

Securing Your Supply Chain

Designing and Implementing Supply Chain Security Programs

Shari Gribbin

CNK Solutions Corp



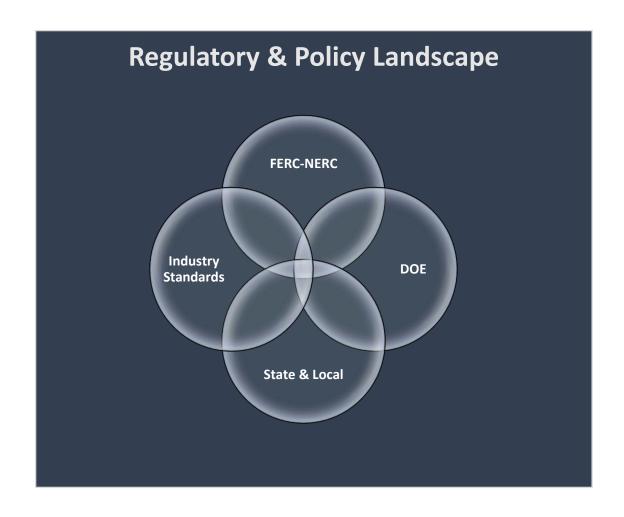


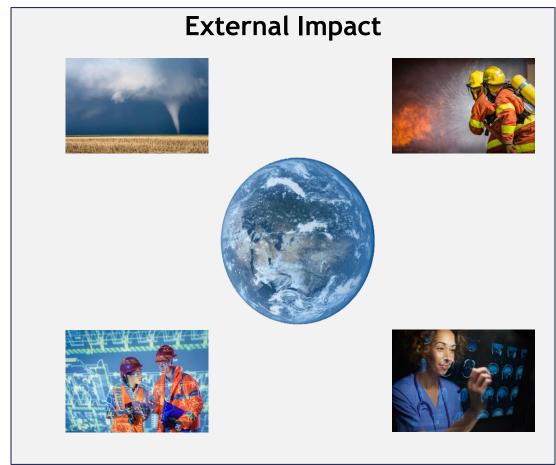
Introduction

- Introduction
- Understanding the landscape
- Defining the Foundation
- Develop and Implement
- Conclusion



Understanding the Landscape





Understanding the Landscape

Supply Chain Risks & Key Considerations

Common Fail Points in Supply Chain Programs

- Procurement Processes
- ➤ Inadequate Contract Terms
- Organizational Silos
- Vendor Security Failures

- Inventory Gaps
- Poor Training
- Remote Access
- Weak QA Controls

Core NERC CIP Supply Chain Requirements

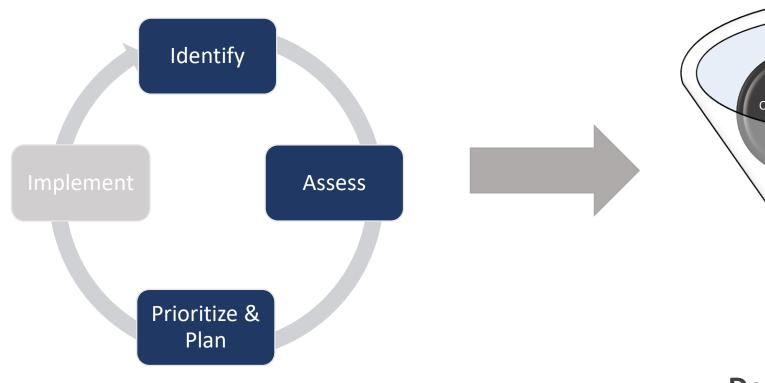
	Documented Program	Formally documented supply chain risk management program with defined elements
	Vendor Notification Requirements	Access requirements, product vulnerability and cyber incident notices
	Remote Access Controls	Enhancements to remote access restrictions/controls for vendors
	Software	Verification and security requirements prior to deployment

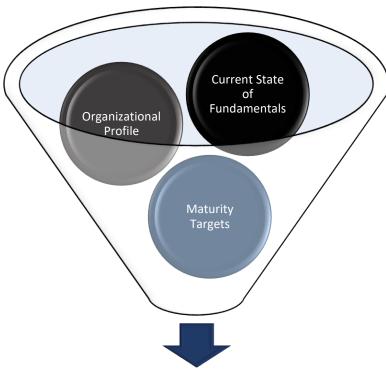






Defining the Foundation





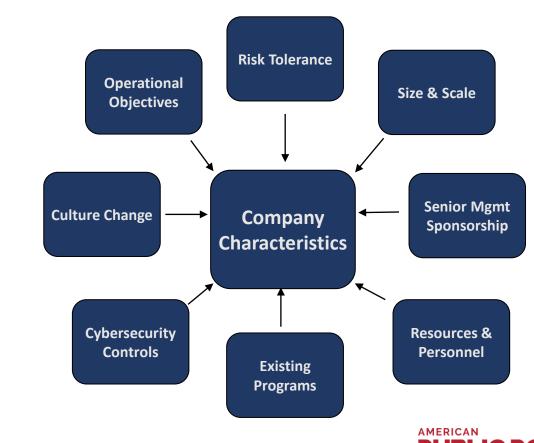
Develop & Implement



Defining the Foundation: Identify & Assess

Develop an Organizational Profile





80 Years of Powering Strong Communities

Defining the Foundation: Identify & Assess

Understanding Current State

Supply Chain

- Supply Chain Security Program
- Procurement Processes
- Vendor Agreements
- Vendors, Assets, Hardware, Software

Enterprise

- Leadership Engagement
- · Regulatory Change
- Governance and Compliance
- Enterprise Risk



Cybersecurity

- Cybersecurity Program
- Existing Controls (e.g., access management, threat and vulnerability, virus / malware)
- NERC CIP and Regulatory Compliance

Tools and Technology

- Systems, tools and other technology supporting supply chain security
- · Existing technology
- · Long-term investments

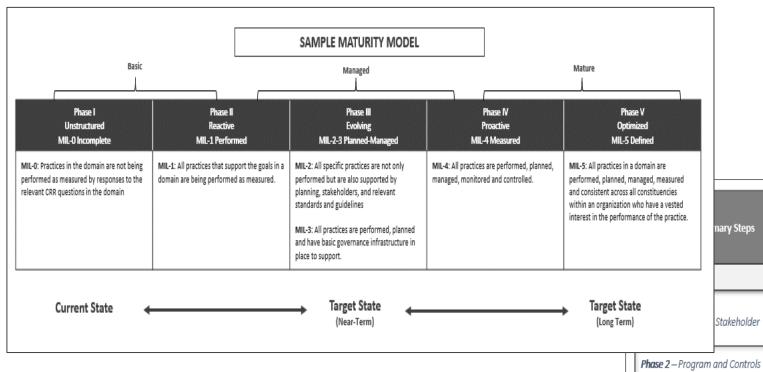


THE ACADEMY | AMERICAN PUBLIC POWER ASSOCIATION

Defining the Foundation: Maturity Targets

Development

Activities



Prioritize and Plan

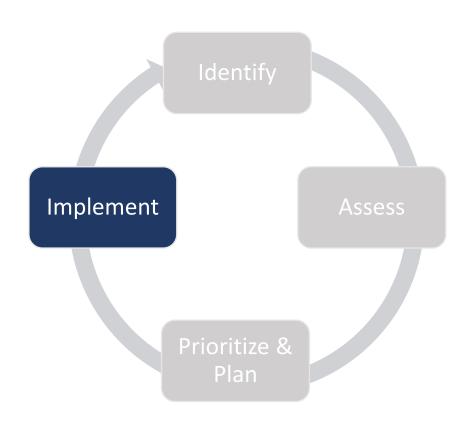








Develop and Implement: Risk Assessment



Develop a Baseline and Risk Assess

1. Priority Assets & Operations

2. Inventory Suppliers

3. Agreements

4. Assets / Components

 Risk-based approach must prioritize high-risk assets and operations

 Focus is first on suppliers and then on improving agreement terms

> Assets and components are evaluated where supplier risk cannot be managed, or other high-risk factors exist



Develop and Implement: Risk Assessment





Supplier Cyber Security Assessment Model Overview

Introduction

Supply chain cyber security risk management continues to receive much industry and regulatory attention. The NATF and other industry organizations have worked together to produce guidance and tools to address various steps in the supply chain cyber security risk assessment lifecycle (Figure 1).1

Criteria for Supplier









Figure 1: The Supply Chain Cyber Security Risk Assessment Lifecycle

The NATF has created a supplier cyber security assessment model that:

- 1. Establishes criteria entities may use to evaluate supplier cyber security practices (NATF Criteria)
- 2. Suggests how entities obtain assurance of the supplier's adherence to the criteria

MUS

Chain Material

the NATF Criteria to evaluate a supplier's cyber security practices. The criteria are mapped to equirements of the NERC standards and common industry security standards and frameworks ped to additional security standards or frameworks.

ne NATF Criteria can be demonstrated using existing industry security standards, frameworks, approaches, allowing suppliers to provide evidence from a certification or an independent how how the supplier's practices support each criterion.3 When a third-party assessment is not iers may provide other evidence to demonstrate their adherence to the criterion (Figure 2).

ses are inputs into the entity's risk analysis for the supplier. Entities determine whether the ained from the supplier identifies risks in the supplier's cyber security practices, and whether be mitigated (by the entity or supplier) or accepted. This determination, along with other factors sk analysis, will guide the entity's purchase decision.

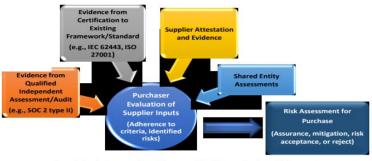


Figure 2: Supplier Demonstration of Adherence to Criteria Supports Purchaser Risk Assessment

North American Transmission Form Supply Chain Security Coordination Initiative:

https://www.natf.net/industry-initiatives/supply-chain-industry-coordination



Develop and Implement: Define a Program

General Program Considerations

Program Documentation

Definitions & Key Concepts

Roles & Responsibilities

Identify executive ownership or sponsor, determine where the program will reside and who should have a primary vs. secondary role in defining and implementing the processes and controls. How will issues and concerns be managed through first few phases of implementation.

Determine appropriate program documentation for your organization, size, scale, culture. Assess existing programs and opportunities for efficiencies. Consider structure and scope required. For example, overarching program with additional implementing program guides and documents or single program document pointing to existing controls or flow charts.

Identify any key terms and concepts you will need to include and ensure definitions that exist in other programs/controls are aligned. For new terms and concepts consider level of guidance and additional reviews by non-SME personnel.

Roles and Responsibilities must be clearly defined and training and change management should account for personnel who have not historically had formally assigned obligations within processes outside their organization (e.g., legal and procurement). Consider role of legal, procurement, risk, IT and security.



Develop and Implement: Procurement Processes

Designing and updating your procurement related processes for integration into your program

Procurement of products & Services

 Processes for procurement, approvals, exceptions, work orders/requisition outliers

Assessing Vendors (Program element)

 Vendor risk assessment process (what it is, who owns it, how it is implemented)

Tracking and Management of Vendors

Controls for the continuous management of an inventory of vendors and agreements

Personnel Risk Assessments

PRAs for vendors, processes and integration with procurement program

Vendor Training

Training requirements, how defined, identified and implemented

Vendor Access

 Ensuring integration with cyber, physical and information security access management controls

Information Sharing

 Standards for information protection, data integrity and compliance requirements

Vendor Metrics

Define performance metrics and minimum standards and include in agreements

Monitoring, QA and Audit

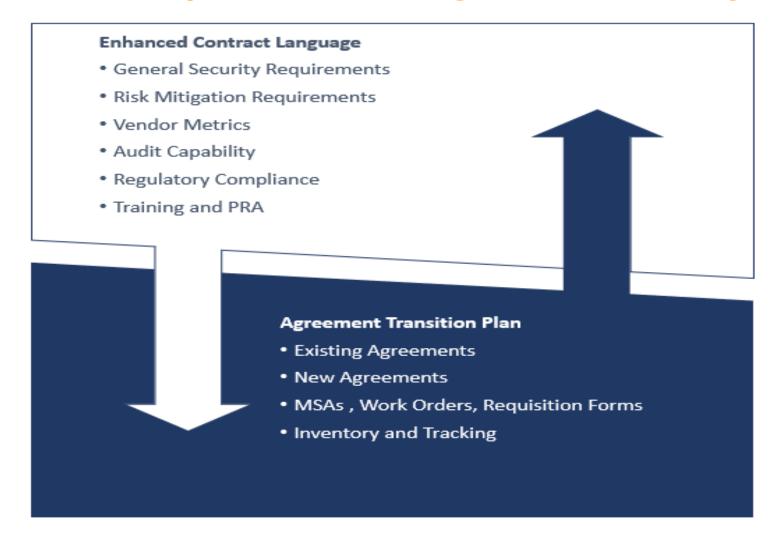
 Include monitoring, QA and audit controls to verify compliance with agreement and controls

Program Administration

 Determine how the program will be managed, reviewed and updated. First two years should have more frequency



Develop and Implement: Agreement Updates





Develop and Implement: Cybersecurity Controls

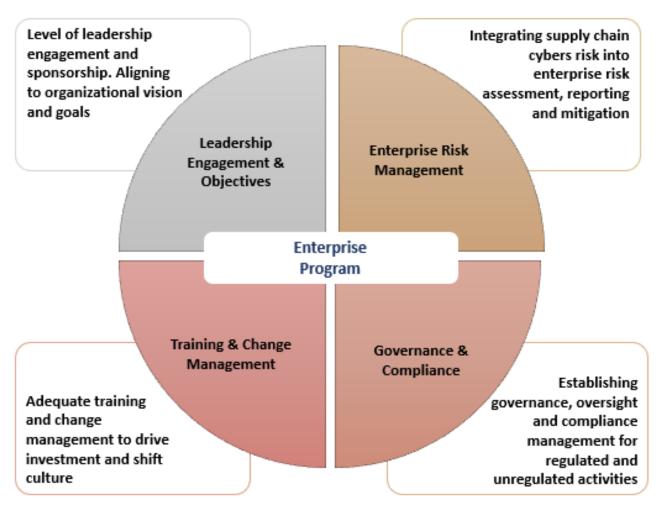


NERC CIP COMPLIANCE

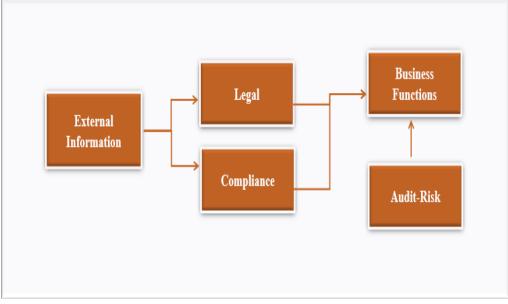
- Assess program and all cyber controls after security updates for NERC CIP implications
- Identify any substantive control gaps and applicability to CIP assets
- Integrate updates as you implement your program updates
- Ensure governance and compliance updates to account for new controls/program changes
- Quality Assurance



Develop and Implement: Enterprise Program



Managing Regulatory Change





Conclusion







