MIDWEST RELIABILITY ORGANIZATION

# MRO SAC to Host Upcoming Webinar on Supply Chain Effectiveness Survey Results

Tony Eddleman, Director of NERC Reliability Compliance, Nebraska Public Power District, MRO SAC Member

Jason Nations, Director of Enterprise Security, Oklahoma Gas and Electric Corp., MRO SAC Member

April 12, 2022

# Disclaimer

**Midwest Reliability Organization (MRO) is committed to providing outreach, training, and non-binding guidance to industry stakeholders on important industry topics. Subject Matter Experts (SMEs) from MRO's organizational groups and the industry may develop materials, including presentations, provided as a part of the event. The views expressed in the event materials are those of the SMEs and do not necessarily express the opinions and views of MRO.**

# MRO SAC/SACTF Tentative 2022 Meetings and Events

- **SAC**
  - Quarter 2 OGOC Joint Meeting on **June 22, 2022**
  - Security Technical Training on **October 4, 2022**
  - Security Conference on **October 5, 2022**
  - Quarter 4 Meeting on **November 9, 2022**
- **SACTF:**
  - Threat Call at 8:15 a.m. on Wednesday Mornings
  - Webinar on ICS/OT Year in Review held on **April 15, 2022**

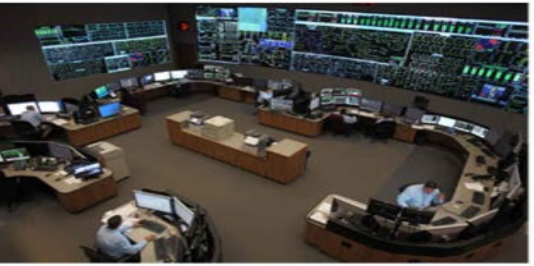
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Supply Chain Working Group

## Supply Chain Effectiveness Survey

Tony Eddleman, NPPD and SCWG Chair
Reliability and Security Technical Committee
March 8-9, 2022

RELIABILITY | RESILIENCE | SECURITY

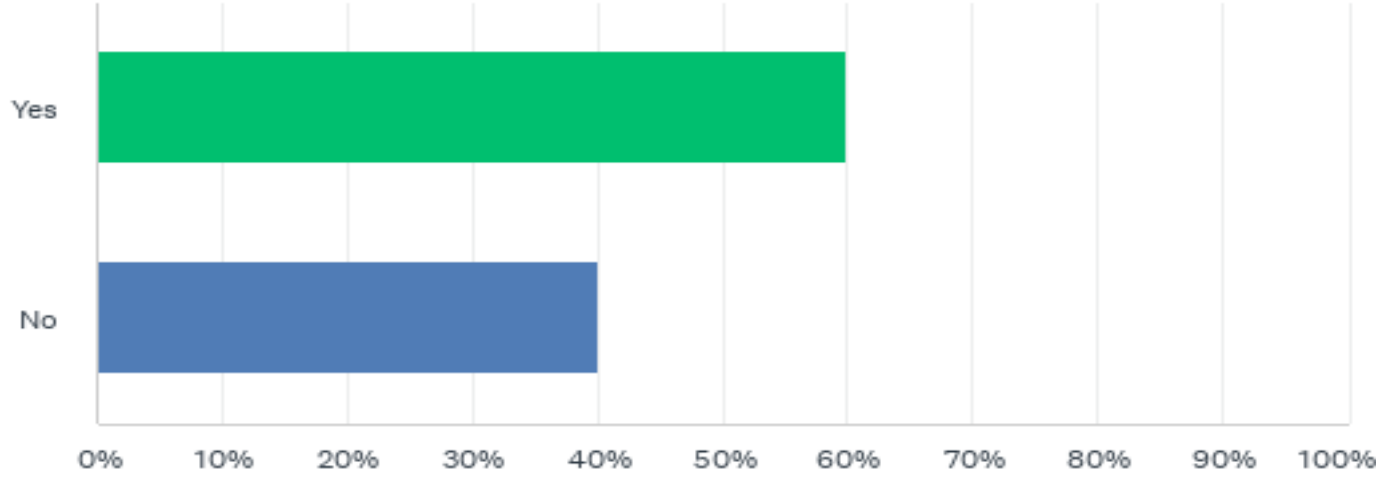



# Survey Overview

- 201 total responses
  - Eleven (11) responders did not select any responses nor provide any comments
  - The survey was sent to approximately 900 compliance contacts at Registered Entities and requested their voluntary response
- Survey responses came from the United States, Canada, and Mexico
  - Responses also came from all six NERC Regions
- Majority of 190 responses, 60% (114), selected NERC Supply Chain Risk Management (SCRM) Reliability Standards applicable to them as Registered Entities.
- Responders provided very good comments which have been incorporated into key take-aways and conclusions.
- Survey was conducted through SurveyMonkey

## Q2: Are the NERC Supply Chain Risk Management (SCRM) Reliability Standards applicable to you as a registered entity?

- Answered: 190 Skipped: 11



## Q2: Are the NERC Supply Chain Risk Management (SCRM) Reliability Standards applicable to you as a registered entity?

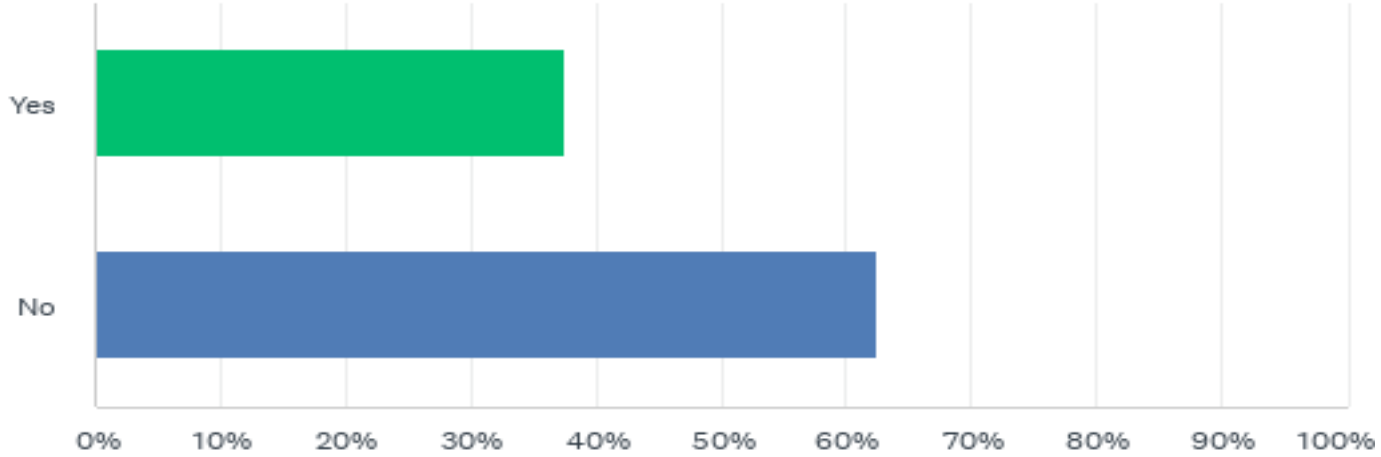
- Answered: 190 Skipped: 11

| ANSWER CHOICES | RESPONSES | |
|---|---|---|
| Yes | 60.00% | 114 |
| No | 40.00% | 76 |
| TOTAL | | 190 |

**SCRM Reliability Standards <u>are not</u> applicable to you as a registered entity:**

**Q3: Are you applying the SCRM principles from the SCRM standards to your operational, business and/or contract language?**

- Answered: 64 Skipped: 137



**SCRM Reliability Standards are not applicable to you as a registered entity:**

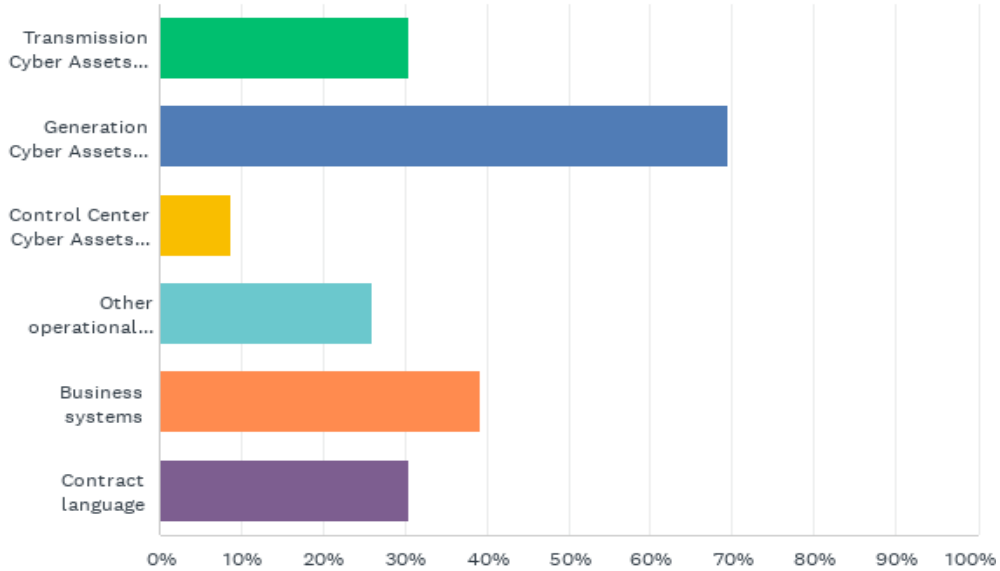
**Q3: Are you applying the SCRM principles from the SCRM standards to your operational, business and/or contract language?**

- Answered: 64 Skipped: 137

| ANSWER CHOICES | RESPONSES | |
|---|---|---|
| Yes | 37.50% | 24 |
| No | 62.50% | 40 |
| TOTAL | | 64 |

**SCRM Reliability Standards <u>are not</u> applicable to you as a registered entity:**
**<u>Selected yes</u>: you are applying the SCRM principles from the SCRM standards**
**Q4: check all that apply:**

- Answered: 23 Skipped: 178



**SCRM Reliability Standards <u>are not</u> applicable to you as a registered entity:**
**<u>Selected yes</u>: you are applying the SCRM principles from the SCRM standards**
**Q4: check all that apply:**

- Answered: 23 Skipped: 178

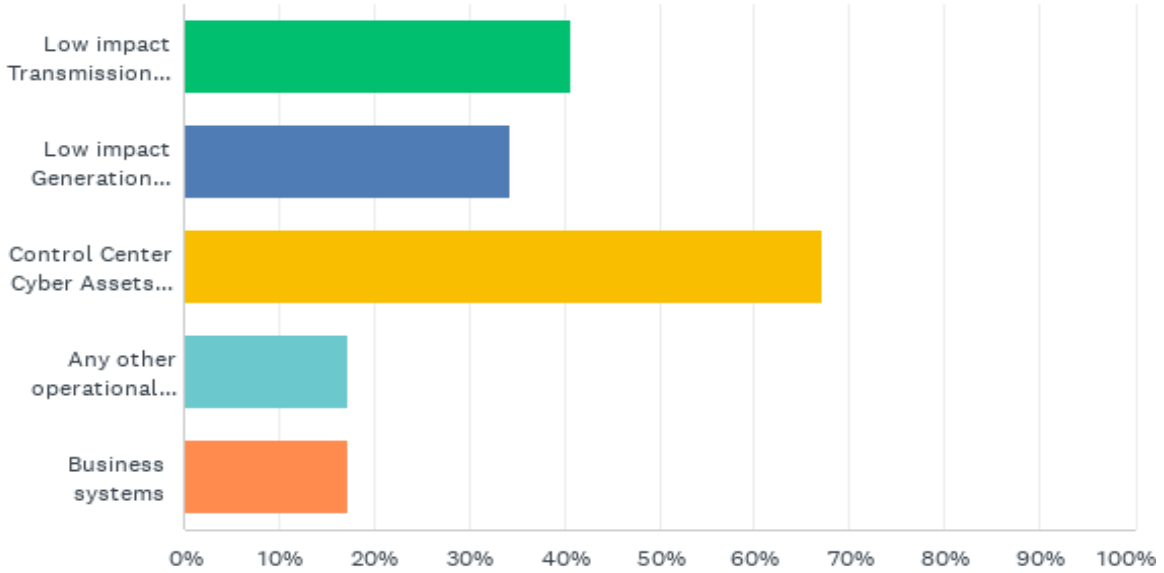
| ANSWER CHOICES | RESPONSES | |
|---|---|---|
| Transmission Cyber Assets and/or services | 30.43% | 7 |
| Generation Cyber Assets and/or services | 69.57% | 16 |
| Control Center Cyber Assets and/or services | 8.70% | 2 |
| Other operational systems | 26.09% | 6 |
| Business systems | 39.13% | 9 |
| Contract language | 30.43% | 7 |
| Total Respondents: 23 | | |

# Key take-aways and conclusions

- Of the 64 respondents that indicate the SCRM requirements are not applicable to their entity, 24 responders are applying the SCRM principles from the SCRM standards to their operational, business, and/or contract language.
- Standards have been a good basis to determine what is needed if entity was to have a formal NERC program.
- **Conclusion:** The SCRM requirements are relatively new, but some entities that don't have compliance requirements are using the requirements to develop programs.

**SCRM Reliability Standards <u>are</u> applicable to you as a registered entity:**
**Q5: In addition to required scope (High and Medium Impact assets) are you applying the SCRM principles from the standards to: (Check all that apply)**

- Answered: 64 Skipped: 137



**SCRM Reliability Standards <u>are</u> applicable to you as a registered entity:**
**Q5: In addition to required scope (High and Medium Impact assets) are you applying the SCRM principles from the standards to: (Check all that apply)**

- Answered: 64 Skipped: 137

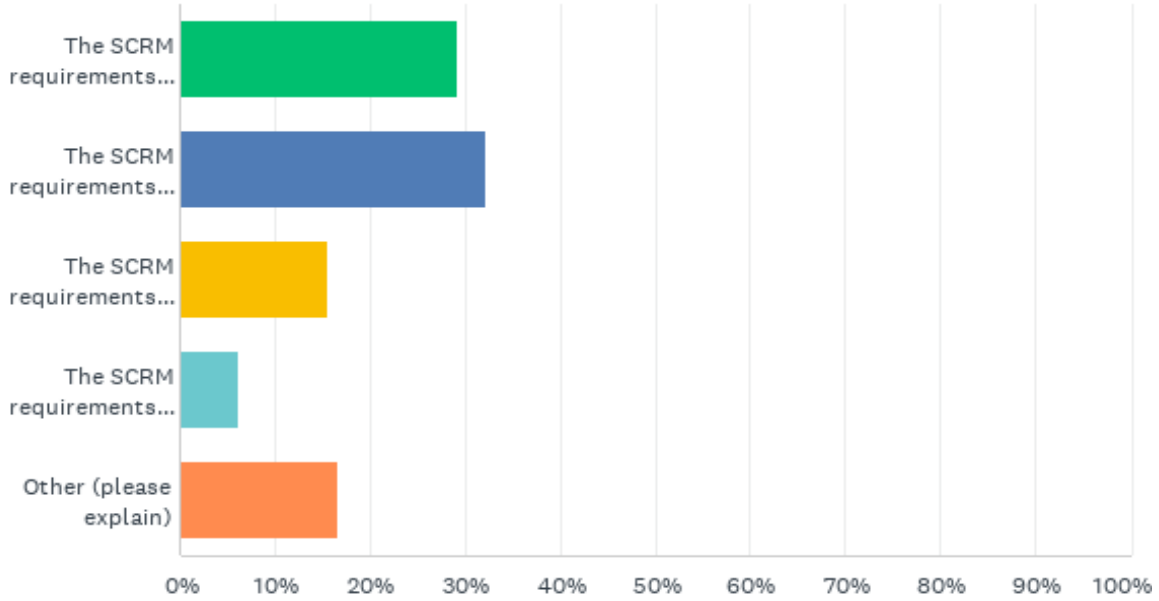
| ANSWER CHOICES | RESPONSES | |
|---|---|---|
| Low impact Transmission Cyber Assets and/or services? | 40.63% | 26 |
| Low impact Generation Cyber Assets and/or services? | 34.38% | 22 |
| Control Center Cyber Assets and/or services? | 67.19% | 43 |
| Any other operational systems? | 17.19% | 11 |
| Business systems | 17.19% | 11 |
| Total Respondents: 64 | | |

# Key take-aways and conclusions

- Of the 60% of respondents (114) that the SCRM requirements are applicable to them, over half (64) of the respondents are applying SCRM principles to some degree to cyber assets not in scope of the requirements.
  - Reasons are due to vendor overlap for High and Medium cyber assets or maintaining same SCRM program across the enterprise.
- Human effort resource constraints were identified as reasons responders cannot apply SCRM principles to low impact cyber assets.
- Once the supply chain process is more mature and the larger implications of the standard are better understood, some will evaluate implementing the SCRM principles in other areas.
- A few are using FISMA and NIST based supply chain programs.
  - A respondent stated that many of the FISMA requirements are overlapping with CIP requirements and are not cost effective to implement above what is required.
- **Conclusion:** Entities are generally working towards applying the SCRM requirements to other systems.

## Q6: Please select the statement that best describes your opinion regarding the clarity of the Supply Chain Risk Management (SCRM) requirements:

- Answered: 96 Skipped: 105



**Q6: Please select the statement that best describes your opinion regarding the clarity of the Supply Chain Risk Management (SCRM) requirements:**

- Answered: 96 Skipped: 105

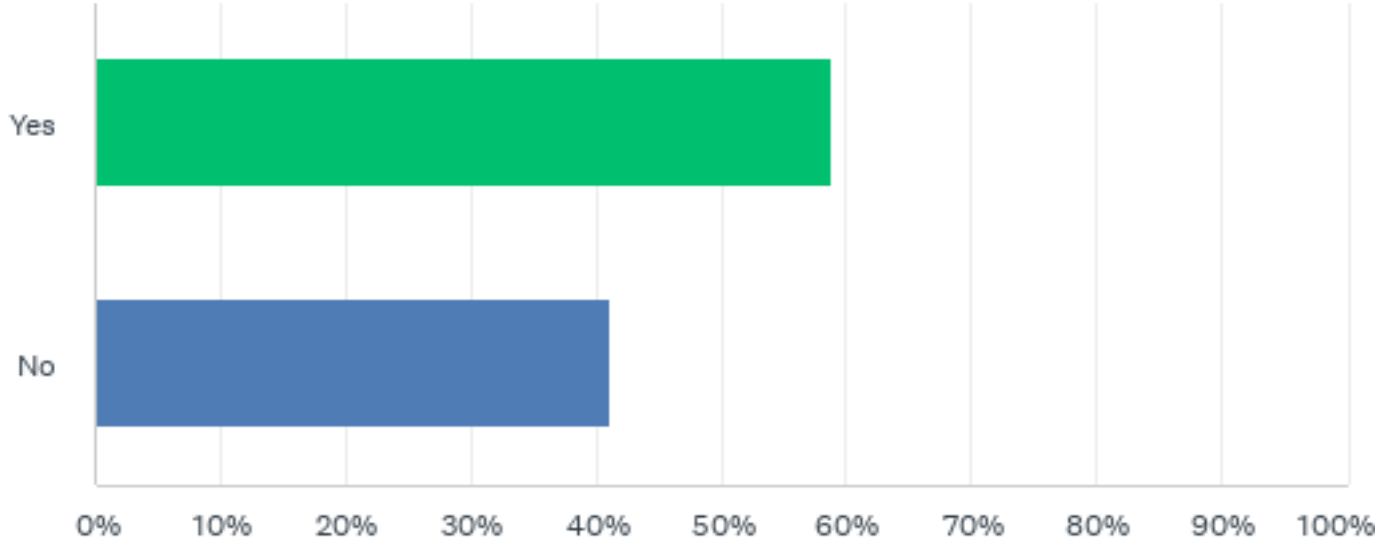
| ANSWER CHOICES | RESPONSES | |
|---|---|---|
| The SCRM requirements are clear. Our program is on track and our security objectives are being met. | 29.17% | 28 |
| The SCRM requirements are clear, however I am unsure of how we will be audited against them and what evidence will be acceptable | 32.29% | 31 |
| The SCRM requirements are somewhat unclear | 15.63% | 15 |
| The SCRM requirements are not clear | 6.25% | 6 |
| Other (please explain) | 16.67% | 16 |
| TOTAL | | 96 |

# Key take-aways and conclusions

- 59 of 96 respondents felt the requirements are clear but questions about compliance evidence are creating concern.
- Compliance ambiguity is a significant concern for respondents.
- What is a “vendor?”
  - Original Equipment Manufacturer (OEM) or a Value-Added Reseller (VAR), and other subcontracts have caused some concerns from a compliance perspective and resulted in confusion on when the risk assessment can be stopped or continued. Should the risk assessment stop at the VAR, or should it continue to the suppliers the VAR acquires product or service?
- The FAQs and guidance create some compliance ambiguity
  - The large amount of guidance, FAQ, and webinars needed to implement the Standard create a concern that entities are expected to address specific risks and/or scenarios not specified in the Requirements.
- There is room for improvement in the guidance provided around applicability and pertaining to the evidence data that has been identified in the Evidence Tool (i.e. Planning Start Date, Procurement Start Date).
- New standards require entities and NERC to review the results from audits to determine effective risk mitigation and compliance.
- **Conclusion:** Entities have some questions about the requirements but are more concerned about what to expect from an audit.

## Q7: Do you have a clear understanding of what constitutes a violation of the requirements?

- Answered: 95 Skipped: 106



## Q7: Do you have a clear understanding of what constitutes a violation of the requirements?

- Answered: 95 Skipped: 106

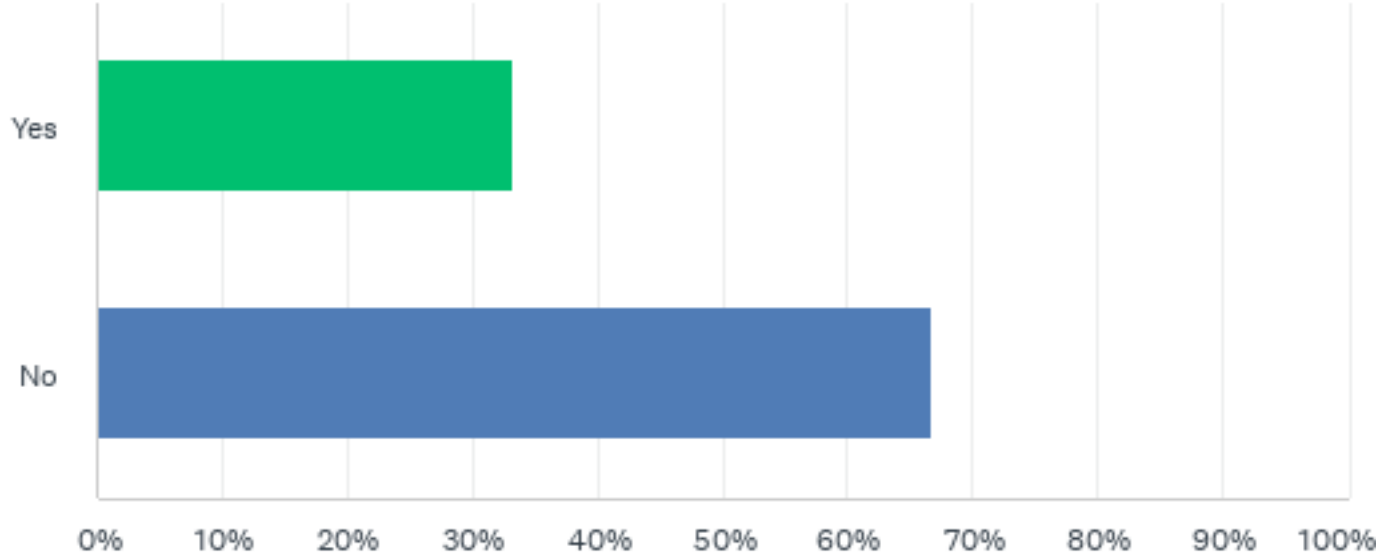
| ANSWER CHOICES | RESPONSES | |
|---|---|---|
| Yes | 58.95% | 56 |
| No | 41.05% | 39 |
| TOTAL | | 95 |

# Key take-aways and conclusions

- 59% of respondents indicate they have a clear understanding of what constitutes a violation while 41% do not.
  - Concerns expressed:
    - While we believe we understand what a violation is, there is still concern until we have been thru an audit.
    - Based on some entities audit experience it would be good for NERC to develop an Audit Practice Guide so there will be consistency among the regions when conducting an audit of the SCRM requirements.
- NERC/ERO should post facts and circumstances for non-compliance.
  - Post results of CIP-013 audits
- **Conclusion:** Entities are relatively unclear about what would be deemed a noncompliance.

## Q8: Do you believe there are gaps in the SCRM requirements?

- Answered: 93 Skipped: 108



## Q8: Do you believe there are gaps in the SCRM requirements?

- Answered: 93 Skipped: 108

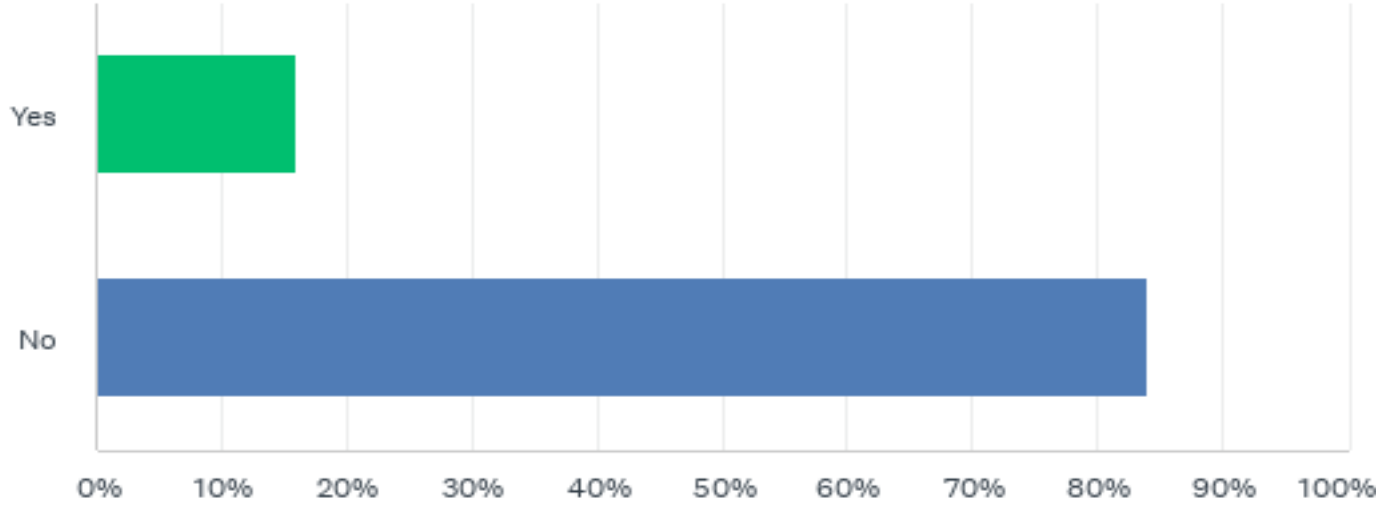
| ANSWER CHOICES | RESPONSES | |
|---|---|---|
| Yes | 33.33% | 31 |
| No | 66.67% | 62 |
| TOTAL | | 93 |

# Key take-aways and conclusions

- Two-thirds of respondents do not believe there are gaps in the requirements.
- Concerns expressed:
  - Different utilities have different levels of risk acceptance and where one company may consider a vendor safe to use (because they have to) others may see the risk with the vendor too great. There is no consistency with the current iteration of CIP-013. A centralized list of vendors could be created and vetted at a much higher level than what is done by each utility.
  - If an entity is developing their plan in the spirit of supply chain risk management, and not just trying to comply with some words on a page, then there are no gaps.
  - Concerned that the SCRM requirements do not reduce the risks to the BES that is commensurate with the amount of effort that it takes to comply with the requirements.
  - All the onus is on the utility with little to no consequence to a vendor who does not follow what was agreed. Vendors need to be part of any solution and the SCRM as written holds them harmless unless the utility chooses to act.
- **Conclusion:** Entities are hesitant to say there are gaps in the standards as they would like stability and answers before more changes are made.

## Q9: Have you reached out to the Electric Reliability Organization (ERO) Enterprise with questions or concerns on the SCRM requirements?

- Answered: 100 Skipped: 101



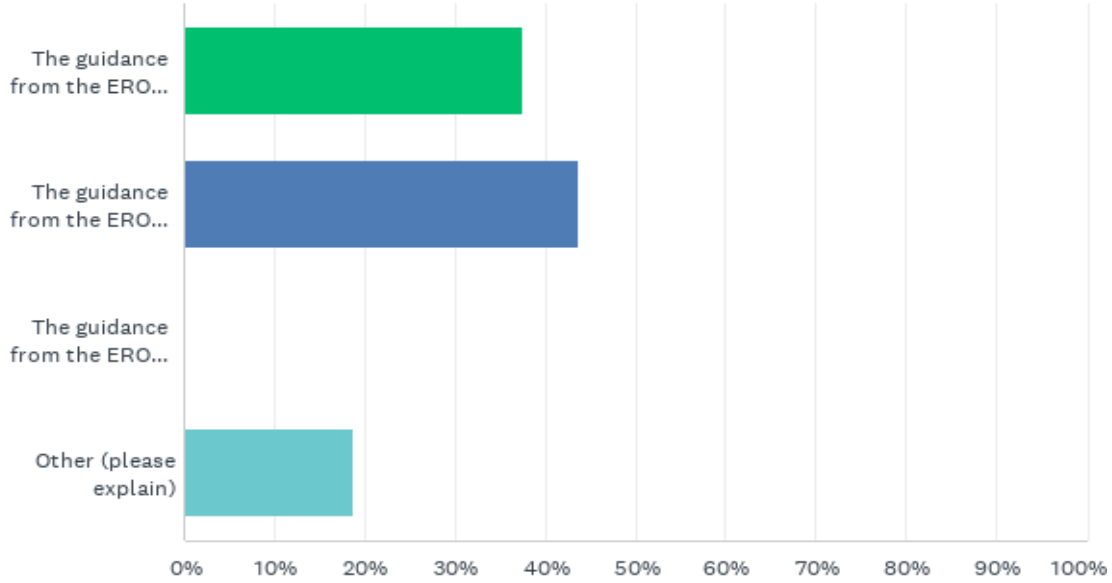
**Q9: Have you reached out to the Electric Reliability Organization (ERO) Enterprise with questions or concerns on the SCRM requirements?**

- Answered: 100 Skipped: 101

| ANSWER CHOICES | RESPONSES | |
|---|---|---|
| Yes | 16.00% | 16 |
| No | 84.00% | 84 |
| TOTAL | | 100 |

**Q10: Have you reached out to the Electric Reliability Organization (ERO) Enterprise with questions or concerns on the SCRM requirements? Responded Yes.**
**Please select the statement that best reflects your experience**

- Answered: 16 Skipped: 185



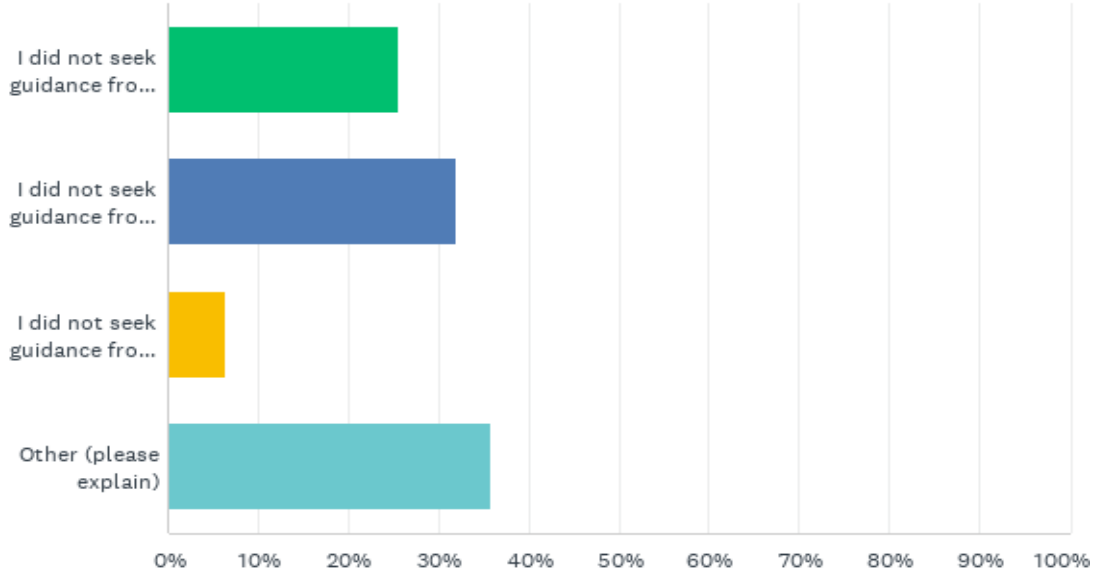
**Q10: Have you reached out to the Electric Reliability Organization (ERO) Enterprise with questions or concerns on the SCRM requirements? Responded Yes.**
**Please select the statement that best reflects your experience**

- Answered: 16 Skipped: 185

| ANSWER CHOICES | RESPONSES | |
|---|---|---|
| The guidance from the ERO Enterprise was helpful in clarifying the SCRM requirements | 37.50% | 6 |
| The guidance from the ERO Enterprise was somewhat helpful in clarifying the SCRM requirements | 43.75% | 7 |
| The guidance from the ERO Enterprise was unhelpful in clarifying the SCRM requirements | 0.00% | 0 |
| Other (please explain) | 18.75% | 3 |
| TOTAL | | 16 |

**Q11: Have you reached out to the Electric Reliability Organization (ERO) Enterprise with questions or concerns on the SCRM requirements? Responded no.**
**Please select the statement that best reflects your experience.**

- Answered: 78 Skipped: 123



**Q11: Have you reached out to the Electric Reliability Organization (ERO) Enterprise with questions or concerns on the SCRM requirements? Responded no.**
**Please select the statement that best reflects your experience.**

- Answered: 78 Skipped: 123

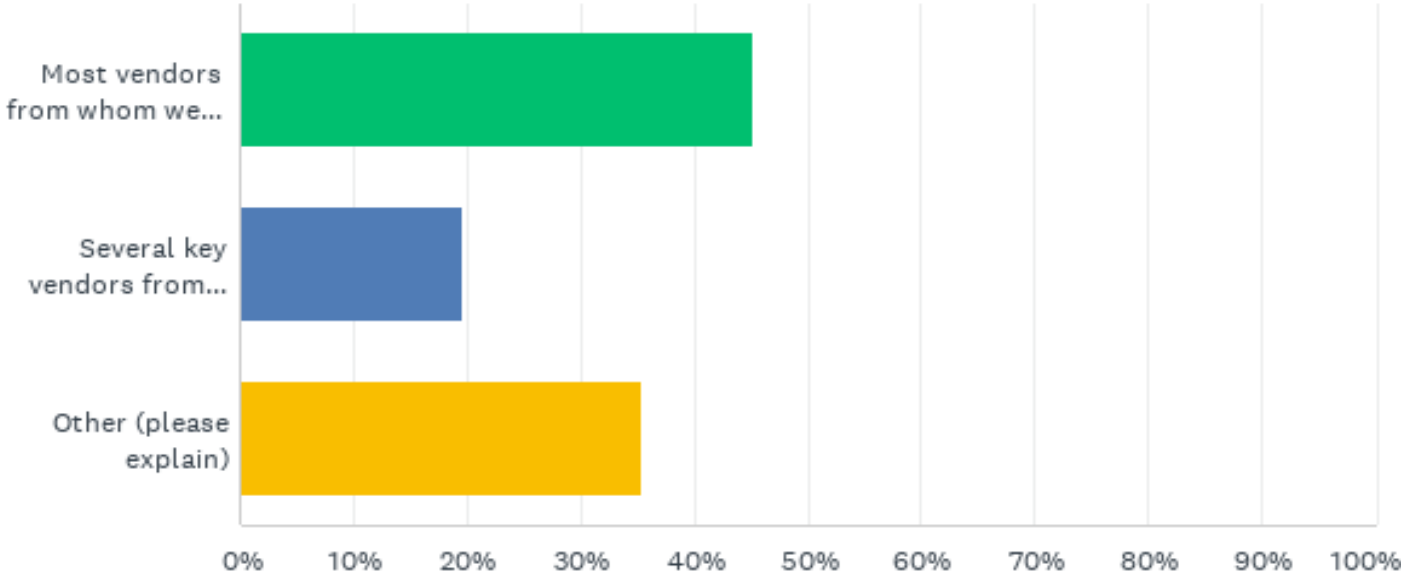
| ANSWER CHOICES | RESPONSES | |
|---|---|---|
| I did not seek guidance from the ERO Enterprise because I understand the SCRM requirement expectations and have no questions | 25.64% | 20 |
| I did not seek guidance from the ERO Enterprise because I leveraged other industry guidelines and have no questions | 32.05% | 25 |
| I did not seek guidance from the ERO Enterprise because I have concerns with using these resources | 6.41% | 5 |
| Other (please explain) | 35.90% | 28 |
| TOTAL | | 78 |

# Key take-aways and conclusions

- 84% of respondents have not reached out to the ERO with questions and concerns.
  - 25% understand the requirements and have no questions.
  - 32% leveraged other industry guidelines.
  - 6% are concerned with using ERO resources.
    - Variety of reasons why entities have not reached out to the ERO
      - "It is what it is"
      - "Fall on deaf ears"
      - Worked with consultants
- **Conclusion:** While a few entities reported positive interactions with regions, most entities are getting answers through workshops, guidance, consultants or other non-personal interactions.

## Q12: Select the statement that most accurately reflects your experience with vendors receptivity to your SCRM program

- Answered: 82 Skipped: 119



## Q12: Select the statement that most accurately reflects your experience with vendors receptivity to your SCRM program

- Answered: 82 Skipped: 119

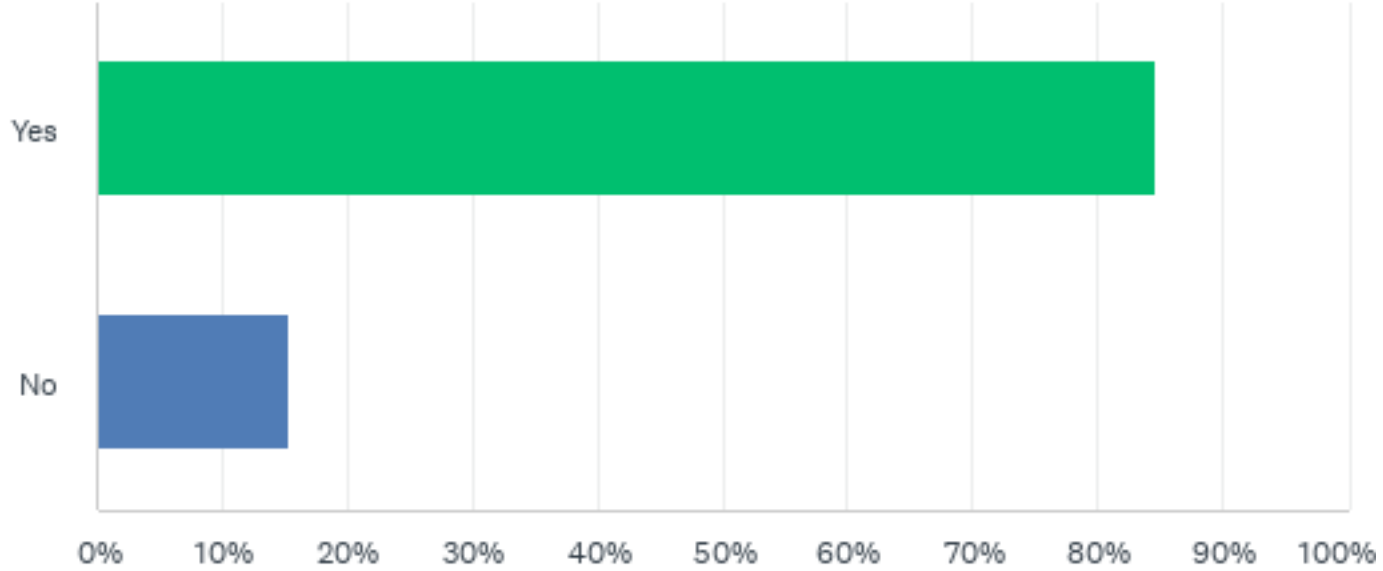
| ANSWER CHOICES | RESPONSES | |
|---|---|---|
| Most vendors from whom we procure software, hardware, or cyber services are reasonably supportive (timeliness, completeness of information) in responding to our risk assessment. | 45.12% | 37 |
| Several key vendors from whom we procure software, hardware, or cyber services are resistant to responding to our risk assessment. | 19.51% | 16 |
| Other (please explain) | 35.37% | 29 |
| TOTAL | | 82 |

# Key take-aways and conclusions

- 45% of respondents indicated vendors are reasonably supportive in responding to requests on risk assessments.
  - 19% indicated vendors are resistive.
  - Comments indicated:
    - There has been a delay in receiving the risk assessments back from some vendors - information is not completed properly, had to go back to them and ask to re-submit.
    - Some vendors require entities to complete non-disclosure agreements.
    - Vendor wanted to charge $5,000 to complete the questionnaire.
    - Vendor consulting side was trying to sell CIP-013 services while their legal side was pushing back on risk assessment for hardware and software
    - Vendors are responsive to our risk assessment questionnaires; however, we are seeing some resistance from vendors in accepting all of our terms and conditions.
    - Vendors may be struggling with the avalanche of requests. This process is also expensive and time consuming for Registered Entities due to the limited number of internal staff involved with collecting large amounts of data initially and annually.
    - Many key vendors are unwilling to respond or participate in our CIP-013 Risk Assessment, particularly as we are a small utility. We have had several vendors state they are working on a response for over a year now.
- Most vendors are amenable to the CIP-013 program requirements, but some of the sub-tier OEMs are not as cooperative in the risk assessment activities. Reasons include that they are not a direct supplier to this organization, therefore do not see it as their obligation to comply with risk assessment requests, or that we may have some difficulty identifying the right contact person if they are not a direct supplier.
- SCRM processes requires more consistent use across all registered utilities.
- Vendors need assistance in how to complete a SCRM questionnaire.
- **Conclusion:** Recognize that vendors receive SCRM questionnaires from multiple clients, in varied formats, across multiple industries. Better consistency and effectiveness can be achieved through industry convergence on a standard questionnaire.

## Q13: Does your risk assessment of a vendor provide you adequate information to determine the risks of the vendor's product or services?

- Answered: 78 Skipped: 123



**Q13: Does your risk assessment of a vendor provide you adequate information to determine the risks of the vendor's product or services?**

- Answered: 78 Skipped: 123

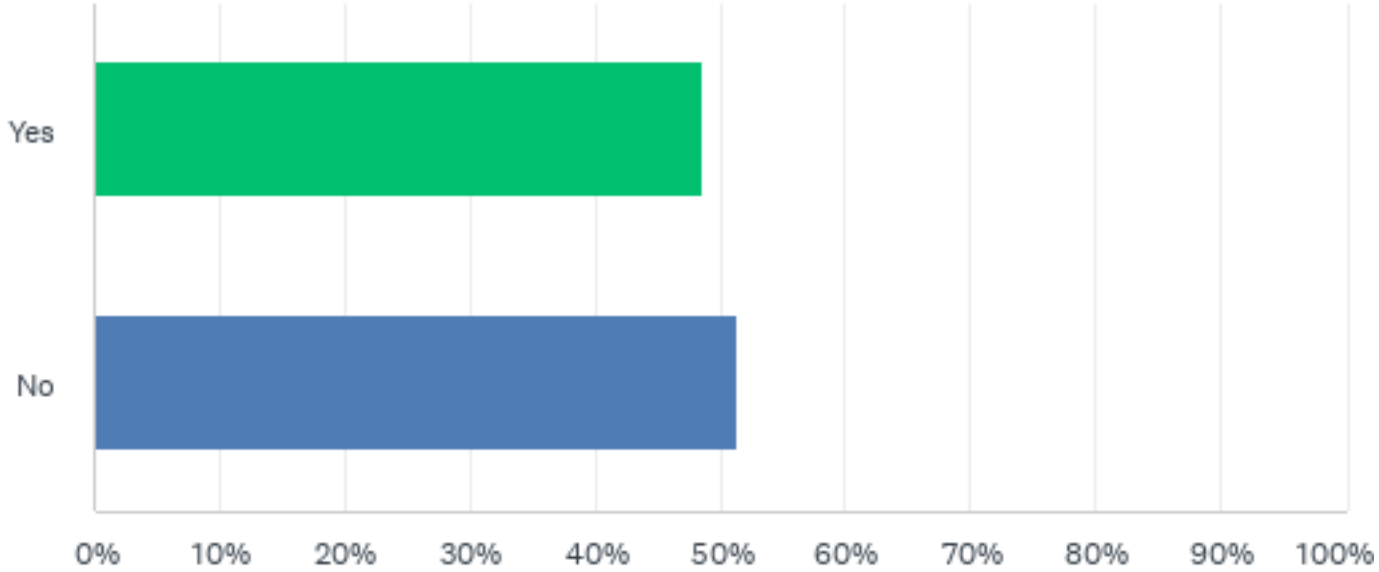
| ANSWER CHOICES | RESPONSES | |
|---|---|---|
| Yes | 84.62% | 66 |
| No | 15.38% | 12 |
| TOTAL | | 78 |

# Key take-aways and conclusions

- 85% of respondents indicate their risk assessment does provide adequate information to determine the risks of the vendor products and services.
  - 15% do not think the risk assessment provides adequate information:
    - As an example, a risk assessment of Solar Winds would not have prevented the vulnerability that occurred.
    - We don't know what we don't know.
- Difficult to interpret vendor responses unless registered entity has an internal SME for review (limited experience).
- Use of “canned” questionnaires are helpful when starting the SCRM process (e.g., NATF questionnaire).
- **Conclusion:** Most entities think they are getting enough information to make a risk assessment but have concerns over whether the supplier provided response is accurate/truthful.

## Q14: Do the vendors provide enough information to determine risks from components or products the vendor procures from others?

- Answered: 74 Skipped: 127



## Q14: Do the vendors provide enough information to determine risks from components or products the vendor procures from others?

- Answered: 74 Skipped: 127

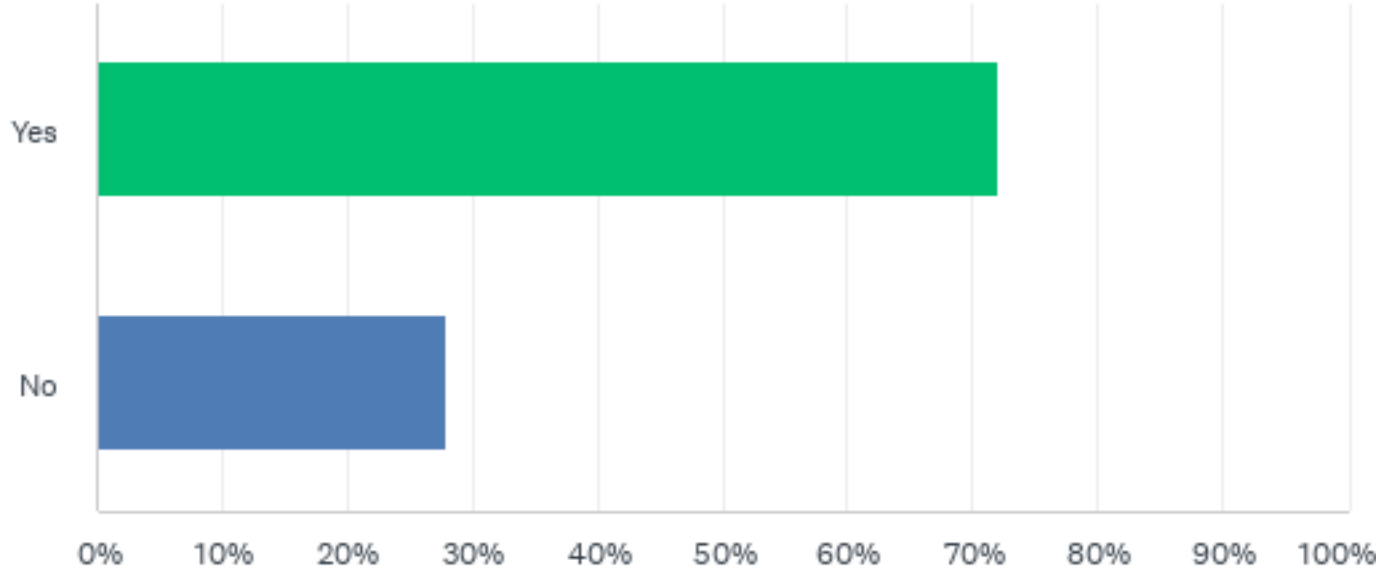
| ANSWER CHOICES | RESPONSES | |
|---|---|---|
| Yes | 48.65% | 36 |
| No | 51.35% | 38 |
| TOTAL | | 74 |

# Key take-aways and conclusions

- 49% of respondents indicate vendors provide enough information to determine risk while 51% indicated vendors don't provide enough information.
  - No: However, terms and conditions of contracts have been designed to mitigate risk.
  - No: In almost all instances we must go back to the vendor for additional information before a risk determination can be achieved, but there are occurrences they will not provide the needed input.
  - Yes: Sometimes the information is not readily provided with the risk assessment they return but is gained after a meeting with the vendor.
  - No: This information is often considered confidential by the vendor.
  - Yes: The responses varied in level of detail and applicability.
- Vendors/resellers may rely on upstream suppliers as part of their direct supplier obligations.
- Inconsistent quality/accuracy of responses to the same question across vendors.
- **Conclusion:** Registered entities should expect to invest more time in vetting questionnaire responses; not all vendors have the knowledge to respond properly.

## Q15: Do you support vendors providing a Software Bill of Materials (SBoM)?

- Answered: 75 Skipped: 126



## Q15: Do you support vendors providing a Software Bill of Materials (SBoM)?

- Answered: 75 Skipped: 126

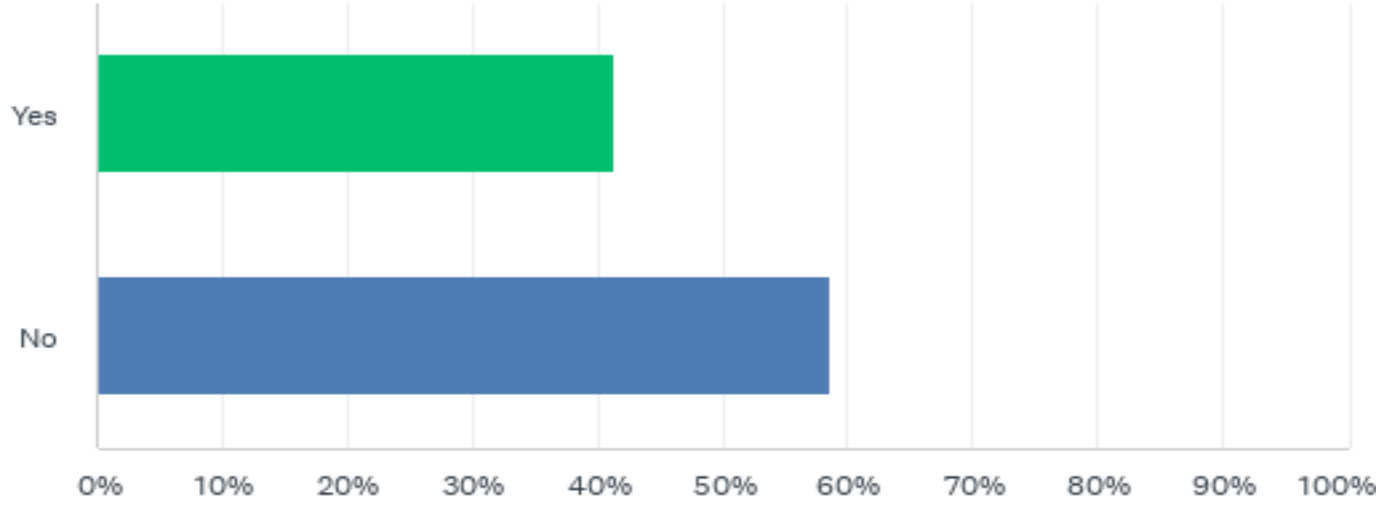
| ANSWER CHOICES | RESPONSES | |
|---|---|---|
| Yes | 72.00% | 54 |
| No | 28.00% | 21 |
| TOTAL | | 75 |

# Key take-aways and conclusions

- 72% of respondents support vendors providing a Software Bill of Material (SBoMs).
- Yes: We support vendors providing an SBoM but would like guidance from NERC with what should happen with the information and what are the compliance expectations.
  - Yes: Providing it is fine, however I do not believe most utilities have the resources to perform a critical review of this data. A centralized entity should perform the review and then provide a recommendation for all BES users of whether a given produce/service is acceptable from a risk perspective. Asking every company to do it themselves is not efficient and will not yield optimal results.
  - No: SBoM is a great idea for entities that have the resources to adequately review these lists. However, most vendors will rightly be concerned about confidentiality and most utilities do not have the resources to understand the risks of all the scores of software contained in an SBoM.
  - No: We'd need some training.
- Having vendors provide SBoMs would improve the assessment process.
- Submission of SBoMs needs a standardized format for consistency in review and risk determination.
- Evaluation of an SBoM requires in-house or contracted expertise.
- **Conclusion:** Entities support the concept of SBOMs, but are concerned about having the resources to conduct analysis; they would like to see a consistent format that provides information from the data.

## Q16: Has CIP-013 enabled you to identify previously unknown supply chain risk?

- Answered: 75 Skipped: 126



## Q16: Has CIP-013 enabled you to identify previously unknown supply chain risk?

- Answered: 75 Skipped: 126

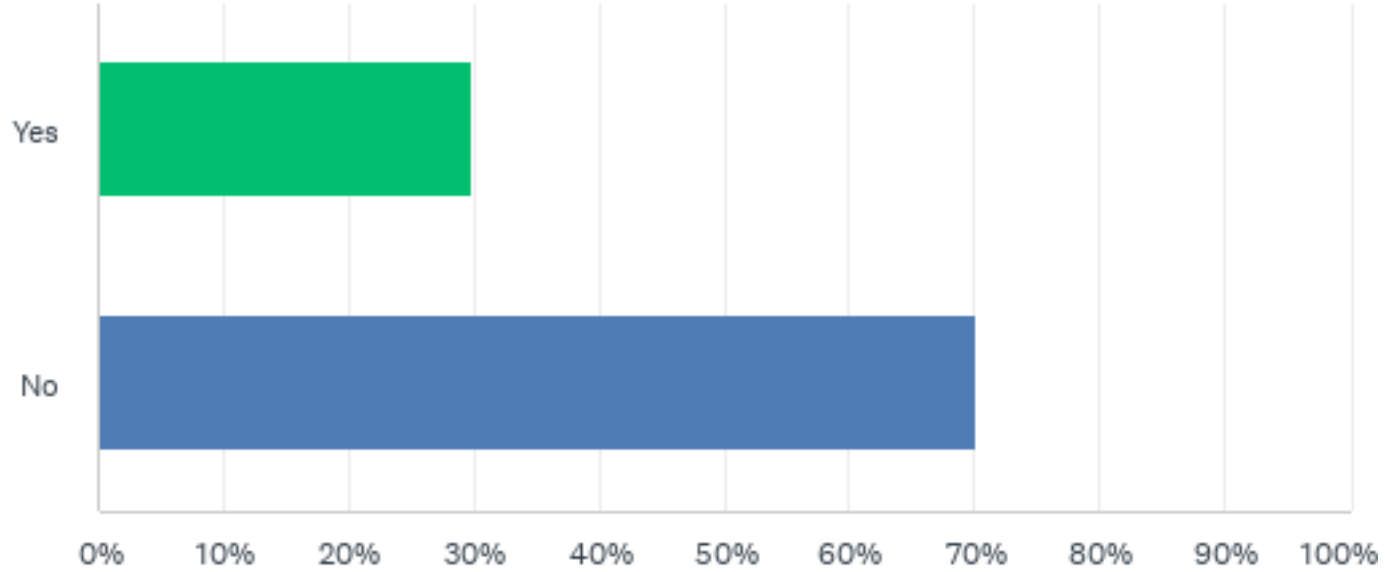
| ANSWER CHOICES | RESPONSES | |
|---|---|---|
| Yes | 41.33% | 31 |
| No | 58.67% | 44 |
| TOTAL | | 75 |

# Key take-aways and conclusions

- 41% of respondents indicated CIP-013 has enabled them to identify previously unknown risks while 59% indicate it has not.
  - Comments indicate:
    - Of those responding “yes”, working with vendors helped identify some risks – with the vendor and within their own organization.
      - Yes: We have had vendors notify us of security issues, leading us to assess potential risks to our systems, review their vendor risk assessment, and in at least one case, temporarily suspend access.
      - Yes: It identified the risk of using resellers.
    - Of those responding “no”, they had not identified any new risks, but there has been limited experience. The standard raised internal awareness and awareness of resources.
      - No: None of our existing vendors (so far) have represented an unacceptable risk. All mitigating measures for the identified risks were already built into our CIP program.
      - No: We did learn about resources that were available to us we previously were unaware.
      - No: it has benefited the organization in spreading awareness of the supply chain vulnerabilities.
- **Conclusion:** People have identified some risks and have had some positive internal actions, but these are limited, which could be due to limited experience with the standard.

## Q17: Have you implemented supply chain mitigations based on your risk assessment that previously you had not implemented?

- Answered: 77 Skipped: 124



## Q17: Have you implemented supply chain mitigations based on your risk assessment that previously you had not implemented?

- Answered: 77 Skipped: 124

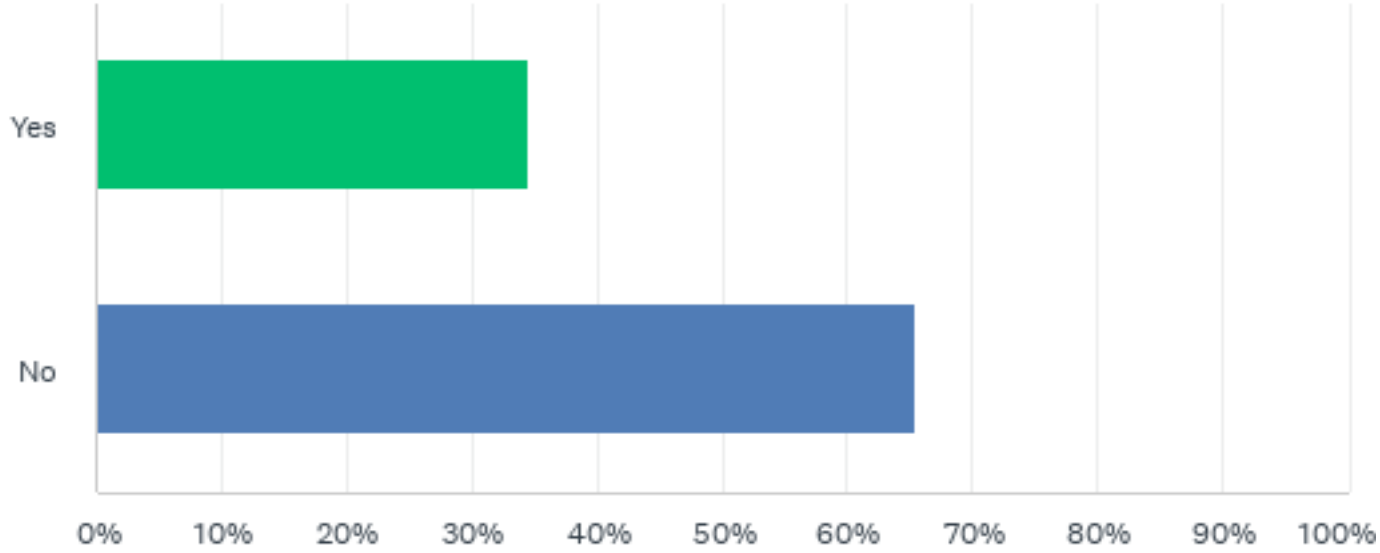
| ANSWER CHOICES | RESPONSES | |
|---|---|---|
| Yes | 29.87% | 23 |
| No | 70.13% | 54 |
| TOTAL | | 77 |

# Key take-aways and conclusions

- 70% of respondents have not implemented new supply chain mitigations.
  - Comments indicate:
    - Of those responding “yes”, comments indicate some mitigations are being implemented and supported with contract terms, or risks are being addressed through contract terms.
    - Of those responding “no”, they had not identified any new risks, had current controls in place to address the risks they found, or had little experience with the standard.
- **Conclusion:** People have limited experience with the standard, so few are implementing new mitigations. Some are implementing new contract terms.

**Q18: Have you implemented compensating security measures other than specification and procurement activities to address security issues because of implementing your CIP-013-1 Risk Management Plan?**

- Answered: 78 Skipped: 123



**Q18: Have you implemented compensating security measures other than specification and procurement activities to address security issues because of implementing your CIP-013-1 Risk Management Plan?**

- Answered: 78 Skipped: 123

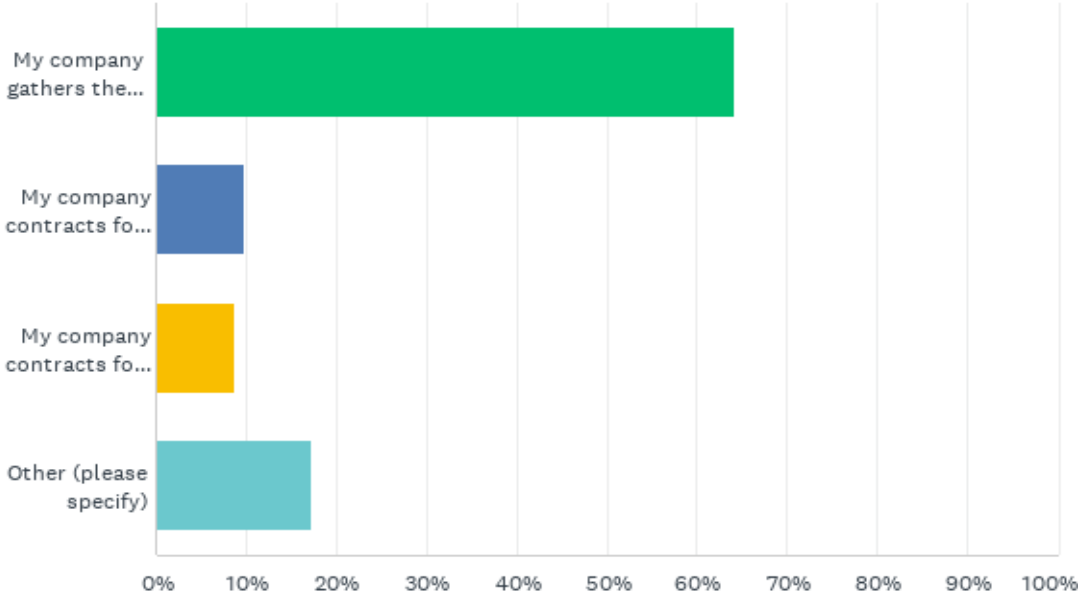
| ANSWER CHOICES | RESPONSES | |
|---|---|---|
| Yes | 34.62% | 27 |
| No | 65.38% | 51 |
| TOTAL | | 78 |

# Key take-aways and conclusions

- 65% of respondents indicate they have not implemented compensating security measures other than specification and procurement activities.
  - Comments indicate:
    - Of those responding “yes”, comments indicate that one responder implemented a lifecycle program, one is in the process, and others indicated that they implemented a scorecard and additional contract terms and conditions.
    - Of those responding “no”, comments indicate that the technical mitigations put in place for the CIP-013 standards have provided the needed security measures.
- **Conclusion:** People appear to be putting analysis tools and contract terms in place for security measures, but other additional security measures have not been required.

## Q19: Select the statement that most accurately reflects how you conduct a risk assessment of a vendor

- Answered: 81 Skipped: 120



## Q19: Select the statement that most accurately reflects how you conduct a risk assessment of a vendor

- Answered: 81 Skipped: 120

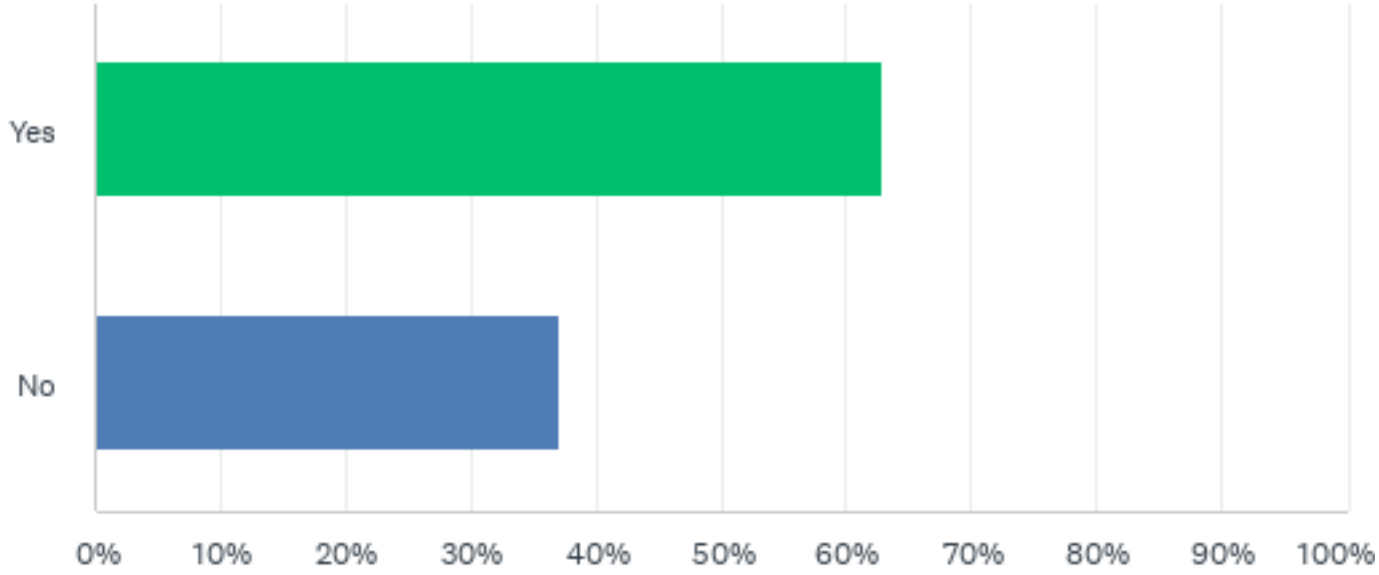
| ANSWER CHOICES | RESPONSES | |
|---|---|---|
| My company gathers the information and performs the risk assessment. | 64.20% | 52 |
| My company contracts for services of others to gather the information and then my company performs the risk assessment. | 9.88% | 8 |
| My company contracts for services of others to gather the information and perform the risk assessment. | 8.64% | 7 |
| Other (please specify) | 17.28% | 14 |
| TOTAL | | 81 |

# Key take-aways and conclusions

- 64% of respondents indicate they gather the information and perform the risk assessment while the other respondents indicate some involvement of contracts for services.
- Comments indicate:
  - Entity used a combination of direct information gathering and external contracted services.
  - Entity gathers the information and performs the risk assessment. However, in cases where our internal risk assessment has identified a vendor as being of critical nature we also employ a third-party to do a more in-depth information gathering which we then utilize to perform our final internal risk assessment.
  - Entity contracts for services of others to gather the information and perform the risk assessment but, additionally, our company also performs a review of the completed third party assessment.
- The majority of entities gather the information and conduct the risk assessment themselves and are doing it without additional resources other than reallocated resources from other departments.
- **Conclusion:** The majority of responders are gathering information and conducting the risk assessments themselves, while others are contracting out some or all of the process.

## Q20: Have you added new or updated contract language to your procurements because of the SCRM requirements?

- Answered: 81 Skipped: 120



## Q20: Have you added new or updated contract language to your procurements because of the SCRM requirements?

- Answered: 81 Skipped: 120

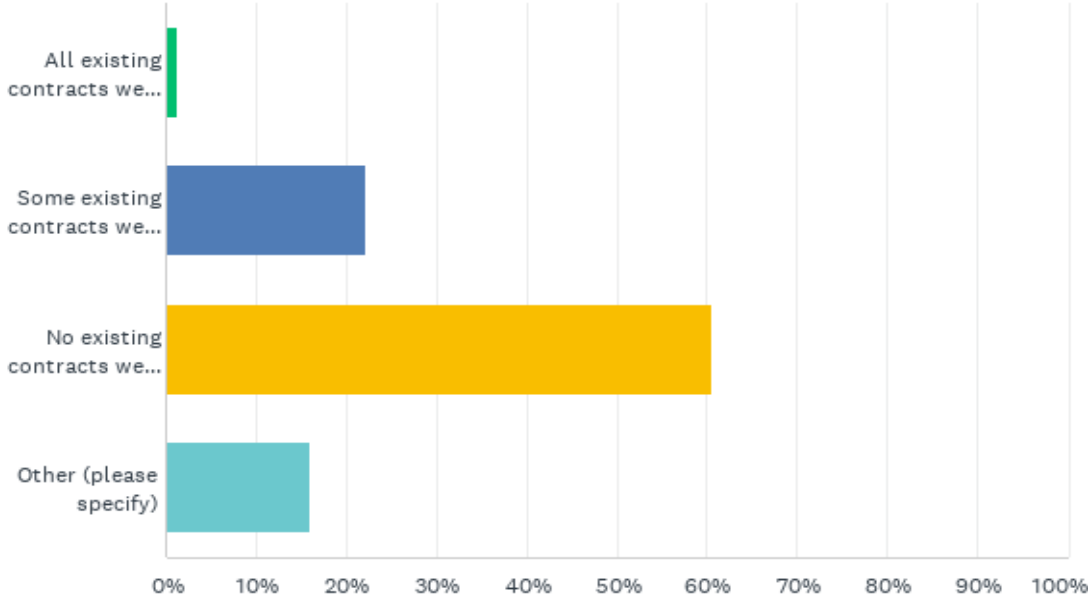
| ANSWER CHOICES | RESPONSES | |
|---|---|---|
| Yes | 62.96% | 51 |
| No | 37.04% | 30 |
| TOTAL | | 81 |

# Key take-aways and conclusions

- 63% of respondents indicate they have added new or updated contract language to procurements.
  - Comments indicate:
    - No: We instead use questions geared toward what the vendor/contractor will do to help us support our CIP-013 program, specifically CIP-013 R1.2.1 through 1.2.6. Adding language to the contract did not add any additional security (in our opinion) and slowed the purchasing process to a crawl with the back and forth between the legal departments in our company and the vendor/contractor.
    - Yes: Updated contract language is added as Master Agreements come up for renewal.
    - Yes: We have added an appendix to our contracts, specific to CIP-013.
    - Yes: Used EEI-suggested language as our template
    - Yes: We've added Attachment A CIP-013-1 Security Controls
- **Conclusion:** The majority of responders are adding attachments to current contracts and are updating contracts as they are renewed.

## Q21: Have you renegotiated the terms of existing contracts within the scope of CIP-013? Select the most appropriate answer.

- Answered: 81 Skipped: 120



**Q21: Have you renegotiated the terms of existing contracts within the scope of CIP-013? Select the most appropriate answer.**

- Answered: 81 Skipped: 120

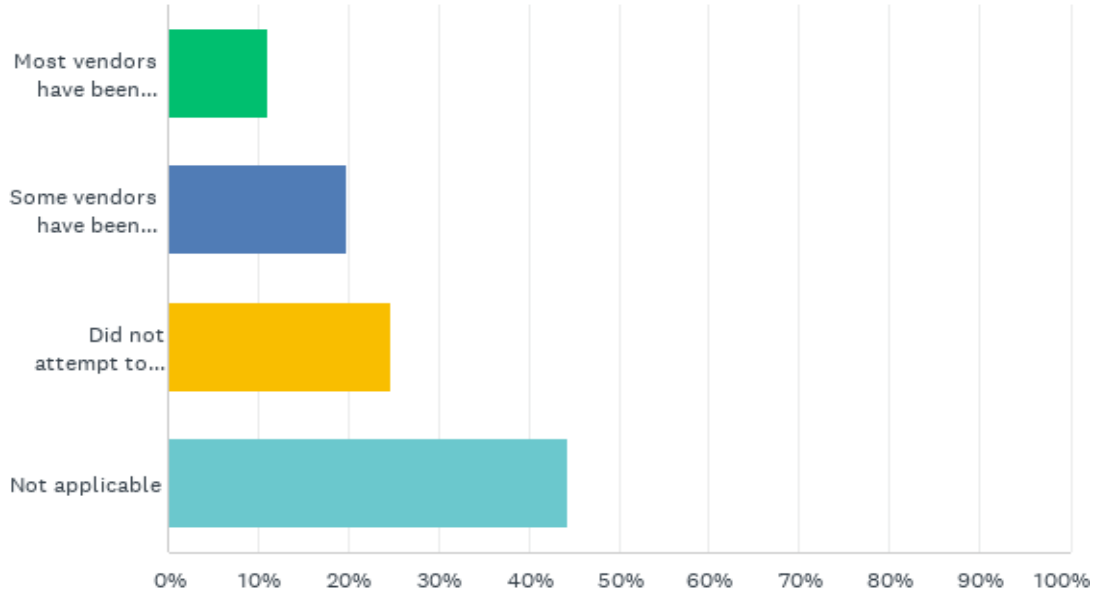
| ANSWER CHOICES | RESPONSES | |
|---|---|---|
| All existing contracts were renegotiated | 1.23% | 1 |
| Some existing contracts were renegotiated | 22.22% | 18 |
| No existing contracts were renegotiated | 60.49% | 49 |
| Other (please specify) | 16.05% | 13 |
| TOTAL | | 81 |

# Key take-aways and conclusions

- 60% of respondents indicate no existing contracts were renegotiated, 1% indicate all were renegotiated while the other respondents are somewhere between.
  - Comments indicate:
    - The “other” responses indicate a blend of amending or updating as opportunities arise.
- **Conclusion:** Responders are not renegotiating all contracts. Most are not updating existing contracts, but some are updating or adding attachments as opportunities arise.

## Q22: Have your vendors been agreeable to renegotiating existing contracts?

- Answered: 81 Skipped: 120



## Q22: Have your vendors been agreeable to renegotiating existing contracts?

- Answered: 81 Skipped: 120

| ANSWER CHOICES | RESPONSES | |
|---|---|---|
| Most vendors have been agreeable | 11.11% | 9 |
| Some vendors have been agreeable | 19.75% | 16 |
| Did not attempt to renegotiate any existing contracts | 24.69% | 20 |
| Not applicable | 44.44% | 36 |
| TOTAL | | 81 |

# Key take-aways and conclusions

- 69% of respondents indicated “not applicable” or did not attempt to renegotiate existing contracts. Of the other respondents, most or some of the vendors are agreeable to renegotiating contracts.
- **Conclusion:** The majority of responders are not renegotiating contracts. Approximately one third of responders that are subject to the standard responded that vendors were agreeable to renegotiating (updating, adding attachments) when responders are requesting it.

## CIP compliance program resources dedicated to the SCRM Standards.
## Percentage growth of CIP Compliance Program as a result of implementing SCRM compliance.

(Include those involved from the procurement/contracting office)

- The SCWG wanted to understand the impact of the new requirements on entities, so SCWG asked for two percentages:
  - Percentage of CIP Compliance Program resources dedicated to SCRM compliance
  - Percentage growth of CIP Compliance Program because of implementing SCRM compliance
  - And, asked for any comments from the entities.
- CIP Programs at entities are consuming significant resources and creating compliance fatigue. By comparing growth of those programs, entities can provide a common number which can be compared across entities of different sizes while not providing specific dollar amounts. SCWG was concerned entities would not provide specific dollar amounts and the results of those dollar amounts would be difficult to interpret and analysis.
- 57 entities responded by providing percentages or comments and some provided both. Entities have implemented Supply Chain Risk Management Programs and are currently in the process of preparing for the CIP-013-2 modifications to be effective on October 1, 2022. The workload on entities and vendors has been significant. Industry groups are attempting to improve the process and make risk assessments more efficient and increase assurance in the results.
  - **Average of 22.5% (49 responses) of CIP Compliance Program resources dedicated to SCRM compliance**
  - **Average of 9.15% (49 responses) growth of CIP Compliance Program because of implementing SCRM compliance**
- Most entities responded that growth is occurring due to resources being reallocated from other departments, not additional FTEs

## CIP compliance program resources dedicated to the SCRM Standards.
## Percentage growth of CIP Compliance Program as a result of implementing SCRM compliance.

(Include those involved from the procurement/contracting office)

- Comments indicate:
  - Just because there are new requirements does not mean my entity has the resources to grow the CIP compliance program. Our CIP compliance program has been half-staffed for over two years.
  - For our software hashing, this program was new for us. It's added about 15-30 minutes per software/patch to timelines. For new/recurring purchases, the program has added weeks. Negotiating and renegotiating contracts, checking checklists, evaluating vendors, waiting on responses, everything is now delayed.
  - Our CIP Compliance team is dedicated to ensuring that this organization is compliant with all CIP regulations. No specific person on the team is responsible for one regulation, all team members work to ensure compliance with all CIP requirements.
  - Effort provided by existing resources. No additional resources have been hired.
  - Our supply chain working group meets weekly, and more as necessary. Supply chain is a noticeable increase in workload for our personnel.
  - We had to add the Procurement Group to our CIP resources.
- A concerning observation from the survey is entities are more apt to pull CIP resources from other areas to address SCRM processes than add additional resources. This may further deplete strained resources in the other CIP areas and continue to increase compliance fatigue. Finding trained, experienced staff willing to tie their career to compliance is getting even more difficult.
- Sobering quote: "We all cringe when we know we have a to make a purchase."
- **Conclusion:** SCRM is requiring significant resources to implement and stealing resources from other CIP programs. The resource drain is both on entities and vendors.

# Selected Open-Ended Responses

- Supply Chain is a global issue for all critical infrastructure and not just electric utilities. Any solution the federal government devises needs to be useful for all sectors, not just ours. Implementing different requirements will only serve to frustrate vendors and over time will shrink the vendor pool. All we must do is look at the nuclear industry as an example of what happened to the vendor pool when 10CFR50 Appendix B was fully implemented. We must also acknowledge that SCRM requirements will drive up the cost of goods and services from vendors that choose to continue to supply our industry. Again, see the nuclear industry for examples. We need to learn from our nuclear brethren and not repeat the same mistakes they made.
- The supply chain requirements as written are reasonable. It's the audit oversight piece that has everyone worried.
- Including low impact BCS in these requirements would create very significant challenges.
- The current Supply Chain requirements are adequate as written. They provide an additional level of security and have proven to be effective.
- Continue to provide additional guidance. Continue to gather feedback and share experiences.

# Selected Open-Ended Responses

- We would like additional clarification on the scope of the term "vendor" as well as the use of the ERT during compliance monitoring.
- Our organization has spent significant time attempting to comply with the SCRM standards without assurance that compliance has been or can be achieved. There is significant confusion over what constitutes an applicable vendor, what is an applicable procurement, what are applicable risks to be identified and mitigated, and what are acceptable mitigations. Guidance from NERC and Regional Entities do not address the many types of vendor relationships that exist, nor is it clear how these requirements result in real reduction of risks.
- Forcing specific answers from Vendors is challenging. Vendors are saying this is time consuming with little incentive to complete. They're receiving multiple requests from multiple Utilities.
- It would have been helpful to have both the evidence workbook and the self-certification templates available prior to the standard enforcement date. Since they were not available, entities are having to go back and adjust their programs accordingly instead building the plans to accommodate these requests during the plans development.

# Selected Open-Ended Responses

- Third-party certification recognized by NERC for example, SOC2 type 2 would simplify the compliance process and address non-cyber security risks (financial, geopolitical) through appropriate channels and/or specialists.
- The vendor is held harmless, and utilities are held accountable for the vendor's actions which utilities have no control over. Simply buying a product or not buying a product from a vendor may not influence their security practices. A better solution would be to have vendors certify their products for security like a UL certification for safety. Expanding the current mandatory requirements to low impact BES Cyber Assets and other cyber assets will only drive the cost up and not address the core problem of vendor security. The vendor must be held accountable and not the consumer using the product.
- A certification should be considered where a third party performs and (this is key) then confirms the security aspects of a given product/service. This would allow entities to accept the certified product/service without additional review. Most entities, especially smaller ones, lack the resources to perform an in depth review themselves.

# Selected Open-Ended Responses

- Suggest perhaps NERC have suppliers register and become "Certified" and then NERC directly audits registered suppliers for supply chain risk. Then entities could purchase from certified suppliers without supply chain risk.
- Based on conversations with other entities there is feeling of duplication of effort for some of the processes around vendor risk mitigation. A possible way to reduce this would be a voluntary vendor supply chain certification program run by NERC. Vendors could review their development and manufacturing processes with NERC and meet specific security measures to earn the certification. This would work to more effectively mitigate risk in the supply chain prior to procurement by utilities.

# Selected Open-Ended Responses

- What's needed is a pre-vetted pool of vendors to streamline internal processes.
  - a) Development of a nationwide Vendor Seal Of Supply Chain Excellence. Vendors, products, and services can be submitted for entrance to the program. If entrance is accepted for a seal of excellence, then no additional assessment action is necessary once a qualifying product or vendor has been selected by an Entity if the Entity's plan allows for this scenario. Smaller entities having fewer personnel would especially benefit.
  - b) Development of a nationwide database of risk assessment results on commonly used vendors, products, and services. If an Entity completes an analysis and submits results, other Entities may leverage the database to review common risks and may be able to use the assessment without additional investigation.

# Selected Open-Ended Responses

- Regional Entities (RE) have indicated they will expect to see Registered Entities (Entity) perform an internal assessment of all requisitioned 3rd party assessments as they feel a 3rd party assessment cannot sufficiently consider the Entity's specific situation. However, the Standard does not specifically require an assessment nor an assessment of an assessment. What has also been said is that it's up to each Entity to design their plan and follow it. One would think that if the Entity's plan determines a second, internal risk assessment of the 3rd party's assessment is not needed, the REs cannot determine otherwise. If Entities are allowed to design their plans as seen fit, Entities could leverage (future) certified or pre-vetted vendors, products, and services and reduce the burden of double assessments.
- We believe that the SCRM requirements do not reduce the risks to the BES that is commensurate with the amount of effort that it takes to comply with the requirements. Additionally, experts from the cyber security community believe that this effort with vendors does not reduce risk with events similar to what occurred with SolarWinds. Therefore, in the end, the CIP-013 SCRM is something that looks good on paper but accomplishes little in real life.

Your feedback is very important to us. Please provide your feedback using the link or QR Code below or the link below:

https://www.surveymonkey.com/r/BD2XNW7

# Thank You!