2020 | THE ACADEMY Public Power Connect
Virtual Summit & Business Meeting

Securing Your Supply Chain

Designing and Implementing Supply Chain Security Programs

Shari Gribbin
CNK Solutions Corp

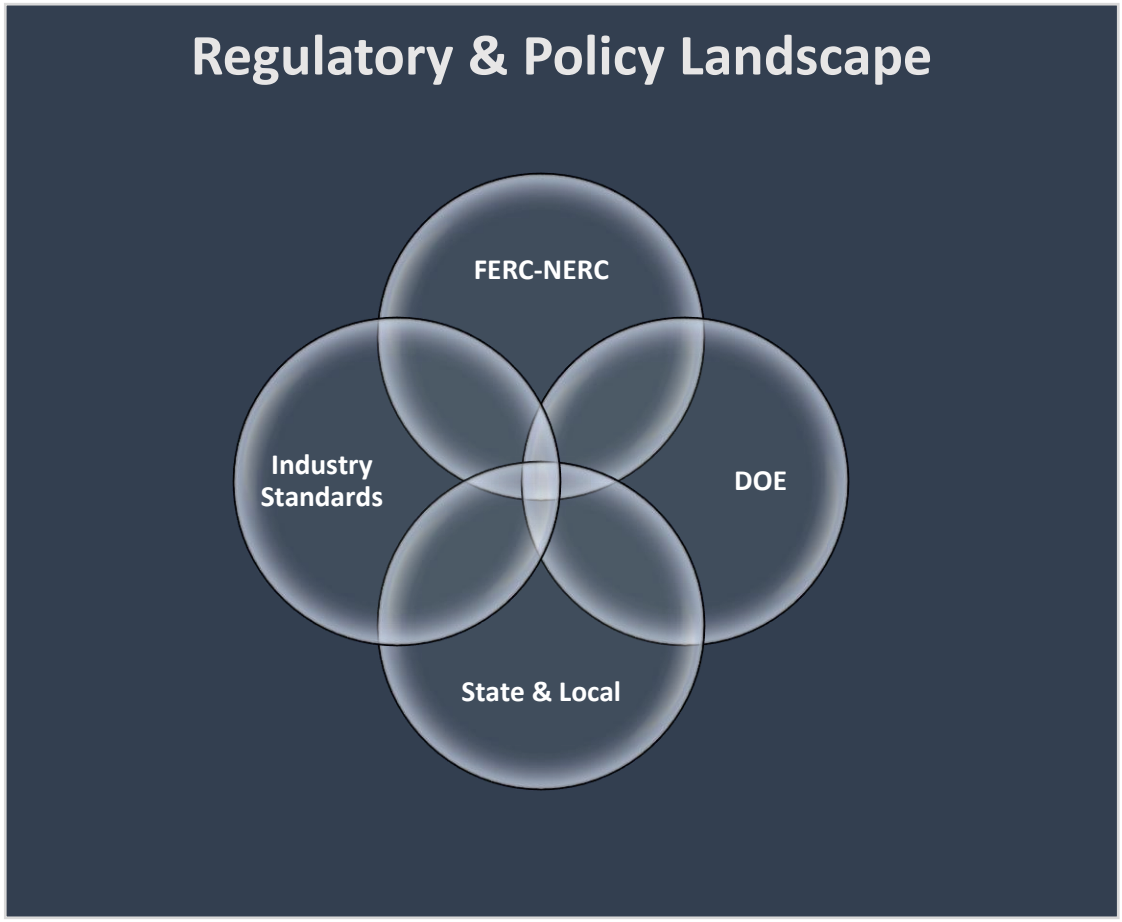
80 YEARS OF POWERING STRONG COMMUNITIES

AMERICAN PUBLIC POWER ASSOCIATION

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

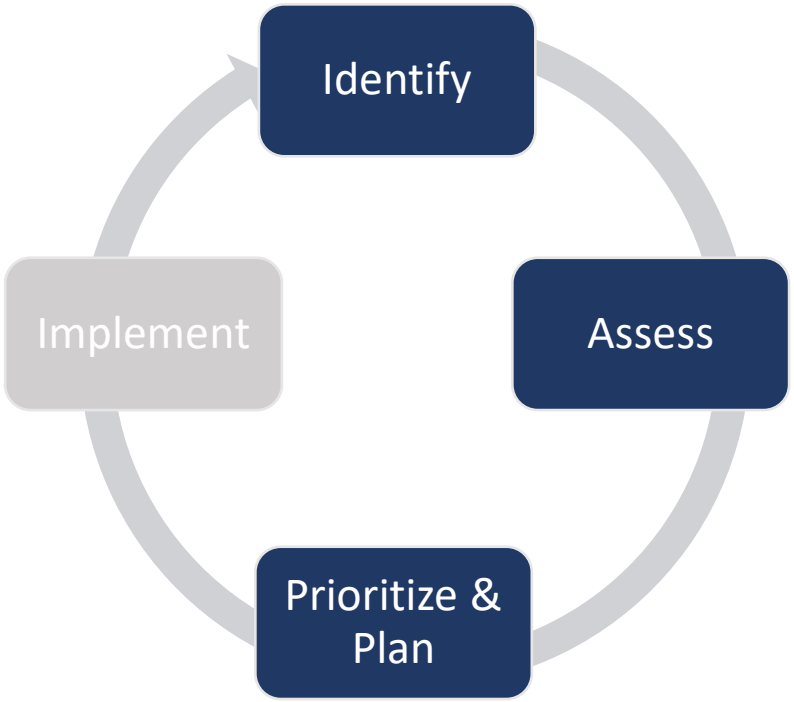
- Procurement Processes
- Inadequate Contract Terms
- Organizational Silos
- Vendor Security Failures
- Inventory Gaps
- Poor Training
- Remote Access
- Weak QA Controls

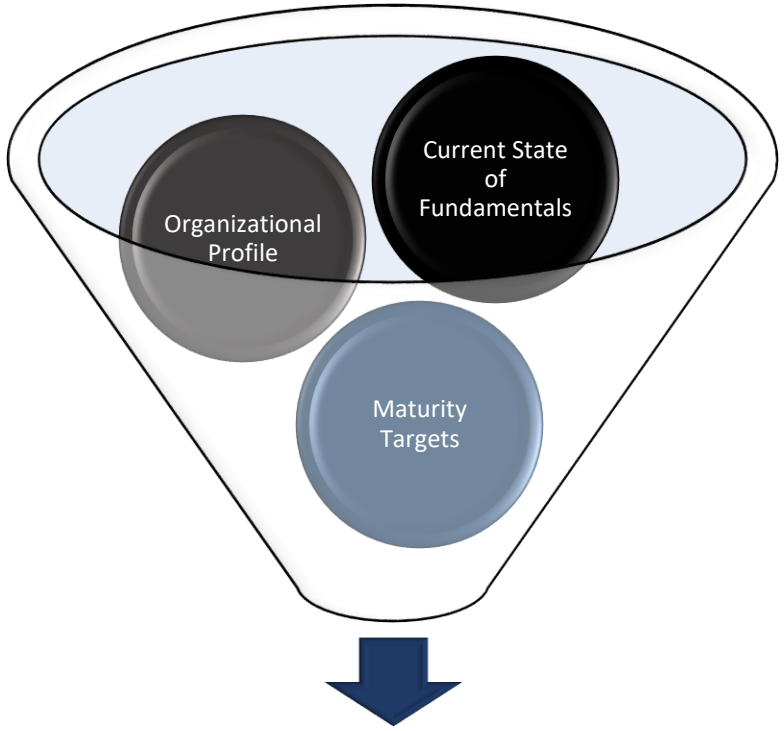
Core NERC CIP Supply Chain Requirements

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

Defining the Foundation





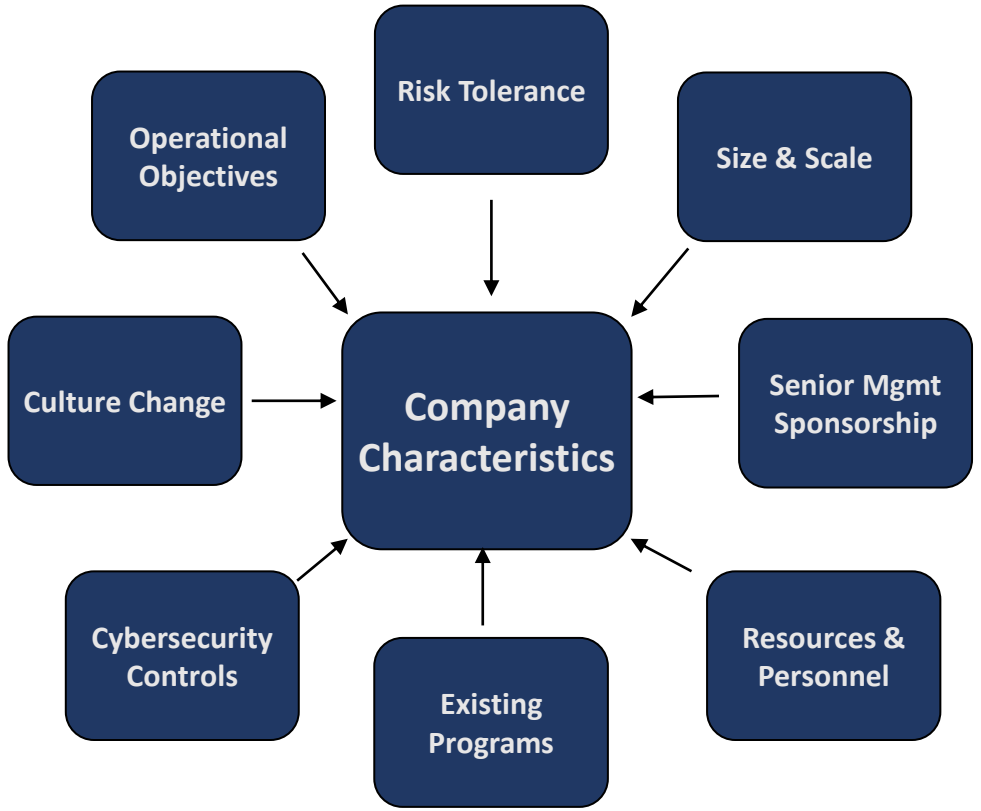
Develop & Implement

Defining the Foundation: Identify & Assess

Develop an Organizational Profile

Cyber Supply Chain Security Risks

- Vendor Cybersecurity
- Software Risks
- Vendor Access
- Compromised Supply Chain
- Third Party Hosting



Defining the Foundation: Identify & Assess

Understanding Current State

Supply Chain

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

Cybersecurity

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

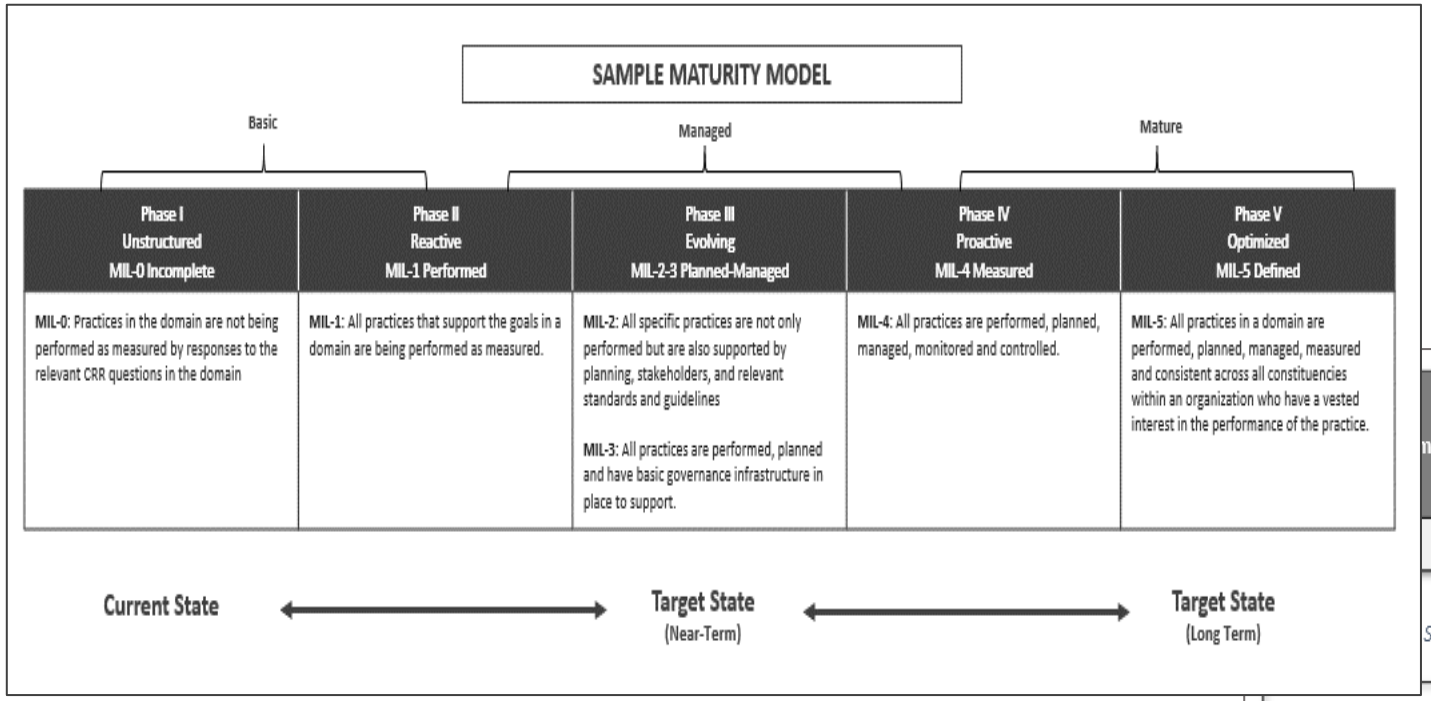
Enterprise

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

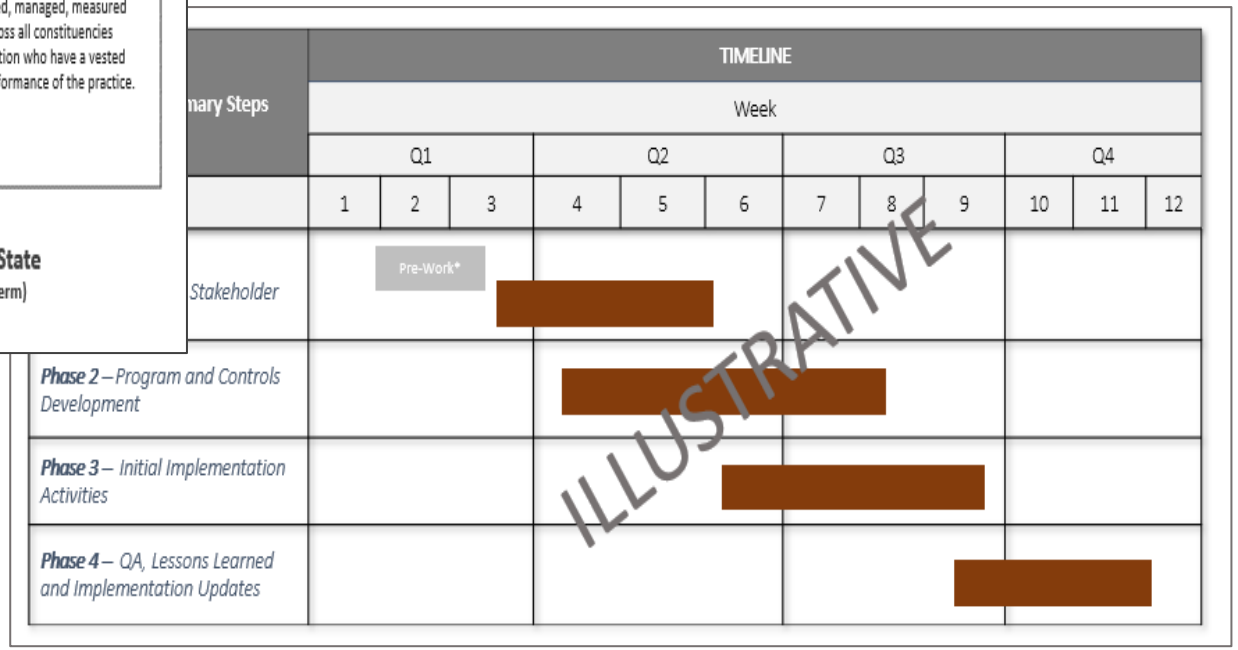
Tools and Technology

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

Defining the Foundation: Maturity Targets

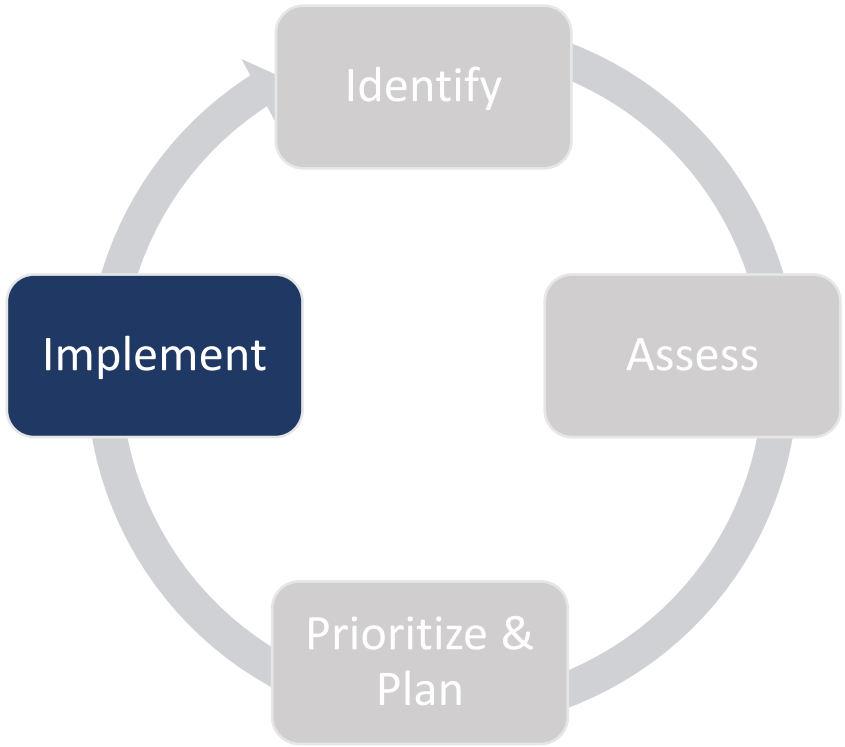


Prioritize and Plan



Develop and Implement

Develop and Implement: Risk Assessment

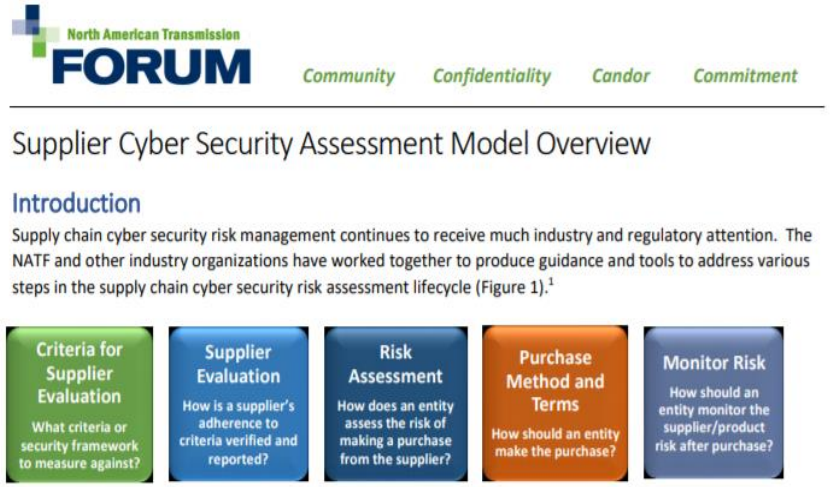


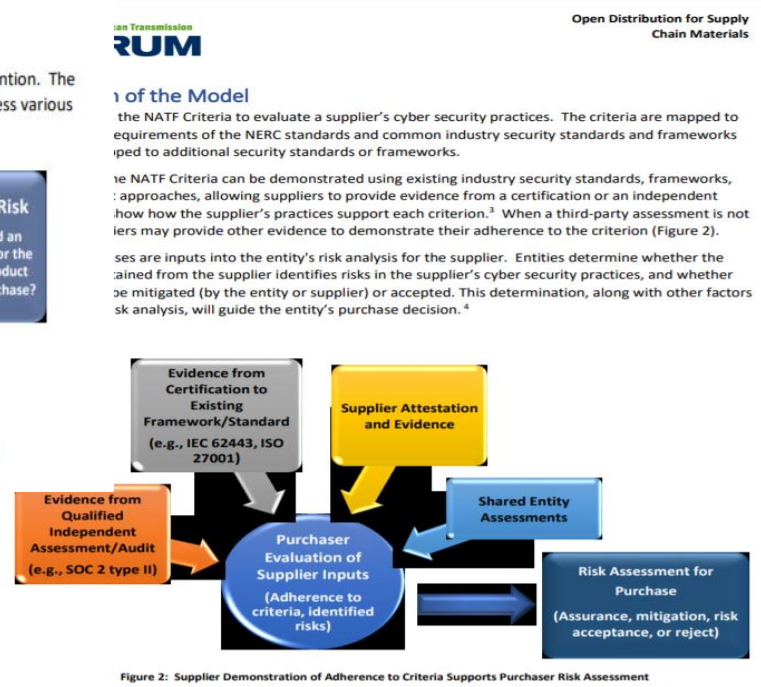
Develop a Baseline and Risk Assess

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





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	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.
Program Documentation	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.
Definitions & Key Concepts	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 & Responsibilities	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

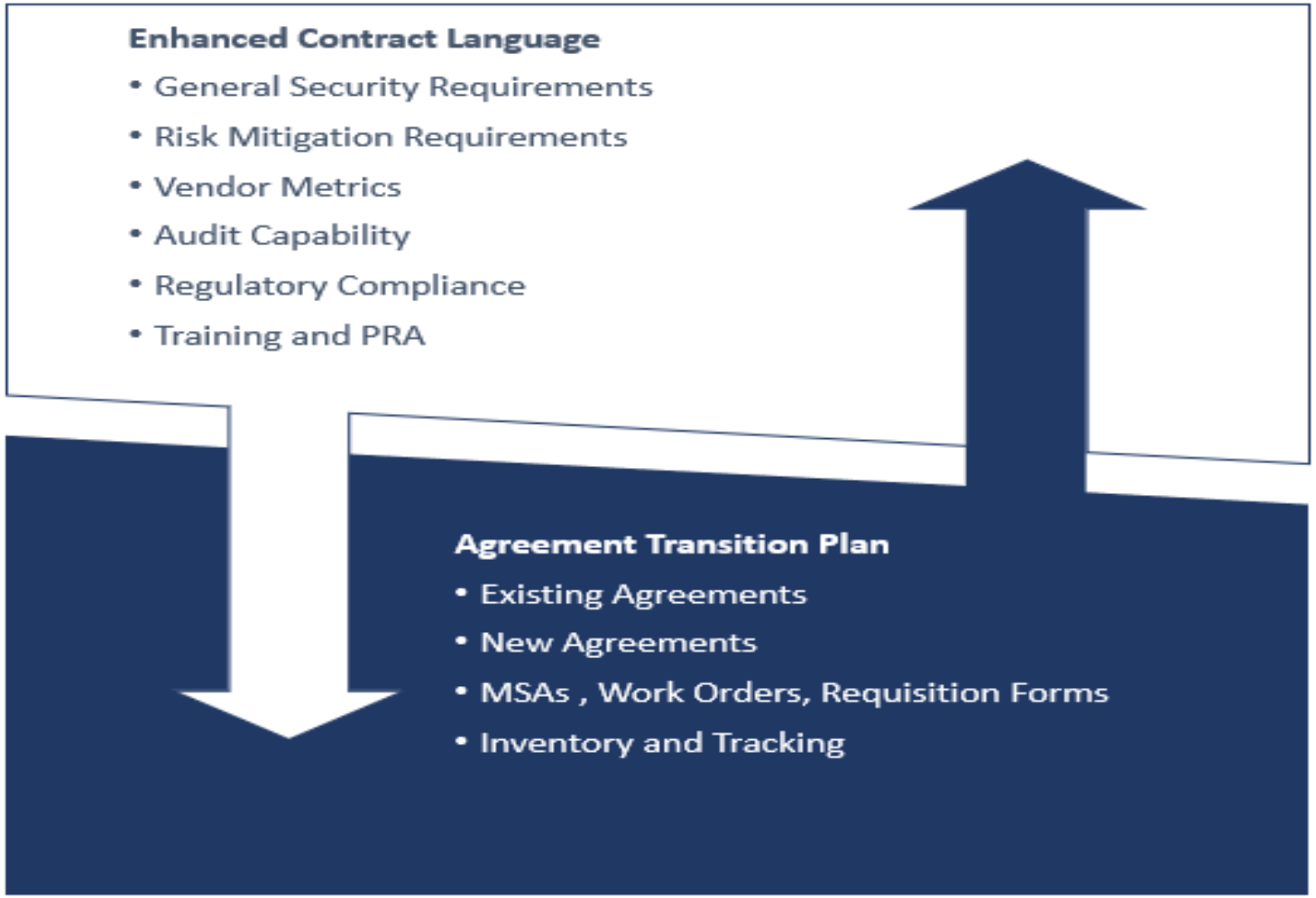
Information Sharing
- Standards for information protection, data integrity and compliance requirements

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



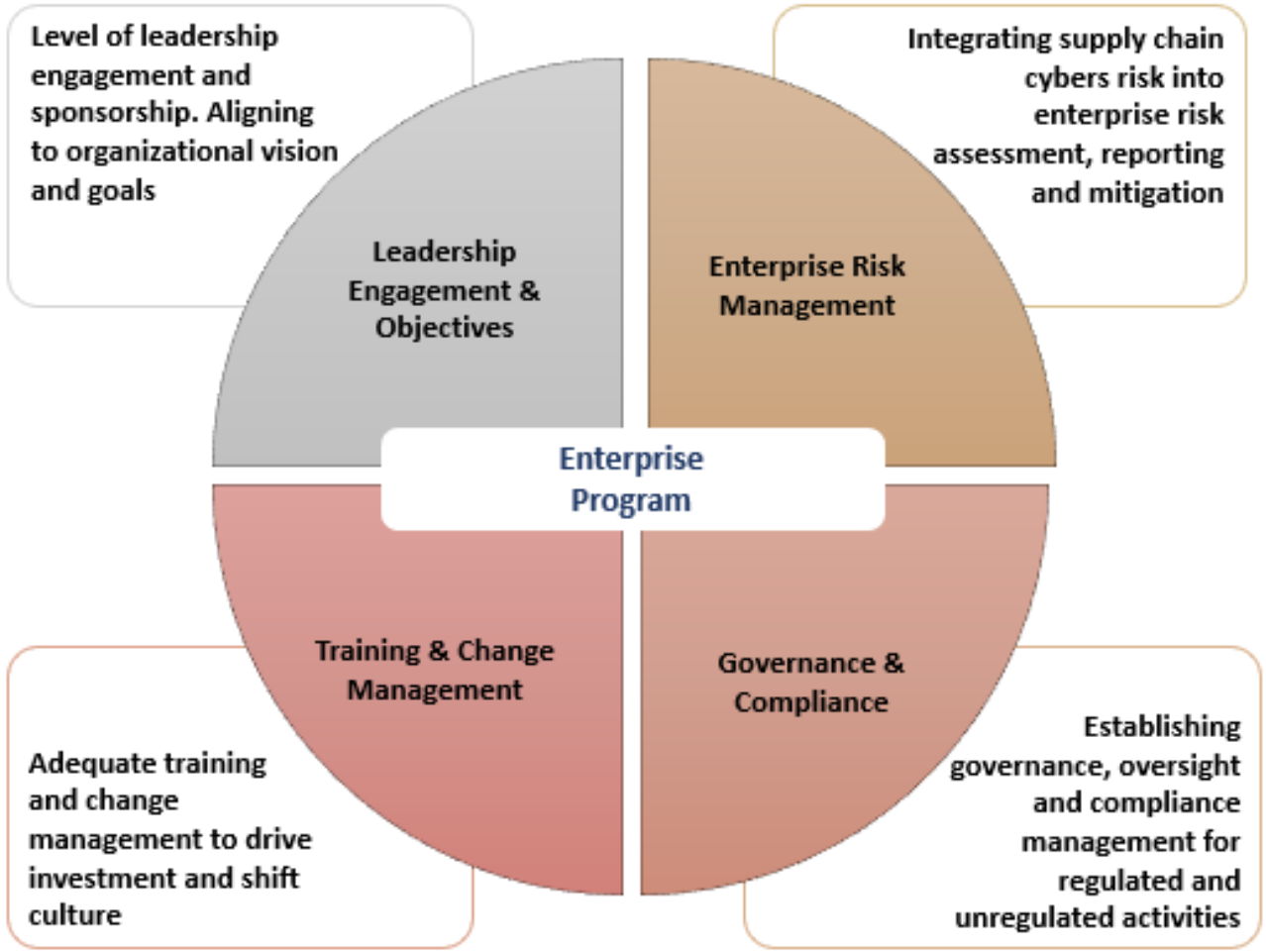
Develop and Implement: Cybersecurity Controls

NERC CIP COMPLIANCE

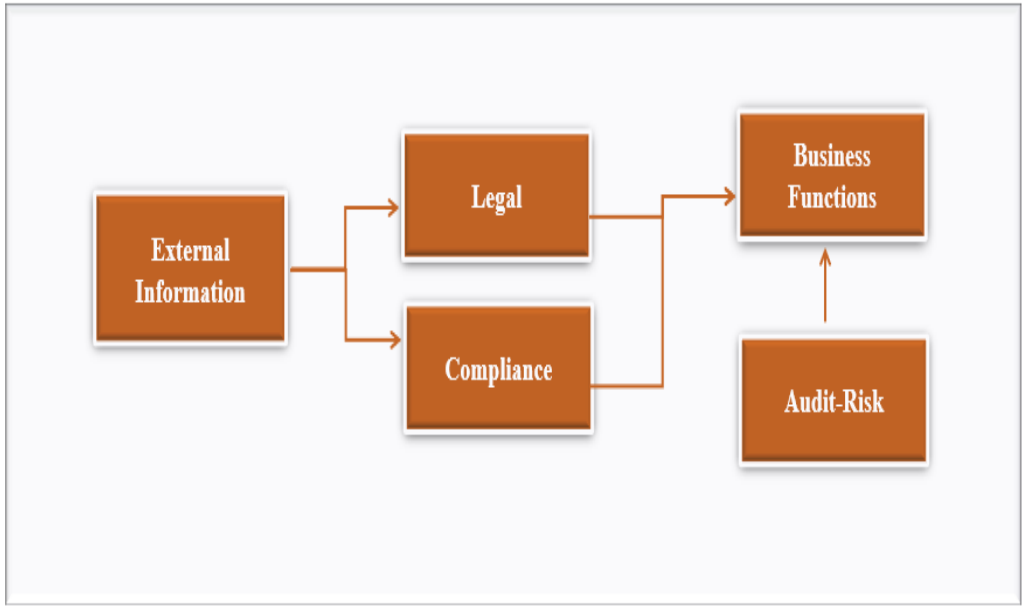
- Assess program and all cyber controls after security updates for NERC CIP implications
- Identify any substantive control gaps and applicability to CIP assets
- Integrate updates as you implement your program updates
- Ensure governance and compliance updates to account for new controls/program changes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

Cybersecurity Controls

Develop and Implement: Enterprise Program



Managing Regulatory Change



Conclusion

Thank You