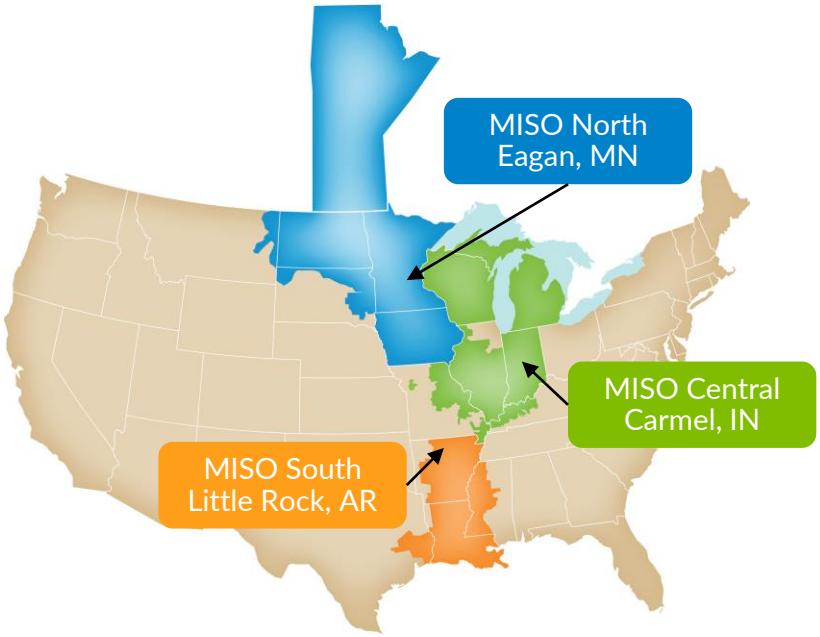
Leveraging Procurement for Cybersecurity Resilience

Prepared for the U.S. Agency for International Development

April 25, 2024

MISO Overview

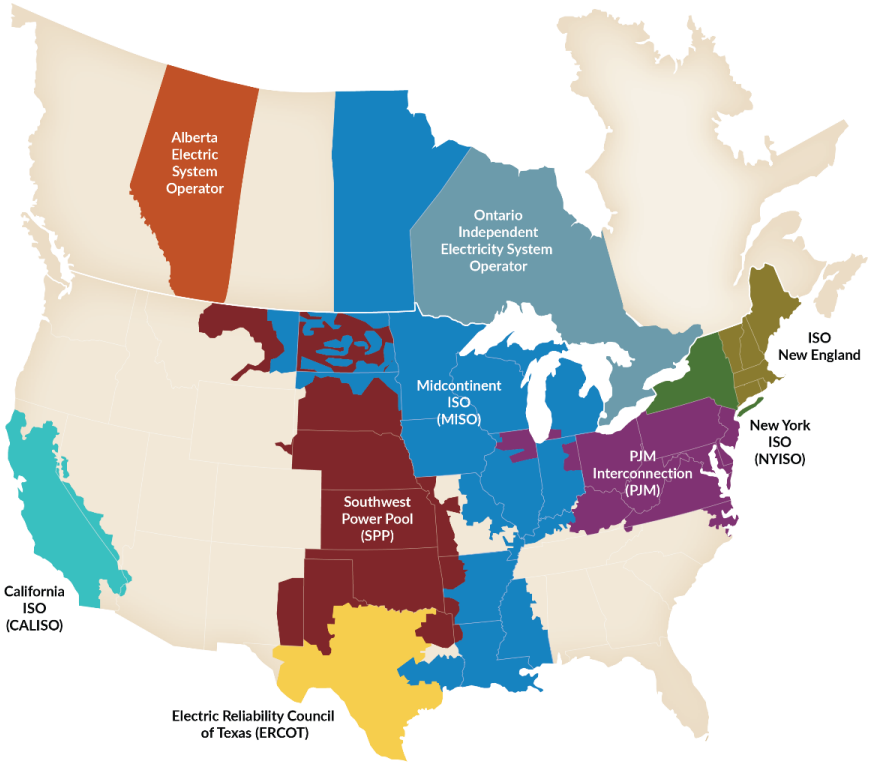


MISO's reliability footprint and regional control center locations

MISO KEY FACTS

Area Served	15 U.S. States and Manitoba, Canada
Population Served	45 Million
Transmission Line	75,000 Miles
Generating Units*	> 2,900
Record Demand	127.1 GW 7/20/2011
Wind Peak	25.6 GW 1/12/2024
Solar Peak	4.5 GW 2/19/2024
Members	54 Transmission Owners
	143 Non-transmission Owners
Market Participants	> 500
Market Transactions	> $40 billion
Carbon Reduction	Approximately 32% since 2014

MISO has the largest geographical footprint of all Regional Transmission and Independent System Operators in North America



MISO's role as a grid operator is similar to the role of an air traffic controller

- Air traffic controllers manage the movement of planes from point A to point B safely and reliably 24/7/365
- Air traffic controllers don’t own the airplanes, the runways, or the terminals

- MISO operators manage the movement of electricity from where it is generated to the local utilities safely and reliably 24/7/365
- MISO doesn’t own the generators, the transmission lines, or any part of the electric grid

Electric Industry Regulators

- **State Public Service Commissions**
  - Adopt and enforce regulations that protect the public's safety and interests, including regulating electricity rates
  - Appointed by Governor or elected
- **Federal Energy Regulatory Commission (FERC)**
  - Congress authorizes FERC to regulate interstate transmission of electricity, oil, and natural gas
- **North American Reliability Corporation (NERC)**
  - FERC authorizes NERC to set and enforce electric reliability standards

Procurement and Cybersecurity

Executive Summary

- Early evaluation and management of key vendors is important to ensure they meet expectations
- Assert established frameworks as global industry standards to ensure reliability
- Consider leveraging independent third-party assessments of vendor risk and quality
- Negotiate and escalate

The Fundamentals – Who, When, What and How

Who

Business area, supply management, IT and legal

When

Establish early expectation to avoid additional cost later

What

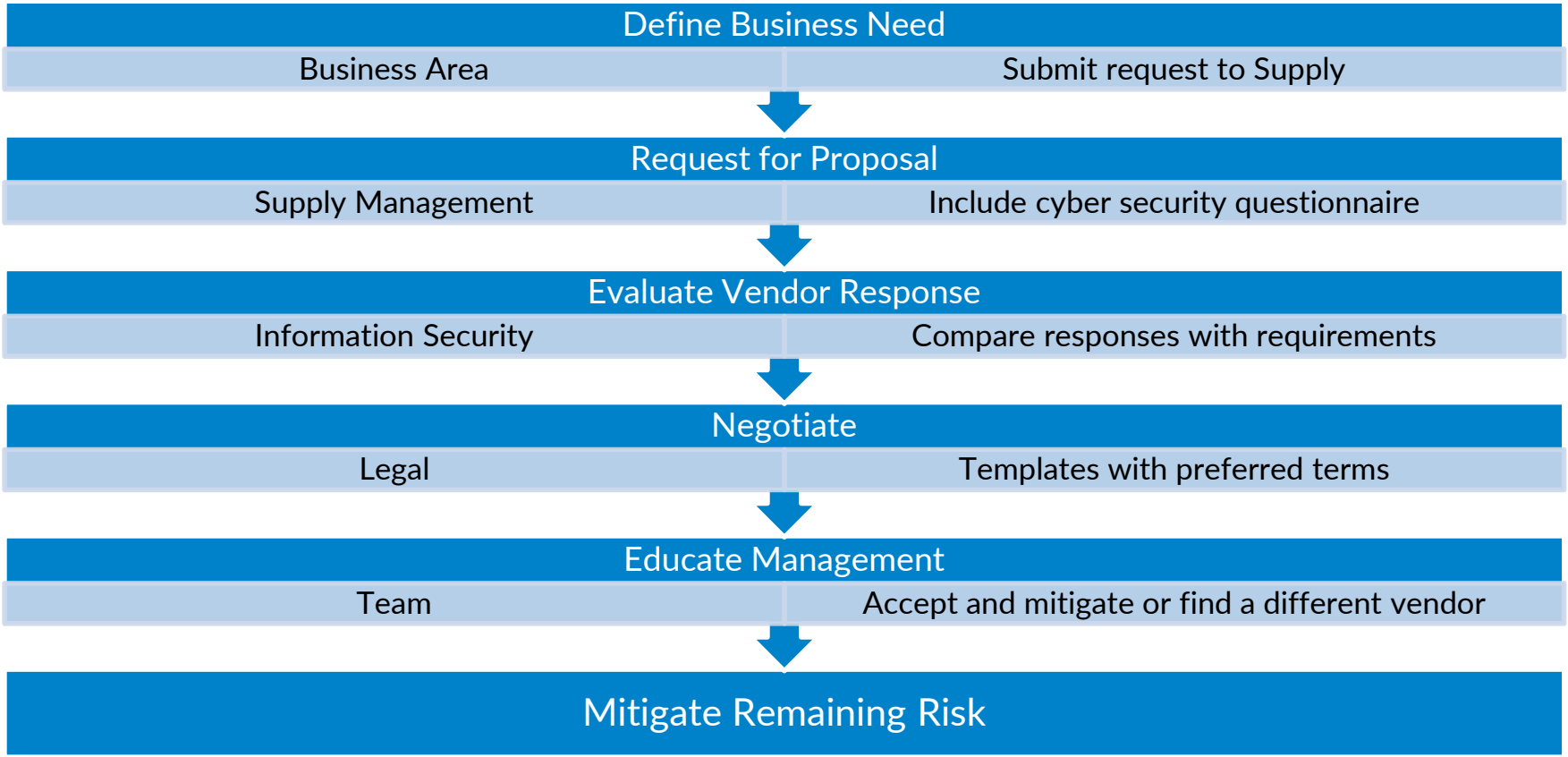
Assessment questionnaire

How

Identify critical and non-critical:

- Rate: Low, Moderate, High
- Educate, mitigate and act

General Process



Plan and manage key vendors to ensure they are meeting security expectations

EVALUATION ATTRIBUTES
Partnership
Security
Schedule
Quality
Cost

- **Plan**:
  - Include requirements in RFP and negotiate contractual terms to ensure alignment with security objectives and performance, including a review of the vendor's security and risk posture
- **Manage**:
  - Include terms that permit audits controls.
  - Evaluate various attributes

Leverage independent third-party assessments of vendor risk and quality

Government Partnership	Develops guidance, frameworks, and regulations that can be used to require compliance
Risk Assessment Vendor	Provides independent industry assessments and ratings of vendor offerings to evaluate their strengths and manage risks
Risk Monitoring Vendor	Helps organizations manage cybersecurity risk by continuously monitoring, assessing and reducing vendor risk

Leverage and assert established frameworks as global baselines for security

- NIST Cyber Security Framework
- ISO/IEC 27001
- Cybersecurity Capability Maturity Model
- European Union Agency for Cybersecurity (ENISA) Frameworks
- Center for Internet Security (CIS) Controls
- North American Transmission Forum (NATF):

  Supply Chain Security Assessment Model

  Energy Sector Supply Chain Risk Questionnaire

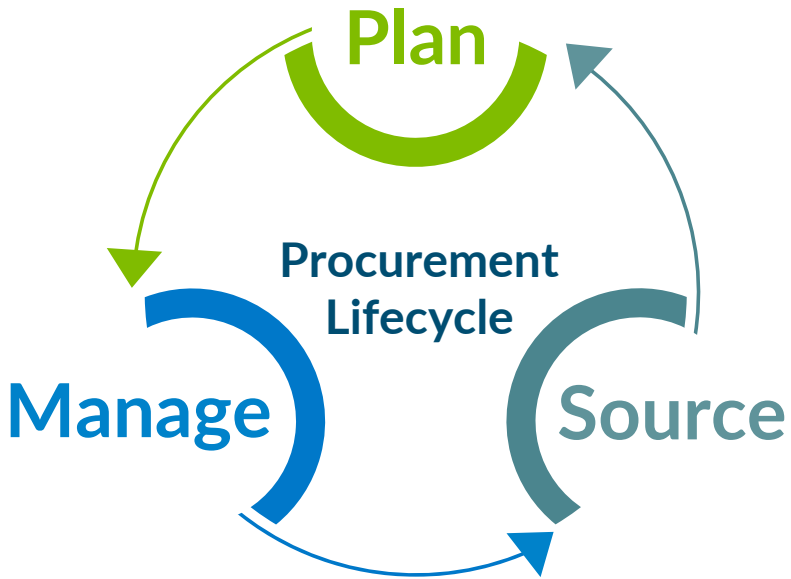
  Supplier List - Suppliers with NATF Criteria and Questionnaire Responses Available

Develop Negotiation Levers and Strategy

- Engage leadership and gain support for security as a priority
- Upfront cost may increase but damages later can greatly exceed start-up
- Reliability, financial and reputation
- Challenge suppliers that disclaim or minimize liability
- Emphasize mutual benefit and partnership
- Provide examples of failures
- Be open to alternatives
- Offer incentives
- Work with regulators

Three Phase Lifecycle

- Plan requirements in advance
- Establish eligibility criteria for suppliers
- Conduct risk assessment
- Identify threats
- Segregate network



- Service Level Agreements
- Lessons learned
- Secure disposal

- Provide cybersecurity training
- Involve supplier in incident management
- Organize maintenance operations
- Secure remote access
- Require patch

Vendor relationships help MISO quickly react to cybersecurity incidents

The vulnerability management process is used to continuously mitigate and remediate product vulnerabilities

Vulnerability

Threat

Risk