looking to launch the benchmarking in September 2020. If you are interested in participating, please contact Daniel.Greenhalgh@exeloncorp.com.



Due Diligence (Pre-engagement)
Qualifying third-parties against defined criteria and developing binding obligations which govern the conditions of commercial third-party engagement.

Onboarding & Monitoring (Engagement)
Provisioning and managing third-party risk and performance for on-going third-party relationships and activities.

Termination (Disengagement)
Separation from third-party bringing conclusion to business obligations

Questions

Thank you for attending!

NATF Contact Information

supplychain@natf.net

kkeels@natf.net

vagnew@natf.net