Disclaimer

The Midwest Reliability Organization (MRO) Compliance Monitoring and Enforcement Program Advisory Council (CMEPAC) is committed to providing training and non-binding guidance to industry stakeholders regarding existing and emerging security topics. Subject Matter Experts (SMEs) developed any materials, including presentations, through the MRO CMEPAC from member organizations within the MRO Region and other government and industry security experts. The views in this presentation are presented by these MRO CMEPAC SMEs, government, and industry experts, and do not express the opinions and views of MRO.

Supply Chain Risk Management Program

"A security perspective fosters compliance"

Reason For Brief

- MPC completed 2022 MRO Audit
- Program took different perspective than others requiring explanation
- Audit team appreciated MPC's efforts: Requested we explain our process & note areas where some plans fall short

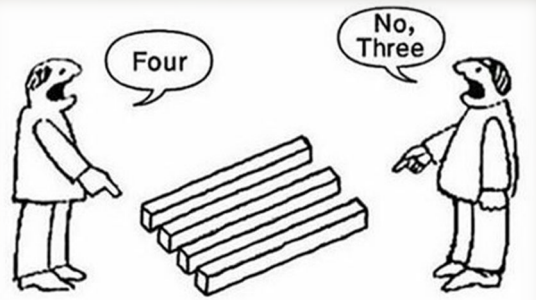

Fig 1. Perspective. Retrieved from https://rentapress.com/images/uploaded/3v4_disagreement.jpeg

MPC's CIP-013 Fast Facts

- MPC employs 390 people, 2 High-, 6 Medium- & 35 Low-Impact cyber systems
- Created Risk Assessment Working Group (RAWG): ~10 people as cross section of MPC
- Did not hire outside assistance or additional personnel

Defined Risk to MPC

- Kept things simple for corporate buy-in
- Single risk: Threat of malicious code
- Goal to expand program in future, not to just meet short-term compliance
- Treated Low-Impact same as higher systems

Vendor & Risk List

- Listed all potential vendors used across cyber systems, assessed 62
- Included TCAs, inventory, patches & freeware
- After defining applicability, larger list pared down to ~35 in-scope vendors

Supply Chain Risk Mgmt Program

- Did not want an overwhelming program doc
- Broke into 4 parts:
  1. Assessment Tools
  2. Risk Identification Methodology
  3. Supply Chain Risk Management Plan
  4. Guideline

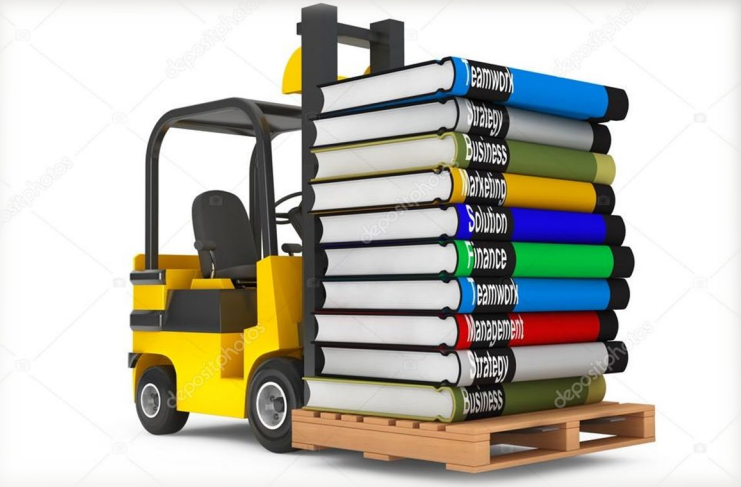

Fig 2. Forklift w/books. Retrieved from https://st2.depositphotos.com/1187563/7129/i/950/d…5813-stock-photo-forklift-with-stack-of-books.jpg

1. MPC's Assessment Tools

- Built tools to assess/document vendor risk
  a. Vendor Questionnaire
  b. Vendor Assessment Workbook
  c. CIP-013 Cybersecurity Contract Addendum

a. Tools- Questionnaire

- Vendor Questionnaire- Called VQ
- Fillable form w/under 45 questions
- Main focus is malicious code risk

b. Tools- Vendor Workbook

- Consolidates all vendor assessment data, including risks and mitigations
- Main tool used by everyone procuring something

Vendor Risk Summary

- Located in Vendor Assessment Workbook
- Summary of how vendor is used by MPC
- Provides brief info on overall risk to BES
- Fosters understanding by anyone in company

Fig 3. Word Collage. Retrieved from https://tbgsecurity.com/wordpress/wp-content/uploads/2020/10/vendor-risk-management-538x218.jpeg

c. Tools- Cybersecurity Addendum

- Not all vendors use/require contracts
- Addendum document treated as an additional mitigation tool
- Addresses all of R1.2 requirements
- All addendum items mapped to questionnaire & mitigations

2. Risk Identification Methodology

- CIP-013 allowed a lot of latitude: How to efficiently narrow the focus?
- Methodology explains how MPC defined risk
- Aligned our tools with NATF checklist & documented MPC rationale for each question
- Philosophy: Leverage security & reliability best practices = inherently meets compliance

3. Risk Management Plan

- Affectionately called SCRiMP
- Directly addresses all CIP-013 requirements
- Defines what a “procurement” is

MPC's Procurement Definition

- Procure means to get possession of something; to obtain by particular care and effort. A procurement may or may not involve the exchange of money. Therefore, this plan must be followed for applicable procurements made by any means, including but not limited to the following:
  - -Requisitions/Purchase orders
  - -Auto-Generated Inventory Replenishment
  - -Loans, Trades and Freeware
  - -Credit Card Purchases
  - -Vendor Transitions
  - -Emergency Procurements

Procurement Applicability

- For each of previous procurement types, explain when the plan is applied which defines the start point
- Focus is needed on: vendor transfers, renewal agreements, extensions, and/or service subscriptions
- All interactions with vendor treated like procurement

Emergency Procurements

- Process should be scalable and applicable in “emergencies”
- Simply assess vendor with public info to understand risk & assign mitigations
- Document these actions in plan

Fig 4. Emergency Exit. Retrieved from https://images.smartsign.com/img/sm/S/fire-no-emergency-exit-sign-s-1518.png

4. Guideline

- A detailed “living” document for anyone involved in Procurement processes
- Includes anyone involved in mitigations:
  -Warehouse personnel
  -Patch managers
  -Supervisors & more

Focus On Residual Risk

- All vendors have inherent risk, so what risks can we minimize?
- All residual risk then requires mitigation

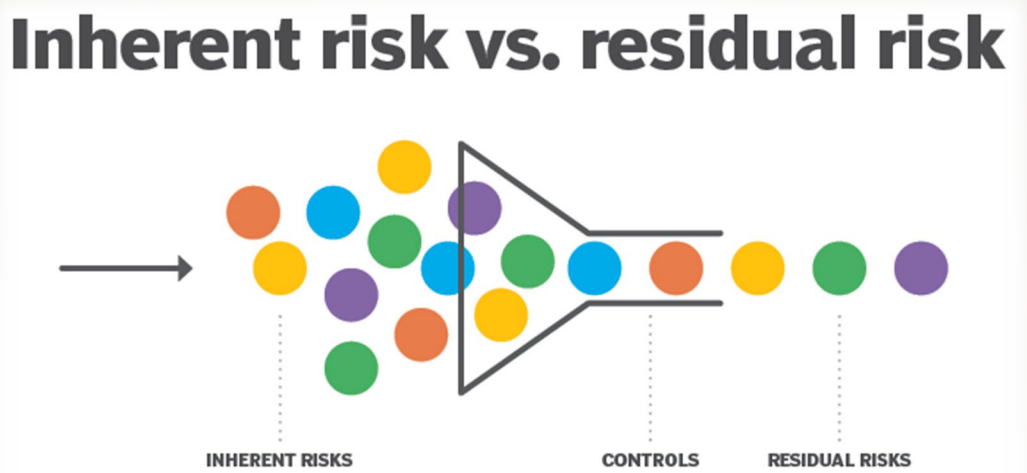

Fig 5. Risk Funnel. Retrieved from https://cdn.ttgtmedia.com/rms/onlineimages/inherent_risk_vs_residual_risk-f.png

Risk Mitigation

- VQ questions have pick list of mitigations based on MPC processes
- All 4 & 5 risk scores (out of 5) are assigned mitigations
- Procurement process requires that mitigations are reviewed before purchase

Internal Controls

- Integrate Supply Chain Risk Management into corporate procedure
- Living process requires rebalance
- Created recurring internal controls
  - -CIP-013 triggers in Procurement system
  - -Annual mitigation pick list review with SME's
  - -Forecast for 3-yr vendor reassessment dates
  - -Periodic training & document reviews

Fig 6. Risk Balance. Retrieved from https://www.corporatecomplianceinsights.com/wp-content/uploads/2020/01/risk-blocks.jpg

Summary

- High level info: specifically left out a lot of program details
- Focused on potential weak areas MRO has noted in past audits
- Ideas easily integrated into any program:
  - -Risk Summaries for vendors
  - -Apply process to similar low impact vendors & TCAs
  - -Internal Controls for reassessments

MPC Supply Chain Risk Contact

- Bob Foote
  Substation CIP Compliance & Cybersecurity
  CIP-013 RAWG Chair
  (701) 795-4338
  rfoote@minnkota.com