Survey

Supply Chain Security Assessment Adoption

July 2021

NOTE - Responses to Questions 1-2 (Responding Company, Person Completing Survey) have been removed from this summary printout.

Requester

The Industry Organizations Metrics Team

Requested Information

The North American Transmission Forum (NATF) surveyed our members and external non-NATF member organizations regarding Supply Chain Security Assessment Adoption Survey. The NATF with the Industry Organizations Team designed and continues to improve the Supply Chain Security Assessment Model (Model) helping utilities' supply chain risk identification, assessment and mitigation. The Model and other information can be found here. Below is a short survey that is pertinent to help the Industry Organizations' Team understand how utilities are using the NATF Model - either in whole, in part, or if their program is influenced by the Model. Your participation in this survey will permit the Model to be refined and increase its future usefulness.

Open Distribution for Supply Chain Materials

Copyright © 2021 North American Transmission Forum ("NATF"). All rights reserved.

The NATF permits the use of the content contained herein ("Content"), without modification; however, any such use must include this notice and reference the associated NATF document name & version number. The Content is provided on an "as is" basis. The NATF makes no and hereby disclaims all representations or warranties (express or implied) relating to the Content. The NATF shall not be liable for any damages arising directly or indirectly from the Content or use thereof. By using the Content, you hereby agree to defend, indemnify, and hold the NATF harmless from and against all claims arising from such use.

For your awareness, the Model purpose statement is as follows:

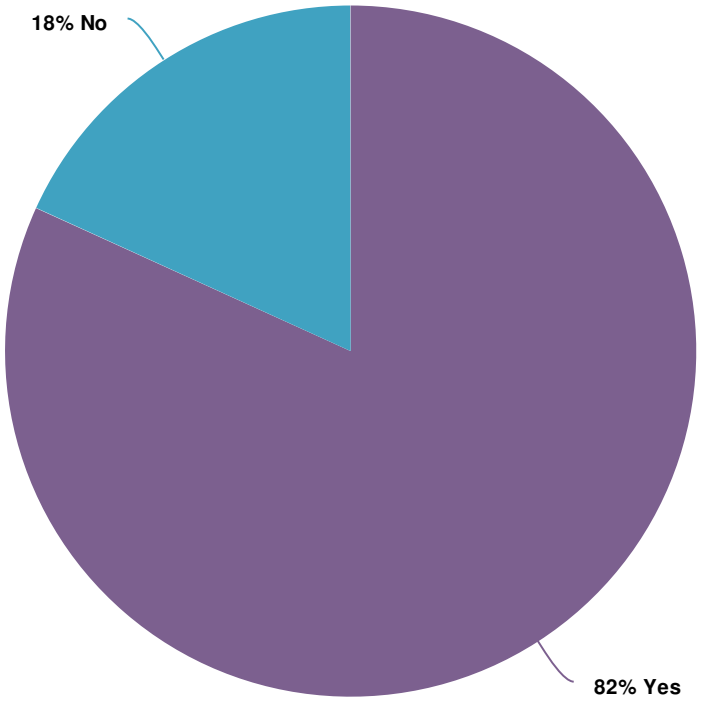
The purpose of the Supply Chain Security Assessment Model (Model) that has been endorsed by industry organizations is to provide a streamlined, effective, and efficient industry-accepted approach for entities to evaluate supply chain security practices, which, if applied widely, *will reduce the burden on suppliers, provide entities with more and better information, and improve supply chain security.*

Results

This report provides a statistical summary of the responses and comments submitted per question. The detailed Excel spreadsheet included in the results material contains the full set of submittals and contact information for each response.

Summary Results - The Industry Organizations Metrics Team - Supply Chain Security Assessment Adoption Survey 09Jul2021

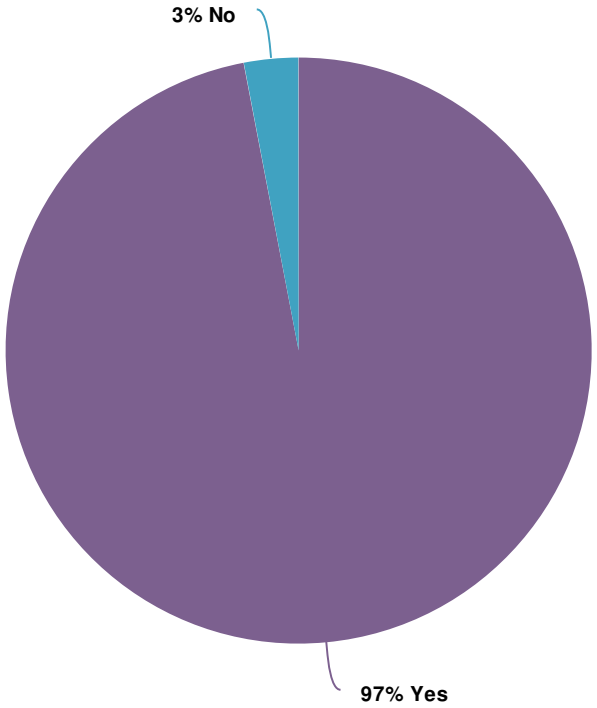
1. Is your organization an NATF member?



Value	Percent	Responses
Yes	81.8%	27
No	18.2%	6

Total: 33

4. Is the topic of this survey (supply chain security) applicable to your company? (If your response is "no," please explain how or why the topic is not applicable in the comments box, then you will be taken to the end of the survey.)



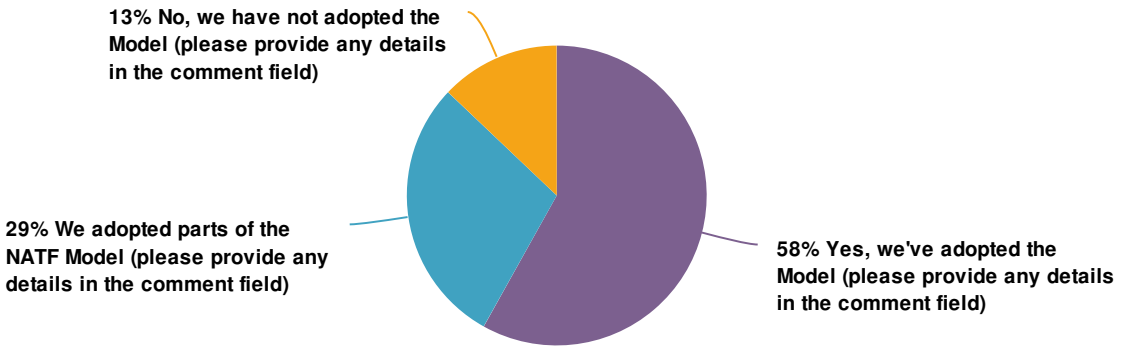
Value	Percent	Responses
Yes	97.0%	32
No	3.0%	1

Total: 33

4. Is the topic of this survey (supply chain security) applicable to your company? (If your response is "no," please explain how or why the topic is not applicable in the comments box, then you will be taken to the end of the survey.) - comments

ResponseID	Response
	Within our company, all contracts with vendors are evaluated individually at a Departmental level with the SMEs and Legal Department. Supply chain security is addressed, but the contract language may vary from contract to contract. For supply chain security related to NERC CIP, we have entered into a contract agreement with another utility where that utility would perform and be responsible for the supply chain security for us.
	We are using the NATF Supply Chain Management survey for our CIP-013 compliance program.
	We are subject to NERC CIP-013 requirements.
	Supply chain security is a critical input into our supply chain and NERC CIP 13 strategies.

5. Has your company adopted the NATF Supply Chain Security Assessment Model (Model) to support your supply chain program?



Value	Percent	Responses
Yes, we've adopted the Model (please provide any details in the comment field)	58.1%	18
We adopted parts of the NATF Model (please provide any details in the comment field)	29.0%	9
No, we have not adopted the Model (please provide any details in the comment field)	12.9%	4

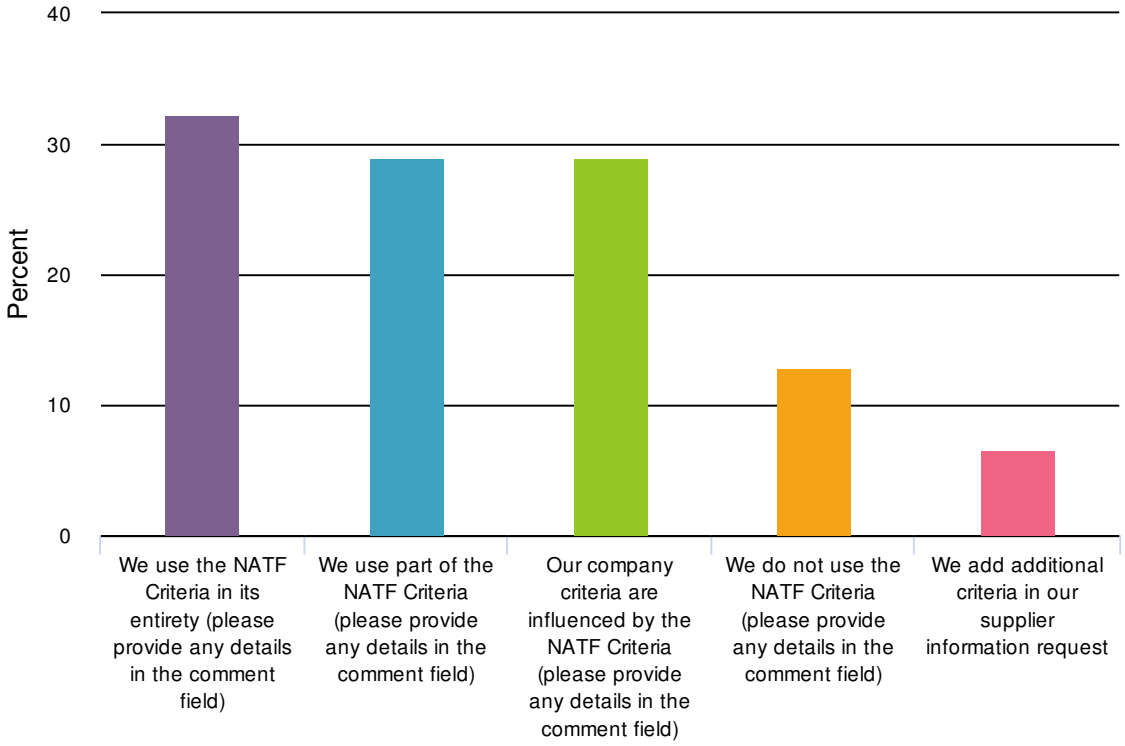
Total: 31

5. Has your company adopted the NATF Supply Chain Security Assessment Model (Model) to support your supply chain program? - comments

ResponseID	Response
	We have adopted a scaled down version of the model via working with a consultant. We also use a third party for vendor risk assessments.
	We use it as it is so that vendors are familiar with it.
	Partially, and mostly just the questionnaire. We used the core CIP-013 questions in the risk questionnaire as basis for our own vendor questionnaire.
	The model and questionnaire were not yet finalized when our program was established.
	We used parts that provide us the most value. We felt internally that the size of the model was very large so we adjusted it in that way.
	We have adopted it in whole, but have highlighted portions that are especially important to our organization.
	Our CIP-013 program doesn't revolve around the NATF Supply Chain Security Assessment Model but follows the same principles and path.
	we utilize the NATF criteria for our questionnaire for our CIP-013 third party risk program
	We use the NATF questionnaire for assessing Vendors.
	Our company's Cyber Security group has a preexisting Third Party Risk Review process in place corporate-wide prior to the implementation of CIP-013. Rather than adopting a new model, the exiting process was modified to address CIP-013. Although our company did not adopt the Model, there are many similarities between the Model and how we evaluate vendors.
	Our SCRM Plan aligns with the model
	We are working with a solution provider to consolidate the various Vendor RiskAssessments, including the CIP-013 assessment (referred to as the VendorCyber Security Assessment, or VCSA), into one assessment. Parts of theNATF model were used to develop the VCSA process.
	Typically, the vendor risk assessment is not a factor that determines one vendor over another.
	Our SCRM Plan aligns with the model

ResponseID	Response
	We have adopted parts of the NATF model. We have also used the following guidance in the development of our consolidated supply chain risk assessment process: NATF: Guidance for CIP-010-3 Software Integrity - Nov 6, 2017 NATF: Cyber Security Supply Chain Risk Management Guidance - June 20, 2018 CIP-013-1 Implementation Guidance - April 3, 2019 NATF: Cyber Security Supply Chain Criteria for Suppliers - July 30, 2019 NATF: Cyber Security Supply Chain Criteria Application Guide - July 30, 2019 NATF: Vendor Remote Access Guidance - December 4, 2019
	We adopt the portions of the NATF Supply Chain Security Assessment Model that make sense for our company since we're a smaller utility.

6. Does your company use the NATF Supply Chain Security Criteria (Criteria) to obtain information for your company's supply chain security program? (Select all that apply)



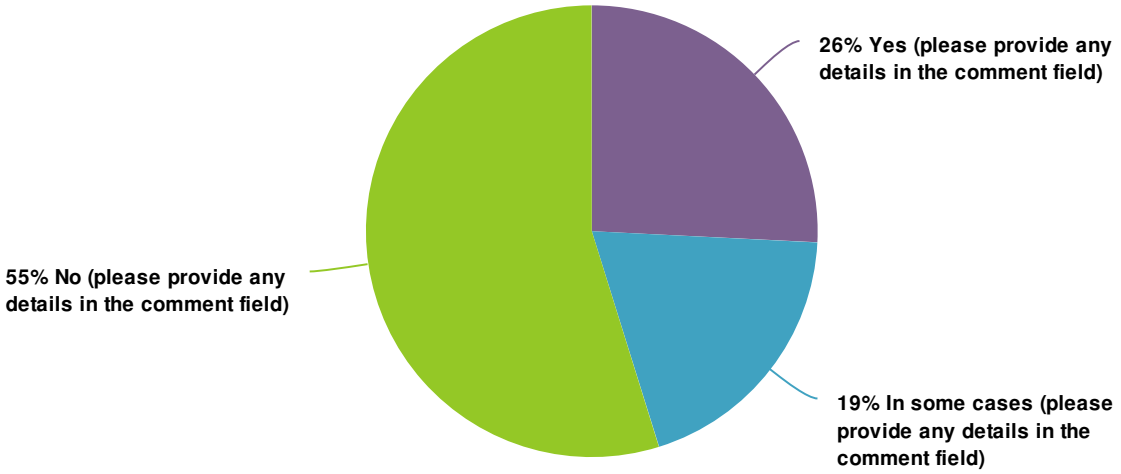
Value	Percent	Responses
We use the NATF Criteria in its entirety (please provide any details in the comment field)	32.3%	10
We use part of the NATF Criteria (please provide any details in the comment field)	29.0%	9
Our company criteria are influenced by the NATF Criteria (please provide any details in the comment field)	29.0%	9
We do not use the NATF Criteria (please provide any details in the comment field)	12.9%	4
We add additional criteria in our supplier information request	6.5%	2

6. Does your company use the NATF Supply Chain Security Criteria (Criteria) to obtain information for your company's supply chain security program? (Select all that apply) - comments

ResponseID	Response
	During our engagement with a consultant, we used the NATF Criteria as a reference point.
	We use approx. 20 of the 60 criteria in performing our vendor risk assessment.
	We used the core CIP-013 questions in the risk questionnaire as basis for our own vendor questionnaire.
	The model and questionnaire were not yet finalized when our program was established.
	We've reviewed all NATF criteria have chosen the most relevant risk for our company and change the wording in the form of a question.
	We removed some questions from the NATF Criteria we felt like were not necessary.
	We. Modified some questions based on our terms and some feedback we received from a few of our most trusted vendors.
	When we send the Supply Chain Security Criteria, we send it in its entirety. In our review, we review all of the material but highlight more critical portions.
	We use a third party vendor for risk assessments but a few times have used the NATF energy sector risk questionnaire for collecting information from vendors. Sometimes a vendor has already completed the NATF questionnaire for another company and we have on certain occasions accepted that for review.
	For service providers or resellers, we have a check box that gives them about half of the criteria as questions, since suppliers were marking N/A for them anyway.
	In an effort to reduce the burden on suppliers while also meeting all cybersecurity requirements, our company assessed the NATF criteria and narrowed the list.
	We developed a questionnaire based on good cyber security practices and incorporated mapping to the items that align with the NATF criteria
	Many of the questions in our VCSA are based on the NATF Supply Chain Security Criteria.

ResponseID	Response
	We partner with a solution provider. Their questionnaire aligns with NATF criteria indirectly.
	We developed a questionnaire based on good cyber security practices and incorporated mapping to the items that align with the NATF criteria
	We used the NATF Supply Chain Security Criteria for guidance when we developed our security supply chain program. As result, we presently use third party audit report(s), SME knowledge & experience with a vendor, established incident response processes, a questionnaire development by our procurement department, and any other data source deemed appropriate to obtain information for our supply chain security program. Our risk assessment is broken down into five functional categories, BES Cyber System functionality and reliability, BES installation deployment & transition, cyber security controls, transition between vendors, and a general category that groups financial and corporate aspects of the vendor. This information is used to identify, evaluate and assess risk.
	We use a proprietary questionnaire that is influenced by the NATF criteria, but we will also accept a vendor's response if they submit a response based on the NATF criteria.

7. Does your company use a third-party, such as a solution provider, to obtain information about your supplier?



Value	Percent	Responses
Yes (please provide any details in the comment field)	25.8%	8
In some cases (please provide any details in the comment field)	19.4%	6
No (please provide any details in the comment field)	54.8%	17

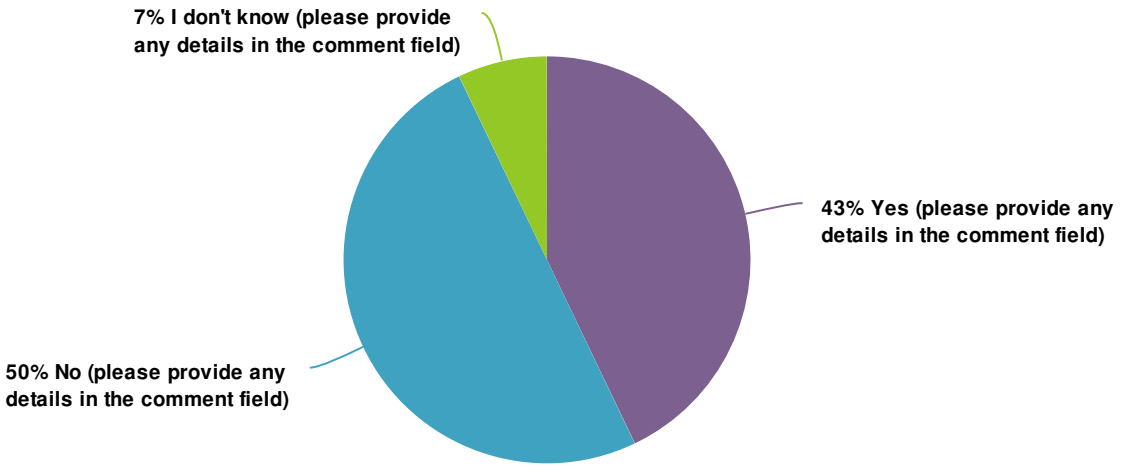
Total: 31

7. Does your company use a third-party, such as a solution provider, to obtain information about your supplier? - comments

ResponseID	Response
	Yes, we use the Asset to Vendor network from Fortress Information Security.
	We are in the RFP process to get a more automated solution.
	We do our own research.
	We perform all vendor risk management functions in house using existing staff.
	A small number of vendors implement certifications like the ISO standards, while most refuse to supply information in a cooperative manner. Third-party solution providers were engaged during the first year of the CIP-013 standard, which resulted in a less-than-satisfactory benefit to actual risk mitigation.
	We have evaluated a solution provider but the cost was deemed to high for the perceived value provided.
	We are currently evaluating service providers in this space.
	We use a solution provider.
	We are looking at this option but are not doing so currently.
	In some cases when we use a contractor to purchase and install equipment, the contractor responds to the questionnaire for related equipment. We are working on getting responses directly from the supplier as well.
	We work with solution provider and the vendor to collect information using a questionnaire. If a vendor does not cooperate by answering the questionnaire, the solution provider will perform a data driven assessment using varying public methods to gather as much information as possible.
	Not at this time, something that we may consider in the future.
	Our company utilizes a solution provider for monitoring and scoring of some high-risk vendors.
	We looked into a solution provider, but do not have it yet
	The third party only provides scoring for vendors that have public information available.

ResponseID	Response
	We looked into a solution provider, but do not have it yet
	At the moment, we use Dun & Bradstreet (D&B) reporting to evaluate solvency, history and overall corporate structure of a vendor. However, we are also researching other solution providers.
	We have partnered with the Department of Energy (DOE) SCRM to obtain supplier information.

8. Since your company uses a third-party at least in some cases to obtain information, does your company's third-party use or include the NATF Criteria?



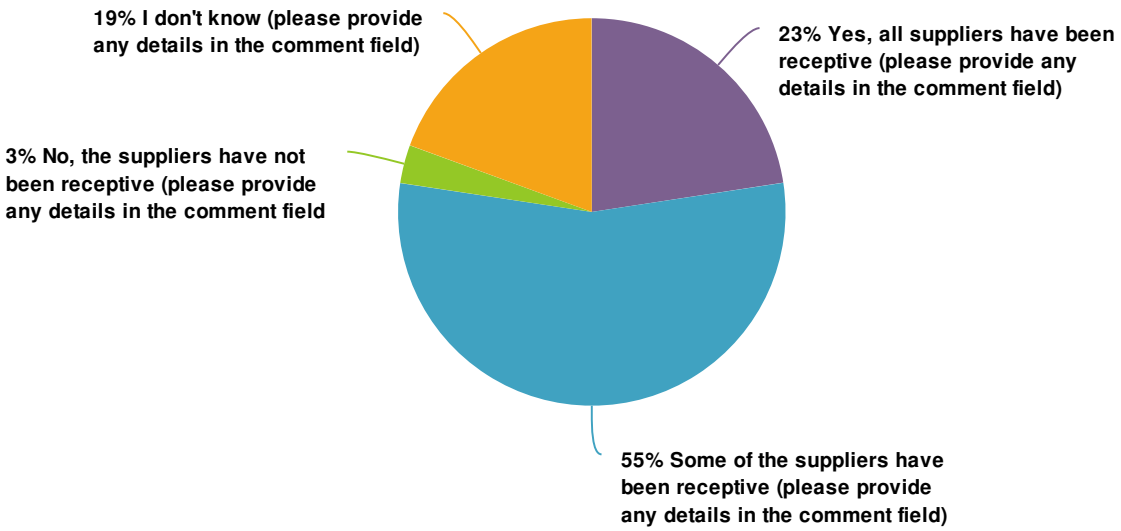
Value	Percent	Responses
Yes (please provide any details in the comment field)	42.9%	6
No (please provide any details in the comment field)	50.0%	7
I don't know (please provide any details in the comment field)	7.1%	1

Total: 14

8. Since your company uses a third-party at least in some cases to obtain information, does your company's third-party use or include the NATF Criteria? - comments

ResponseID	Response
	My understanding is that Fortress uses the NATF Criteria.
	Third parties use other standard risk questionnaires, primarily based on existing standards like ISO.
	None of the companies we have currently contacted have made use of the NATF Criteria or Questionnaire, however they all understand the benefit of the use of a common questionnaire.
	Our solution provider does not use NATF's Criteria.
	I think there are many similar questions but there are more questions in the third party questionnaire than the NATF energy sector questionnaire.
	The third party makes an evaluation based on publicly reviewable security posture, such as patching on internet facing systems.
	Information obtained by our third party is at the direction of our company, which is informed by NATF Criteria.
	See response to question #6
	They use a maturity assessment approach - not a tactical controls assessment
	N/A
	The DOE SCRM developed a customizable questionnaire with a series of up to nineteen (19) control questionnaires. These control questionnaires are mapped to the NERC-CIP, NIST 800-53, and NIST 800-161 special publications.
	Yes, our solution provider has our proprietary questionnaire which is influenced by the NATF criteria.

9. Have the suppliers used by your company been receptive to responding to the NATF Criteria?



Value	Percent	Responses
Yes, all suppliers have been receptive (please provide any details in the comment field)	22.6%	7
Some of the suppliers have been receptive (please provide any details in the comment field)	54.8%	17
No, the suppliers have not been receptive (please provide any details in the comment field	3.2%	1
I don't know (please provide any details in the comment field)	19.4%	6

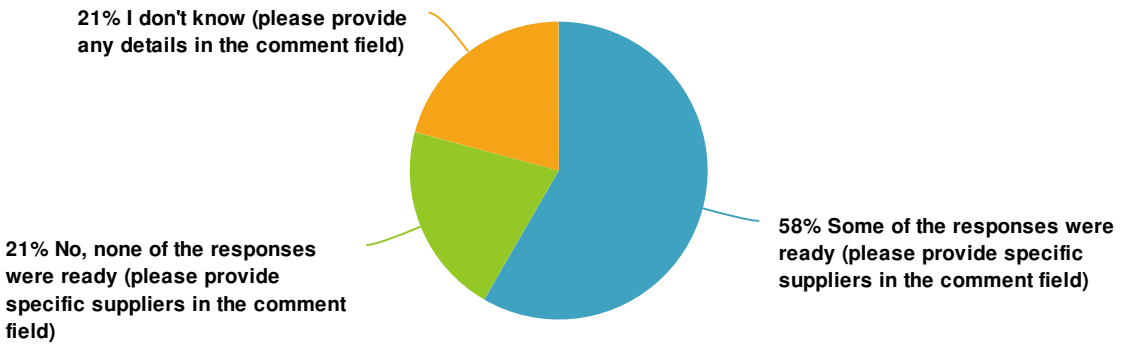
Total: 31

9. Have the suppliers used by your company been receptive to responding to the NATF Criteria? - comments

ResponseID	Response
	Some assessments are tougher to get completed than others.
	I would say 50% actually have taken the time to fill it out.
	80% have been responsive; 20% have been resistant...
	We use the criteria internally for the risk assessment and do not send it the vendors
	There seems to be a sweet spot. Larger vendors like Microsoft just send a canned package of information. Smaller equipment vendors were sometimes clueless didn't know how to respond.
	Have not used the NATF Criteria, as stated in question #6.
	Those that we've had good working relationships with have responded. Large resellers are not receptive.
	Many have been receptive, however, we have had difficulty obtaining response from the larger general technology players.
	Some suppliers were happy to fill out the questions associated with the NATF Criteria. However some Vendors are reluctant and point us to other sources of information.
	We started very early so in the beginning we got good response. We are seeing a decline now with new or updating vendors. They seemed to want to provide a canned response. We are also still seeing companies act dumbfounded about the standard. This is particularly frustrating since one of them provide regular input and have been on the NATF team. It seems they are not good at getting the info communicated within their company
	Use of the NATF questionnaire is still relatively new for vendors and suppliers, and there is a bit of a learning curve to get them to accept this solution.
	We've only used NATF material for a few vendors. In general, some vendors have not been receptive to a questionnaire. More vendors have not been willing to sign our CIP-013 Ts & Cs.
	I would say 90% or more have been receptive due to it being short (26 org. and 60 criteria)
	Yes, but some had a lot of questions about it. Also, turnaround time is anywhere from 3-8 weeks with multiple reminders to do it.

ResponseID	Response
	Occasionally, suppliers will push back but respond to the criteria once they understand it is a requirement for doing business with the company.
	We proactively assessed existing Vendors. Most responded to our unique questionnaire that contains the NATF Criteria
	There is some push-back and discuss with vendors however, we come to agreement on responding.
	we rely heavily on data driven vendor evaluations performed by our solution provider. Very few vendors have agreed to respond to the 400+ questionnaire.
	Some vendors already used NATF, which we accepted. Our preference is to use our contract language and the third party maturity assessment to manage risk. We don't use NATF as a primary tool
	We proactively assessed existing Vendors. Most responded to our unique questionnaire that contains the NATF Criteria
	Please see answer to question number 8 above.
	While the majority of our suppliers have been receptive, some have refused to respond. Not all have provided specific concerns, however examples include confidentiality, technical resource availability, and maturity level concerns.
	Generally, utility industry suppliers are receptive, but vendors that cross industries are less receptive and want to use other responses that are already prepared (e.g., SOC 2).

10. Since at least some of the suppliers have been receptive to responding to the NATF Criteria, have those suppliers been prepared with responses to the Criteria (i.e., they had pre-populated responses)?



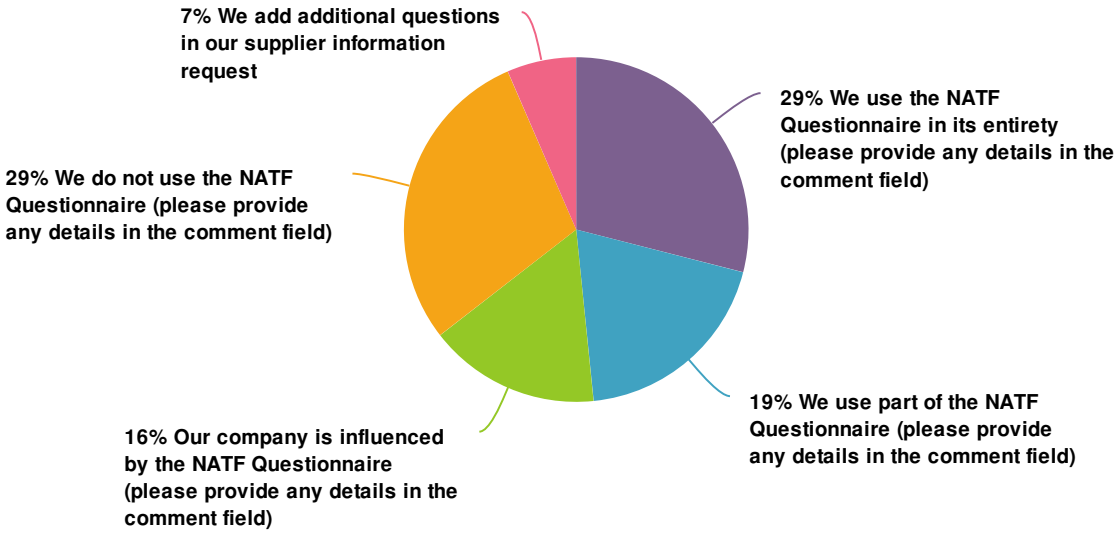
Value	Percent	Responses
Some of the responses were ready (please provide specific suppliers in the comment field)	58.3%	14
No, none of the responses were ready (please provide specific suppliers in the comment field)	20.8%	5
I don't know (please provide any details in the comment field)	20.8%	5

Total: 24

10. Since at least some of the suppliers have been receptive to responding to the NATF Criteria, have those suppliers been prepared with responses to the Criteria (i.e., they had pre-populated responses)? - comments

ResponseID	Response
	This is handled by Fortress Information Security for us.
	Most vendors familiar with it just handed us the filled out form they keep on file.
	a few vendors had pre-populated responses; most did it for the first time in response to our requests
	It was hard to tell if the answers we got were from prepared sources.
	The criteria we have is posed as a question with checkboxes as selections.
	Yes it seems the have create canned response packages to most of the model.
	None of the responses were ready when we sent the request, but several were working on their responses for multiple customers.
	I'm not 100% sure but at least one of the vendors had already completed the NATF energy sector questionnaire.
	Many companies have cybersecurity departments that respond to these questions on a regular basis. In those cases, the suppliers are able to cut and paste the responses.
	We proactively assessed existing Vendors. Most responded to our unique questionnaire that contains the NATF Criteria. Some provided other information that contained the information in our questionnaire.
	We proactively assessed existing Vendors. Most responded to our unique questionnaire that contains the NATF Criteria. Some provided other information that contained the information in our questionnaire.
	DOE SCRM questionnaire is influenced by the NATF questionnaire; however, responses may require translation.

11. Does your company use the Energy Sector Supply Chain Risk Questionnaire (known as the "NATF Questionnaire") to obtain information for your company's supply chain program?



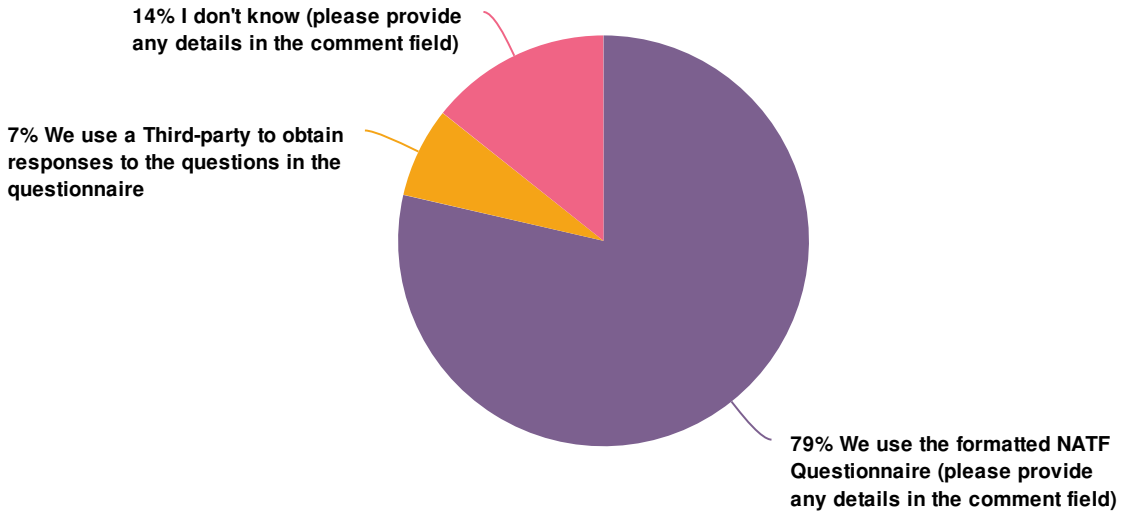
Value	Percent	Responses
We use the NATF Questionnaire in its entirety (please provide any details in the comment field)	29.0%	9
We use part of the NATF Questionnaire (please provide any details in the comment field)	19.4%	6
Our company is influenced by the NATF Questionnaire (please provide any details in the comment field)	16.1%	5
We do not use the NATF Questionnaire (please provide any details in the comment field)	29.0%	9
We add additional questions in our supplier information request	6.5%	2

Total: 31

11. Does your company use the Energy Sector Supply Chain Risk Questionnaire (known as the "NATF Questionnaire") to obtain information for your company's supply chain program? - comments

ResponseID	Response
	We ask the providers to format it so they can complete the applicable cells.
	We used the core CIP-013 questions in the risk questionnaire as basis for our own vendor questionnaire.
	The model and questionnaire were not yet finalized when our program was established.
	We used the base for our start. We did reduce the number and changes some terms to match our company terms.
	When we send the Supply Chain Security Questionnaire, we send it in its entirety. In our review, we review all of the material but highlight more critical portions.
	It's not our main avenue for collection information but if a vendor provides this information, we will accept it for review and assessment.
	we are using the NATF Criteria instead
	Our company has developed its own questionnaire.
	We developed a questionnaire prior to the NATF questionnaire being available. This questionnaire is based on good cyber security practices and incorporates mapping to the items that align with the NATF criteria. These items are similar to the NATF questionnaire, and we will re-evaluate our alignment during the annual review.
	We use the VCSA, not the NATF Questionnaire.
	We use a condensed version of the NATF Questionnaire.
	We developed a questionnaire prior to the NATF questionnaire being available. This questionnaire is based on good cyber security practices and incorporates mapping to the items that align with the NATF criteria. These items are similar to the NATF questionnaire, and we will re-evaluate our alignment during the annual review.
	Our company's procurement uses its own questionnaire as described in the answer to question 6.

12. Does your company use the formatted or unformatted Questionnaire?



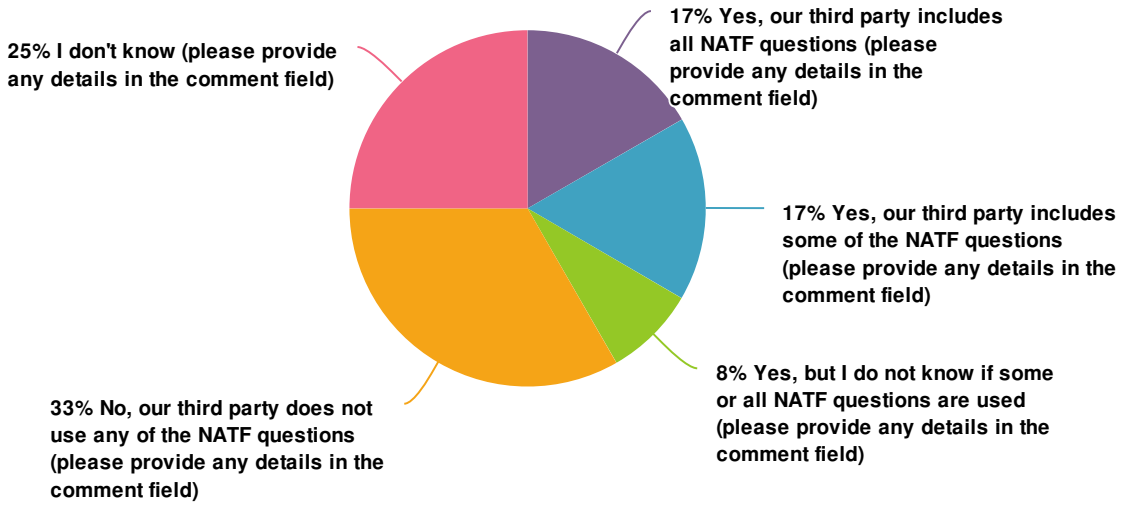
Value	Percent	Responses
We use the formatted NATF Questionnaire (please provide any details in the comment field)	78.6%	11
We use a Third-party to obtain responses to the questions in the questionnaire	7.1%	1
I don't know (please provide any details in the comment field)	14.3%	2

Total: 14

12. Does your company use the formatted or unformatted Questionnaire? - comments

ResponseID	Response
	We copied and pasted from the formatted questionnaire to create our own version.
	We use a questionnaire that we created ourselves, based on the NATF Questionnaire.

13. Since your company uses a third-party to obtain information, does your third-party use or include questions from the NATF Questionnaire?



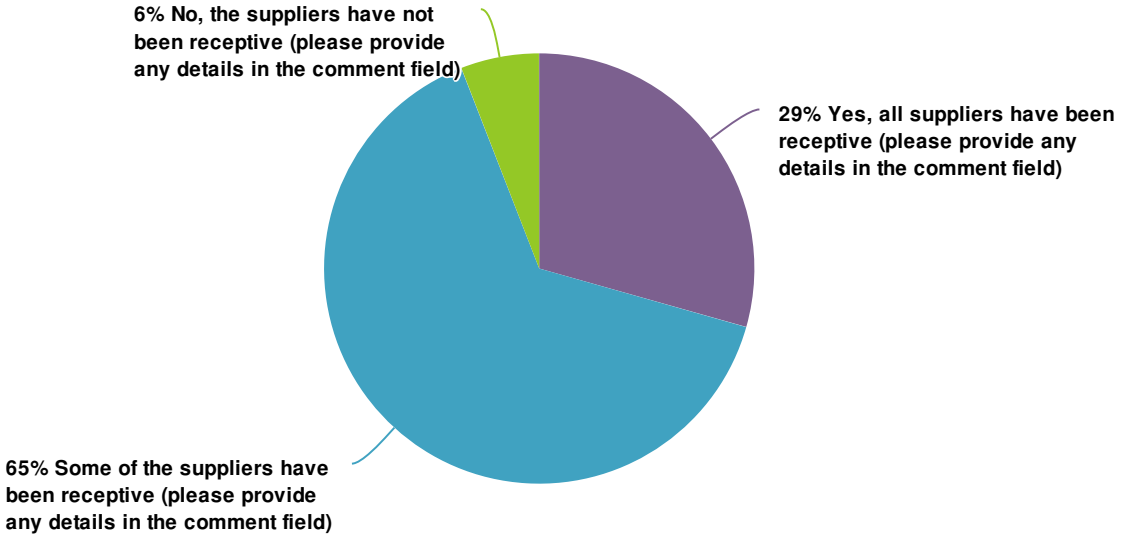
Value	Percent	Responses
Yes, our third party includes all NATF questions (please provide any details in the comment field)	16.7%	2
Yes, our third party includes some of the NATF questions (please provide any details in the comment field)	16.7%	2
Yes, but I do not know if some or all NATF questions are used (please provide any details in the comment field)	8.3%	1
No, our third party does not use any of the NATF questions (please provide any details in the comment field)	33.3%	4
I don't know (please provide any details in the comment field)	25.0%	3

Total: 12

13. Since your company uses a third-party to obtain information, does your third-party use or include questions from the NATF Questionnaire? - comments

ResponseID	Response
	Third parties use other standard risk questionnaires, primarily based on existing standards like ISO.
	We have not finalized an agreement, however the finalists have all indicated we can make use of the NATF Questionnaire, and map it into their question set.
	I'm not completely sure of how much but there is some overlap in questions between the two.
	Our process includes a third party effort and an internal effort; all NATF questions are covered.
	Please see answer to question 8.
	The DOE SCRM developed a customizable questionnaire with a series of up to nineteen (19) control questionnaires. These control questionnaires are mapped to the NERC-CIP, NIST 800-53, and NIST 800-161 special publications.

14. Have the suppliers used by your company been receptive to responding to the NATF Questionnaire?



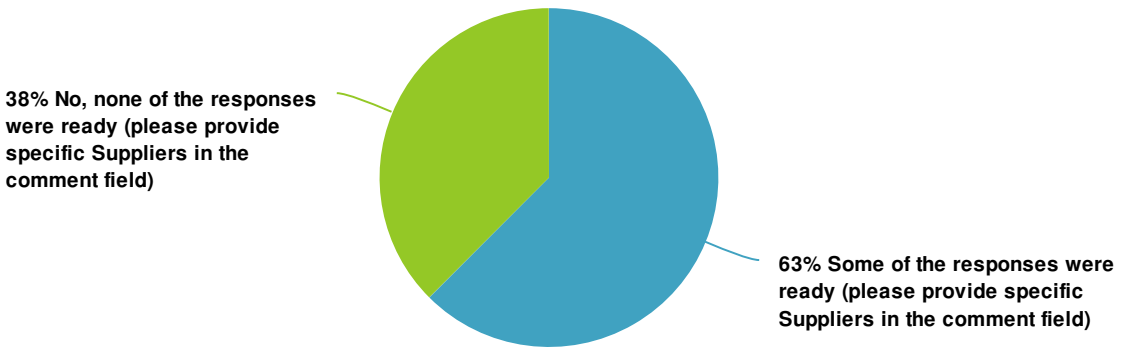
Value	Percent	Responses
Yes, all suppliers have been receptive (please provide any details in the comment field)	29.4%	5
Some of the suppliers have been receptive (please provide any details in the comment field)	64.7%	11
No, the suppliers have not been receptive (please provide any details in the comment field)	5.9%	1

Total: 17

14. Have the suppliers used by your company been receptive to responding to the NATF Questionnaire? - comments

ResponseID	Response
	same as above: 80/20 have been receptive/npn-receptive
	There seems to be a sweet spot. Larger vendors like Microsoft just send a canned package of information. Smaller equipment vendors were sometimes clueless didn't know how to respond.
	Many have been receptive, however, we have had difficulty obtaining response from the larger general technology players.
	Use of the NATF questionnaire is still relatively new for vendors and suppliers, and there is a bit of a learning curve to get them to accept this solution.
	In some cases, suppliers have questions about the relevance of questions and need to be educated on why the questionnaires are necessary.
	The NATF questionnaire does require some education for vendors that are not electric utility industry specific and some are reluctant to complete it.

15. Since at least some of the suppliers have been receptive to responding to the NATF Questionnaire, have those suppliers been prepared with responses to the Questionnaire (i.e., they had a questionnaire ready with pre-populated responses)?



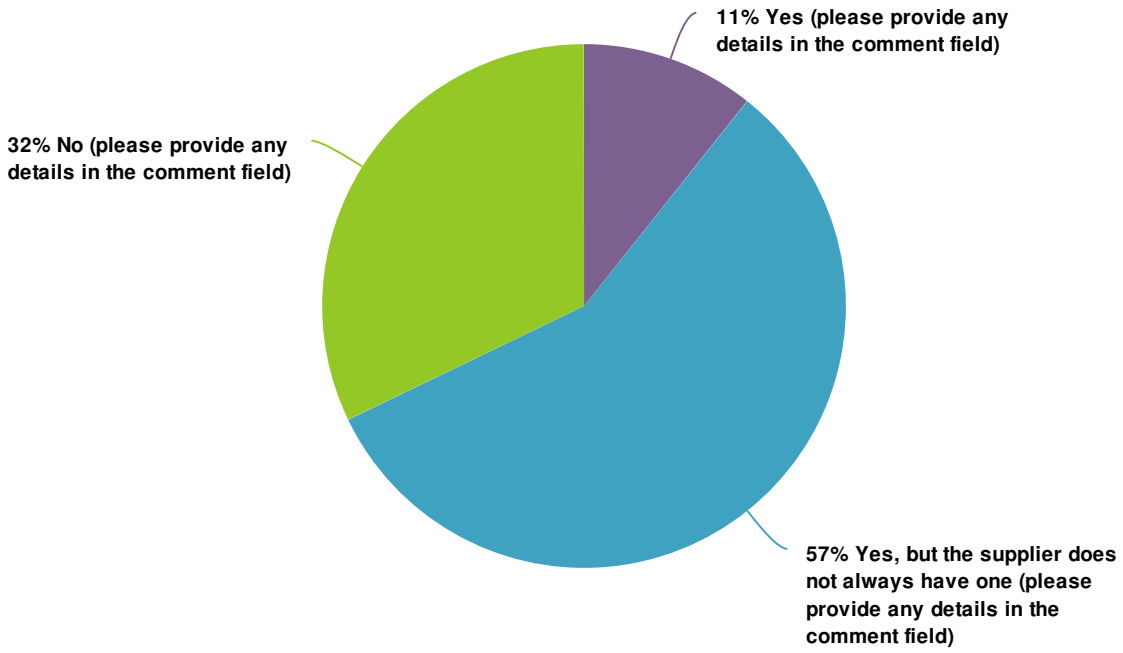
Value	Percent	Responses
Some of the responses were ready (please provide specific Suppliers in the comment field)	62.5%	10
No, none of the responses were ready (please provide specific Suppliers in the comment field)	37.5%	6

Total: 16

15. Since at least some of the suppliers have been receptive to responding to the NATF Questionnaire, have those suppliers been prepared with responses to the Questionnaire (i.e., they had a questionnaire ready with pre-populated responses)? - comments

ResponseID	Response
	It was hard to tell if the answers we got were from prepared sources.
	None of the responses were ready when we sent the request, but several were working on their responses for multiple customers.

16. Does your company request one or more third-party verifications (a certification or qualified assessment e.g., ISO 27001, IEC 62443 or a SOC II) to verify the suppliers' responses?



Value	Percent	Responses
Yes (please provide any details in the comment field)	10.7%	3
Yes, but the supplier does not always have one (please provide any details in the comment field)	57.1%	16
No (please provide any details in the comment field)	32.1%	9

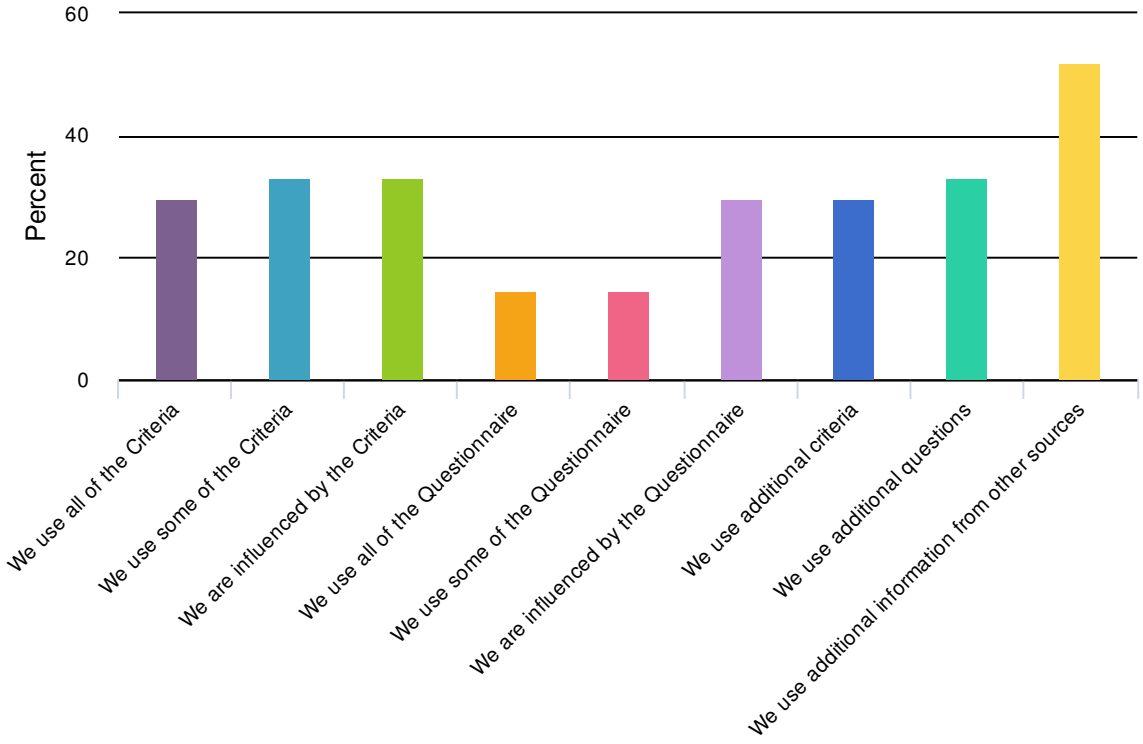
Total: 28

16. Does your company request one or more third-party verifications (a certification or qualified assessment e.g., ISO 27001, IEC 62443 or a SOC II) to verify the suppliers' responses? - comments

ResponseID	Response
	This is handled by Fortress Information Security.
	It is easy to map certain certifications to the controls but not all companies have this.
	We ask politely for evidence but aren't vigorous about following up if they ignore us.
	The majority of the vendors we have engaged do not have any third-party certifications and those that do not are also not willing to negotiate the inclusion of terms to support third-party audit controls.
	We ask if a supplier has a certification and if they can provide the the certification should we need it.
	If they have one of those they can supply it and it reduces the questions we ask.
	Our organization typically requests a SOC II report or a ISO 27001. Not all vendors have been able to supply these.
	We don't request but have received SOC2s once or twice. We treat it as icing on the cake and use it for our review and assessment process.
	If the supplier has a certification (ISO, IEC) we obtain a copy of the certification
	ISO 27001 certification
	Our company always asks for a third party verification, but it is not required because we understand the supplier may not have one in the utility sector.
	We request third-part verifications if the Vendor has them
	N/A
	We ask for validation based on the risk of the product/service. In low risk cases, we rely on the attestations of the vendor. For higher risk cases, we request evidence of practices (done by our third party vendor)
	We request third-party verifications if the Vendor has them

ResponseID	Response
	We have not had to request for a third party assessment at the moment because we have only completed assessment on existing vendors for purchases after October 1, 2020. We already have sufficient work history and SME expertise to complete assessments. However, our program allows for third party verifications/audits/certifications. That stated, if a third party verification is necessary for new vendors, we will make the sufficient request at that time.
	Third party verifications may be submitted as part of the attestation to controls; however, they are not requested.
	Some vendors, such as wholesalers, do not have this level of third-party verifications.

17. Does your company use the information obtained through the NATF Criteria or Questionnaire to identify supplier risks and evaluate a supplier's supply chain security posture? (select all that apply)

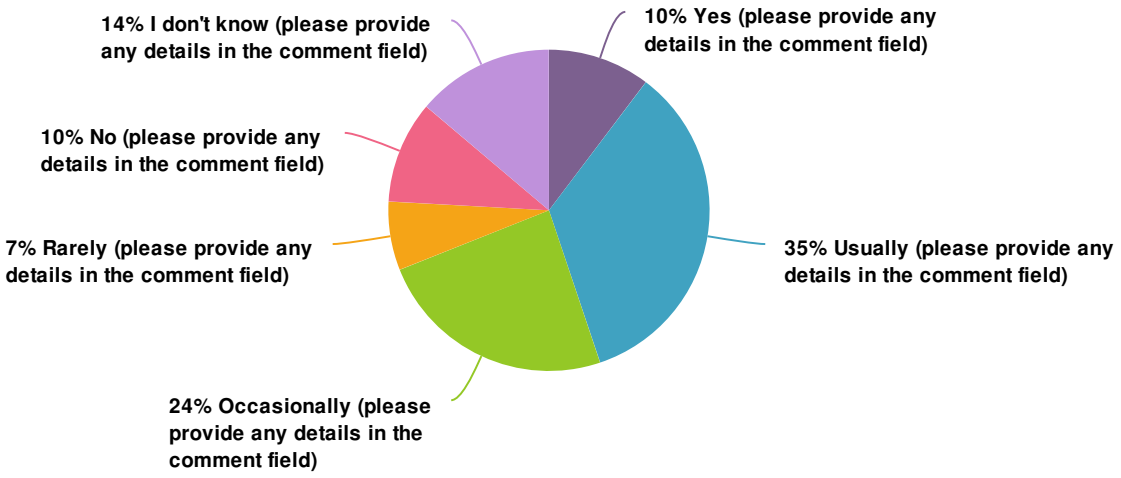


Value	Percent	Responses
We use all of the Criteria	29.6%	8
We use some of the Criteria	33.3%	9
We are influenced by the Criteria	33.3%	9
We use all of the Questionnaire	14.8%	4
We use some of the Questionnaire	14.8%	4
We are influenced by the Questionnaire	29.6%	8
We use additional criteria	29.6%	8
We use additional questions	33.3%	9
We use additional information from other sources	51.9%	14

17. Does your company use the information obtained through the NATF Criteria or Questionnaire to identify supplier risks and evaluate a supplier's supply chain security posture? (select all that apply) - comments

ResponseID	Response
	We use it as part of our Selection Advisory Committee rankings.
	If the vendor is not responsive to the questionnaire we perform the risk assessment using additional criteria from other souces.
	The criteria was not established when we developed our program, so we developed criteria independent of these resources.
	We tried to use it along with our own already developed questions. We had been doing risk assessment for a few years before the standard. The standard just expanded our program.
	We use selected questions from the NATF criteria, open-source research by the sybersecurity analysts, and vendor supplied supporting documentation (ISO, SOC, Pentest, etc).
	We use our VCSA process (which is based in part on the NATF criteria) to gather information on vendors.
	We utilize an internally created questionnaire, based on the NATF Questionnaire, and a score from a third-party assessor, to create a risk rating for each vendor.
	As we previously identified, our plan does not presently utilize the NATF Questionnaire. However, we have created our own risk identification and assessment process by utilizing NATF guidance (and other industry guidance). We have also used some aspects of the NATF Supply Chain Security Criteria risk areas: (1) Access Control and Management, (2) Governance, (3) Incident Response, (4) Information Protection and (5) Vulnerability Management. Access Control & Management Our plan leverages our access management processes and controls to manage risk for physical, electronic and BCSI access. However, we do evaluate risks (if applicable) associated with chain of custody and protection during delivery and/or installation. We also evaluate risk associated with electronic access, interactive remote access, and system to system remote access. Governance Some of the supply chain criteria that fall under governance are risks that fall under the last or "General" category of our company's c

18. Are your company's suppliers willing to work with your company to mitigate identified risks with their products?



Value	Percent	Responses
Yes (please provide any details in the comment field)	10.3%	3
Usually (please provide any details in the comment field)	34.5%	10
Occasionally (please provide any details in the comment field)	24.1%	7
Rarely (please provide any details in the comment field)	6.9%	2
No (please provide any details in the comment field)	10.3%	3
I don't know (please provide any details in the comment field)	13.8%	4

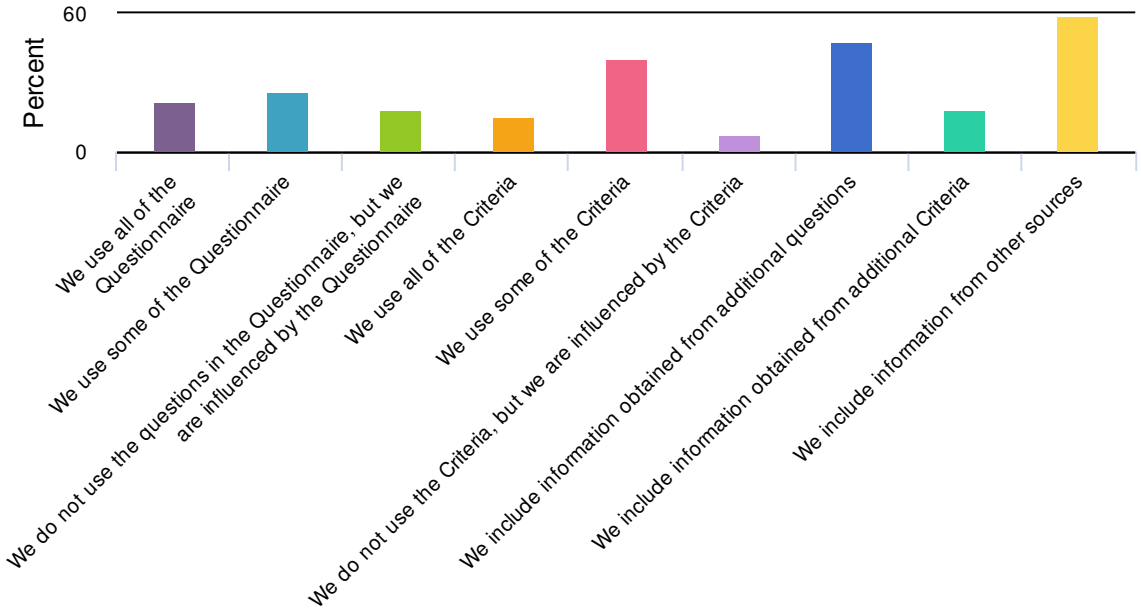
Total: 29

18. Are your company's suppliers willing to work with your company to mitigate identified risks with their products? - comments

ResponseID	Response
	We have not had an instance where we needed to work with suppliers to mitigate any risks. We have a very low volume of in-scope procurements.
	Most companies take the approach of "as is" so we have to perform mitigating activities.
	We haven't had any issues to date.
	Our initial evaluations were more along the lines of data collection, so we did not press (hard) on our vendors when risks were identified. That data informed a risk score for each vendor that will drive decision-making for future purchases from that supplier.
	Some vendors are proactively addressing risks and agree to our risk mitigation controls identified in our terms. Others outright refuse to negotiate the inclusion of any of our terms, forcing a manual risk evaluation to determine if the requested controls are being performed without an agreement or formally for our organization.
	Most mitigations fall on our company's responsibility.
	Some have been some have really pushed back hard.
	We'd had some suppliers provide follow up information as requested but sometimes questions go unanswered and we receive partially completed questionnaires. This is when we use other alternatives for vendor assessment such as public data driven assessments.
	still new working with OT suppliers with this
	Contract Terms and Conditions and Questionnaire attestations satisfy this need based on the level of risk posed by that Vendor
	Depends on the vendor.
	We were able to have vendors that agreed to alter their shipping processes to address concerns over tamper-proofing.
	We base our risk assessment off known deficiencies and identify internal controls to mitiage risk. Rarely do we require a vendor to provide further remediation.
	Not enough experience with this scenario yet to give a good answer

ResponseID	Response
	Contract Terms and Conditions and Questionnaire attestations satisfy this need based on the level of risk posed by that Vendor
	We have not had a new vendor whose risks required a mitigation beyond those already stipulated in our contracts,
	The process is immature; however, indications are that suppliers are willing to improve in this space.
	We have not had this situation yet.

19. Does your company use the information obtained through the NATF Criteria and Questionnaire in your risk assessment for the supplier? (select all that apply)

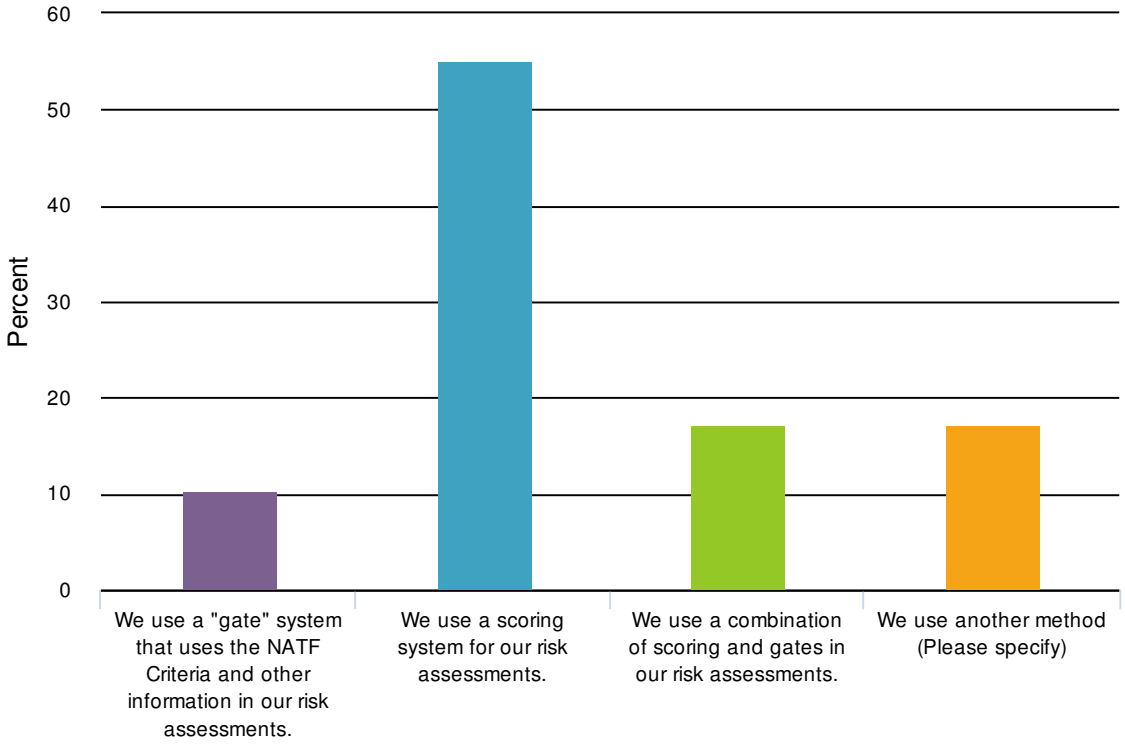


Value	Percent	Responses
We use all of the Questionnaire	22.2%	6
We use some of the Questionnaire	25.9%	7
We do not use the questions in the Questionnaire, but we are influenced by the Questionnaire	18.5%	5
We use all of the Criteria	14.8%	4
We use some of the Criteria	40.7%	11
We do not use the Criteria, but we are influenced by the Criteria	7.4%	2
We include information obtained from additional questions	48.1%	13
We include information obtained from additional Criteria	18.5%	5
We include information from other sources	59.3%	16

19. Does your company use the information obtained through the NATF Criteria and Questionnaire in your risk assessment for the supplier? (select all that apply) - comments

ResponseID	Response
	We worked with consultant to develop a custom risk questionnaire and assessment.
	Same answer here. We developed our own criteria prior to this being available and find our process to be adequate.
	we use info from our solution provider too
	In an effort to reduce the burden on suppliers while also meeting all cybersecurity requirements our company assessed the NATF criteria and narrowed down the list.
	We use our VCSA process (which is based in part on the NATF criteria) to gather information on vendors.
	We utilize an internally created questionnaire, based on the NATF Questionnaire, and a score from a third-party assessor, to create a risk rating for each vendor.
	Please see answer to question 17.
	We have another source / solution provider that we use during our assessment process.

20. How does your company use the information obtained through the evaluation of the supplier risks, and mitigation of those risks, to conduct a risk assessment for the supplier? (select all that apply)

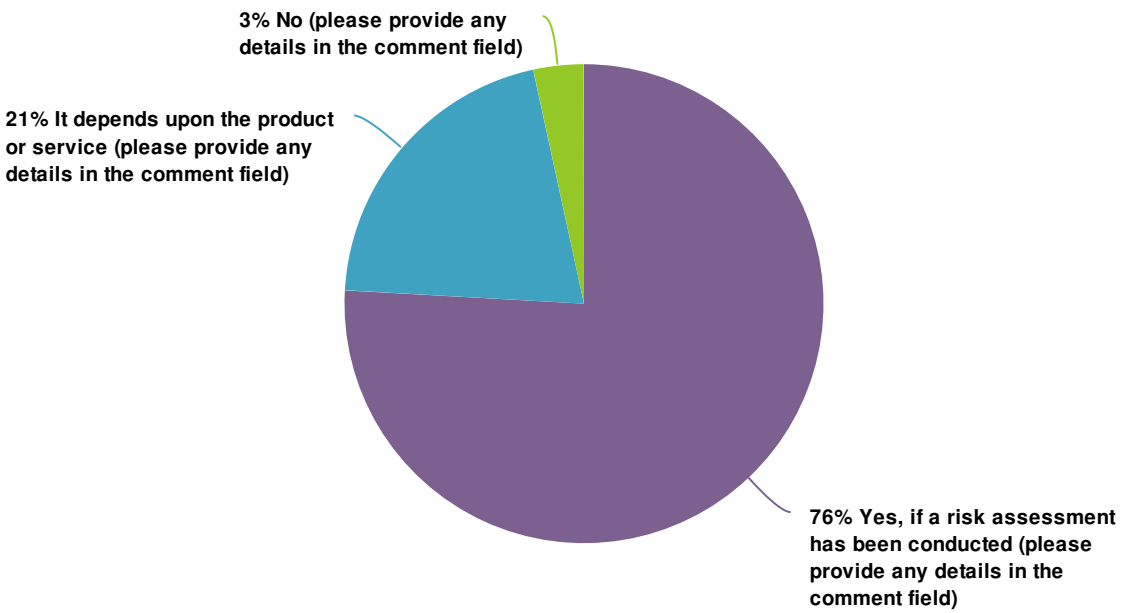


Value	Percent	Responses
We use a "gate" system that uses the NATF Criteria and other information in our risk assessments.	10.3%	3
We use a scoring system for our risk assessments.	55.2%	16
We use a combination of scoring and gates in our risk assessments.	17.2%	5
We use another method (Please specify)	17.2%	5

20. How does your company use the information obtained through the evaluation of the supplier risks, and mitigation of those risks, to conduct a risk assessment for the supplier? (select all that apply) - comments

ResponseID	Response
	We use a custom questionnaire and risk assessment process plus an evaluation and sign off by the asset owner.
	A scoring system is driven by the agreements and information gathered from vendors, which identifies risk. These risks identify areas where we may need to apply additional mitigations to account for controls that vendors do not agree to perform on our behalf.
	We actually have a 2 part scoring system. This allows us to accept some risk without a compliance issue directly related to CIP-013
	Assessments are reviewed and approved by management.
	We are using an overall review process, but looking to change to a scoring system in the near future.
	Our company uses selected questions from the NATF criteria, Open Source research by the cybersecurity analysts and vendor supplied supporting documents (ISO, SOC, Pentest, etc.).
	VCSA scoring is broken into four risk areas. Minimum score for each risk area is based on the impact rating of the BCS / EACMS / PACS that the good or service will be used in. Mitigation is required in any risk area where the vendor failed to reach the minimum score.
	We assume all findings are a risk and identify internal controls necessary to mitigate risk.
	We use scoring by third party maturity assessment, plus agreement to our contract language
	We use a ranking/scoring methodology for our risk assessments. Our risk assessment methodology first determines: • The likelihood of a vendor's product/service adversely impacting the BES; then we determine; • The impact of the vendor's product/service on the BES. The likelihood AND impact of the risk is ranged as "high", "medium" or "low" across the five risk categories listed in question six above: (1) BES Cyber System (BES) functionality and reliability, (2) BES installation deployment & transition, (3) cyber security controls, (4) transition between vendors and a (4) general category. Any risk ranked as medium or high has to be mitigated.

21. Does your company consider the results from your supply chain risk assessment when making purchase decisions?



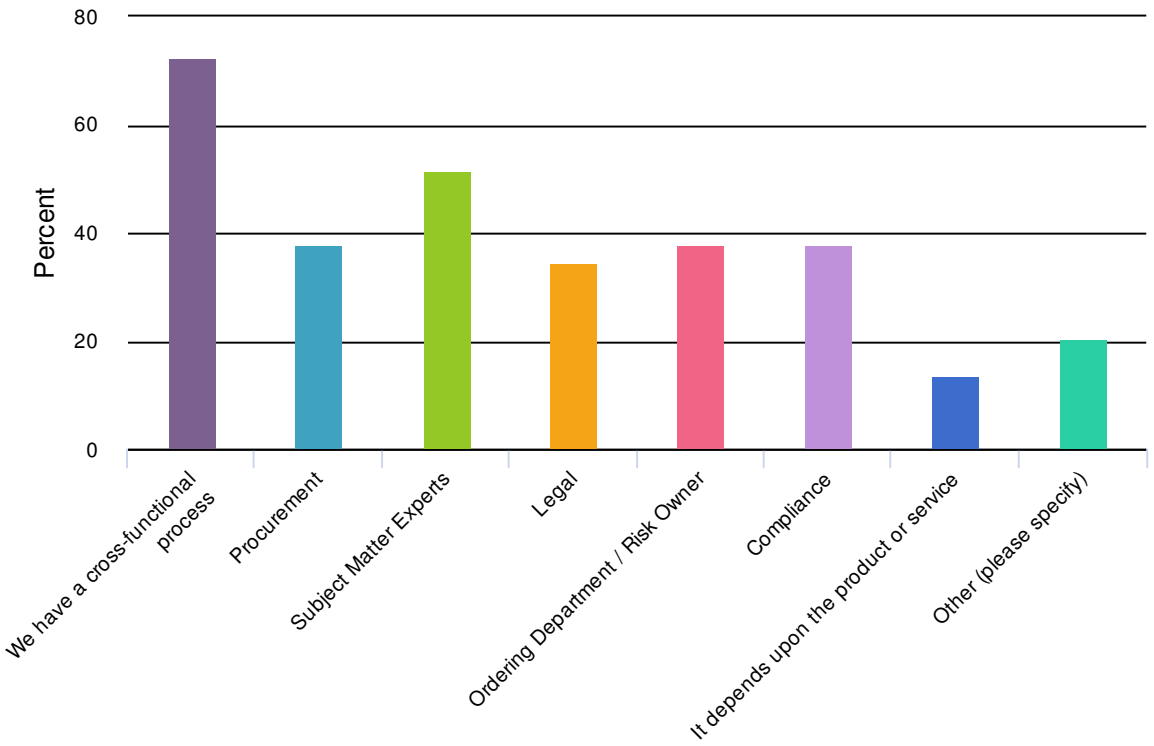
Value	Percent	Responses
Yes, if a risk assessment has been conducted (please provide any details in the comment field)	75.9%	22
It depends upon the product or service (please provide any details in the comment field)	20.7%	6
No (please provide any details in the comment field)	3.4%	1

Total: 29

21. Does your company consider the results from your supply chain risk assessment when making purchase decisions? - comments

ResponseID	Response
	Yes, for any in-scope CIP-013 procurements.
	Yes, we will not proceed with a procurement unless mitigation controls are applied, either by us or the vendor, for risks applicable to the vendor product or service.
	Vendors must be approved via our vendor risk assessment approval process before purchases can be made.
	all part of the overall evaluation
	The Vendor is required to pass a risk assessment in order to become a CIP-Approved supplier. A CIP-Approved Supplier has passed a risk review with appropriate contractual language or a sybersecurity deviation has been signed.
	The results from our supply chain risk assessments determine if we will proceed with the Vendor and may influence how the product will be used.
	We don't want to be caught in a situation where we can't buy from a sole source vendor because they scored poorly on the assessment. The assessment is used to determine what, if any, risk areas require mitigation. It does not drive the purchasing decision.
	The risk assessment results allow a purchase decision to be made, however, the assessment is not a factor in selecting one vendor over another.
	We have not declined a purchase based on the risk assessment. We identify controls necessary to mitigate risks and proceed with procurement.
	Can't always choose not to use a vendor - particularly for niche product areas or for compatibility with existing technology
	The results from our supply chain risk assessments determine if we will proceed with the Vendor and may influence how the product will be used.
	The risk assessment results are used to negotiate terms and conditions should that be necessary to mitigate any assessed risk. Our plan also incorporates sample contract language that could be used in negotiations.
	We have established a risk tolerance threshold with Senior Management elevated risk decisions.
	We've tiered our vendors based on the products that we purchase and risk assess the vendors that are in the highest (riskiest) tiers.

22. Please indicate how your company assesses the overall risk of making a purchase from a supplier - does your company have a cross-functional process, or is there a department(s) that makes the decision? (select all that apply)

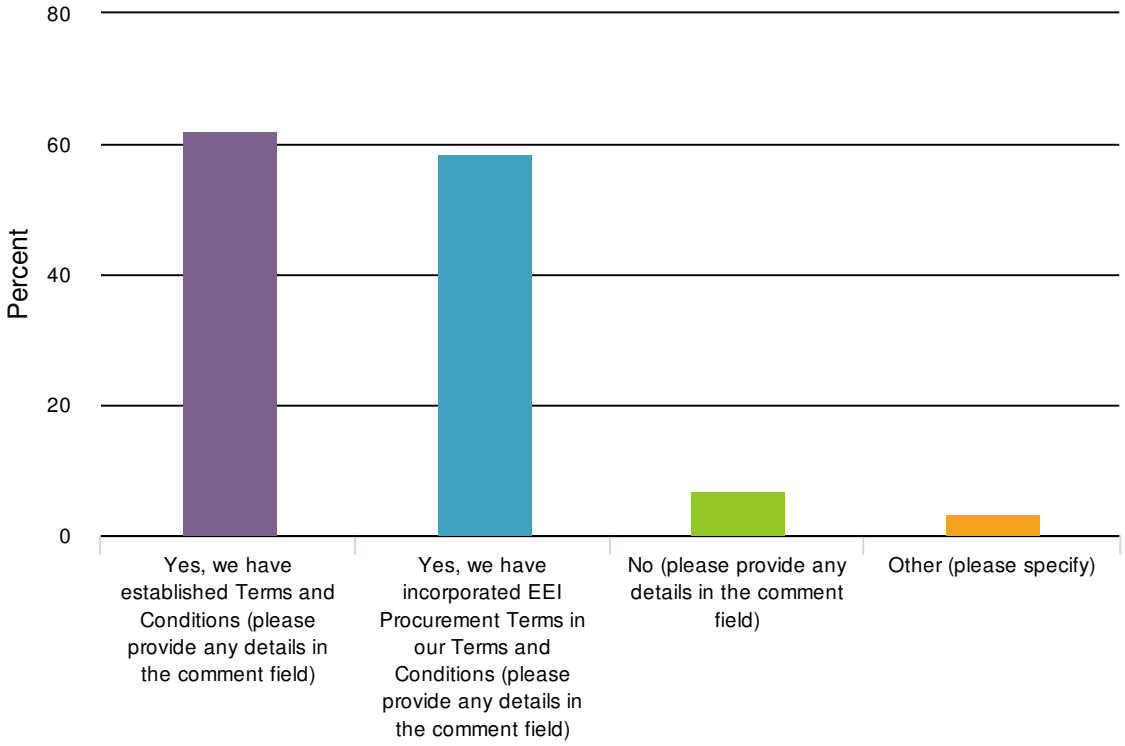


Value	Percent	Responses
We have a cross-functional process	72.4%	21
Procurement	37.9%	11
Subject Matter Experts	51.7%	15
Legal	34.5%	10
Ordering Department / Risk Owner	37.9%	11
Compliance	37.9%	11
It depends upon the product or service	13.8%	4
Other (please specify)	20.7%	6

22. Please indicate how your company assesses the overall risk of making a purchase from a supplier - does your company have a cross-functional process, or is there a department(s) that makes the decision? (select all that apply) - comments

ResponseID	Response
	We have dedicated 3rd Party Risk Management team.
	We are a cooperative, so everyone gets a say in things.
	Risk Assessments for CIP-013 applicable procurements are processed by one department, although occasionally procurement and legal department staff are also engaged for support. Risk assessments for other non-CIP eligible procurements are distributed throughout the organization and largely fall on the purchaser.
	We rely on our Cybersecurity work group to assess the risk based on Questionnaire responses.
	We have a team that could meet if there are questions about the risk. If this team can't come to a conclusion it escalates to an executive.
	Corporate Risk Management and IT
	The Business Unit, Supply chain, and Cybersecurity work together to identify prospective companies to become a CIP-approved Supplier. Regulatory and Legal are available to support as required.
	Cyber Security
	Business Leadership as needed
	Our consolidated supply chain risk management plan requires assessment input from all stake holders of the product or service. This includes, but is not limited to, a multi-disciplinary team made up of SMEs, Legal/Procurement department, compliance, and the department making the purchase.
	We utilize a cross functional team to review third-party risk assessments and develop mitigations based on identified risks.

23. Does your company use contract terms to support any mitigations implemented by the supplier to address supply chain risk? (select all that apply)

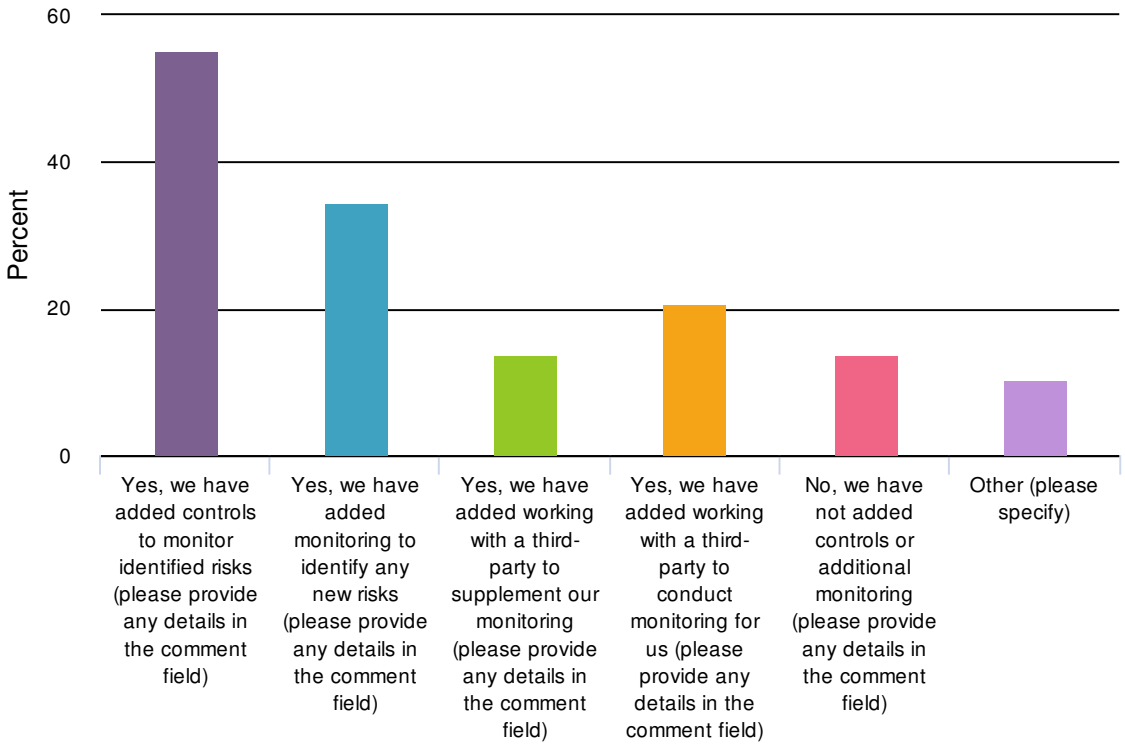


Value	Percent	Responses
Yes, we have established Terms and Conditions (please provide any details in the comment field)	62.1%	18
Yes, we have incorporated EEI Procurement Terms in our Terms and Conditions (please provide any details in the comment field)	58.6%	17
No (please provide any details in the comment field)	6.9%	2
Other (please specify)	3.4%	1

23. Does your company use contract terms to support any mitigations implemented by the supplier to address supply chain risk? (select all that apply) - comments

ResponseID	Response
	We attempt to maintain Master Service Agreements.
	We haven't had any issues to date.
	So far so good with the EEI criteria, which frankly surprises me considering how involved it is. We've found a section or two that most vendors have heartburn with, so we've simply stopped including those words.
	We have formal terms that were base on the EEI language, but have been modified to address additional risk areas and coordinate with other existing risk management agreements (e.g., NDAs, etc.).
	We have developed a security addendum based on the EEI Procurement Terms
	We have had these contract terms since 2010 and they have gone though several updates.
	We have established T&Cs, however we do not use revised T&Cs to address discovered risks.
	Cybersecurity Provisions were created to align with EEI
	Our T&Cs are based largely on the EEI T&Cs. Not exactly the same but very similar in many areas.
	Our T&Cs were influenced by the EEI language.
	We have updated the T&C's of our general services agreement. We have also updated purchase order terms and conditions as well as our access management contract language (Security Requirements Certification Agreement). Our updated General Service Agreement is influenced by language from the EEI Procurement Terms.
	We have developed Supply Chain Security specific Terms and Conditions to be included in technology procurement solicitations.
	We have not had any mitigating implementations.

24. By implementing the supply chain Model, has your company added controls and monitoring processes? (select all that apply)



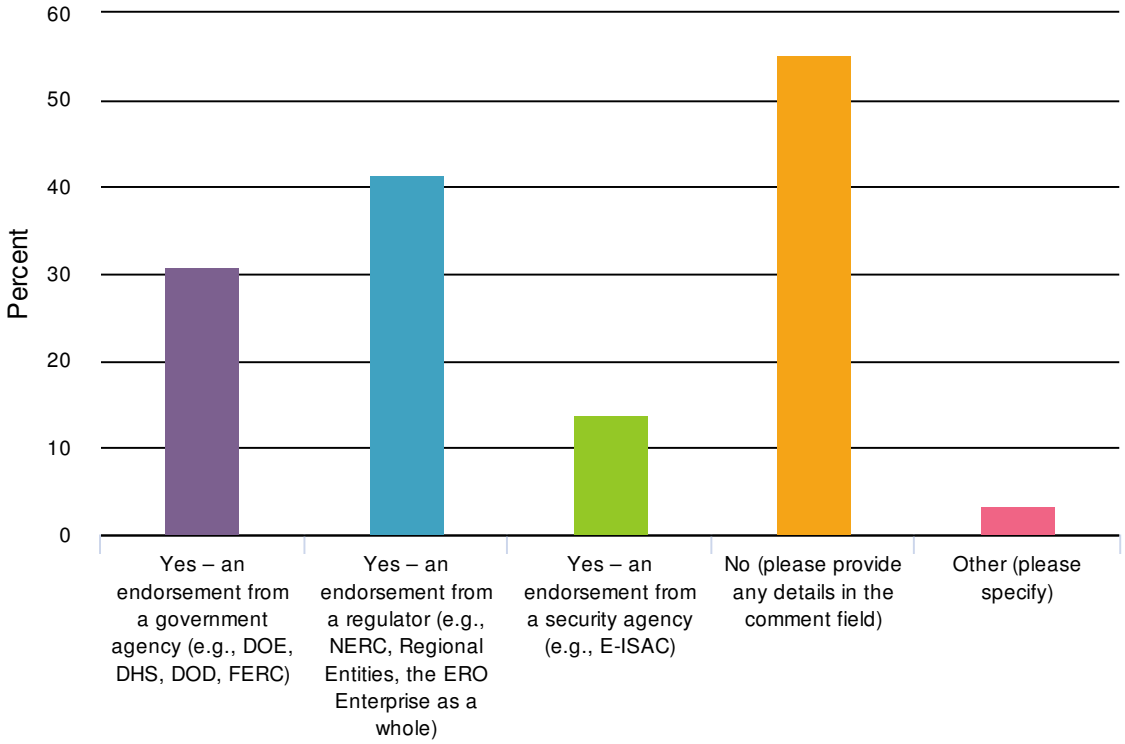
Value	Percent	Responses
Yes, we have added controls to monitor identified risks (please provide any details in the comment field)	55.2%	16
Yes, we have added monitoring to identify any new risks (please provide any details in the comment field)	34.5%	10
Yes, we have added working with a third-party to supplement our monitoring (please provide any details in the comment field)	13.8%	4
Yes, we have added working with a third-party to conduct monitoring for us (please provide any details in the comment field)	20.7%	6
No, we have not added controls or additional monitoring (please provide any details in the comment field)	13.8%	4
Other (please specify)	10.3%	3

24. By implementing the supply chain Model, has your company added controls and monitoring processes? (select all that apply) - comments

ResponseID	Response
	We currently conduct annual updates to the questionnaires. We are looking to move to more dynamic monitoring.
	We're doing bare minimum at this time. Prior to CIP-013 we had no program to speak of, so this is all brand-new ground for us.
	We had existing controls in place prior to the introduction of this program, including monthly activities that are performed to detect new vendor product and service risks. A third-party vendor reputation monitoring tool was used and evaluated in 2020, although was found to provide no value due to the absence of any meaningful data for specific risk indicators associated with our implemented products and services (e.g., monitoring a vendors internet presence, or "curb appeal", does not equate to a risk assessment of a specific product they sell).
	We have a group that monitors things including the use of bitsight
	If our CIP-013 Ts &Cs are agreed upon by the supplier, they agree to inform us of cyber security incidents. We've had several suppliers not agree to our Ts&Cs so we were doing manual monitoring of them via vendor website/correspondence, E-ISAC alerts, US-CERT alerts, etcc...More recently we have partnered with a third party to provide continuous monitoring of our vendors.
	We utilize a solution provider to monitor our high risk suppliers
	We review our existing risk assessments annually. Our compliance tool acts as a control to make sure the timeframe is met.
	Our Company's cybersecurity group already had a third party risk review process in place corporate-wide prior to the implementation of CIP-013. Rather than adopt a new model, the existing process was modified to address CIP-013. Although we did not adopt the Model, there are many similarities between the Model and how we evaluate vendors.
	We implemented triggers at the SMEs discretion based on Vendor notifications, receiving a different model number than what was ordered, equipment failures, or information from internal monitoring services.
	We have added controls, but they are more for controlling compliance risk rather than security risk. The controls for the security risk is the assessment process itself. The compliance controls ensure that the process was followed before placing the good or service into an Applicable System.

ResponseID	Response
	We have existing functions that perform ongoing risk monitoring but it has not been fully integrated into the SCRM procedures.
	We implemented triggers at the SMEs discretion based on Vendor notifications, receiving a different model number than what was ordered, equipment failures, or information from internal monitoring services.
	We have added controls around our access management and asset management processes which places a halt on BES access or BES cyber system installation if no assessment is on file.
	Our DOE third-party SCRM service reassesses vendors during the timeframes determined by business criticality.
	We are not monitoring the business health of vendors. The cost of a third-party monitoring solution is not beneficial to us.
	Depending on the tier of the vendor, there are either annual or every other year reviews to verify that the vendor is still fulfilling their contractual cyber security obligations.

25. Please indicate if having an endorsement for the NATF Criteria and Questionnaire would be a determining factor in your company's continued use or adoption of the NATF Criteria and Questionnaire, and "who" the endorsement would need to come from? (select all that apply)



Value	Percent	Responses
Yes – an endorsement from a government agency (e.g., DOE, DHS, DOD, FERC)	31.0%	9
Yes – an endorsement from a regulator (e.g., NERC, Regional Entities, the ERO Enterprise as a whole)	41.4%	12
Yes – an endorsement from a security agency (e.g., E-ISAC)	13.8%	4
No (please provide any details in the comment field)	55.2%	16
Other (please specify)	3.4%	1

25. Please indicate if having an endorsement for the NATF Criteria and Questionnaire would be a determining factor in your company's continued use or adoption of the NATF Criteria and Questionnaire, and "who" the endorsement would need to come from? (select all that apply) - comments

ResponseID	Response
	It would be nice if we started to see the vendor community publish CIP-013 compliance narratives the same way they talk about other frameworks (ISO, etc).
	This program's initial goal was to establish standard criteria and host a vendor/customer portal to store responses from each vendor in a common location, reducing the burden for everyone. This approach was the most attractive reason for pursuing the use of this specific criteria rather than other standard models that already exist. Endorsements would only be useful if they ultimately result the portal being made available as originally planned.
	We use the NATF resources
	But an endorsement would add weight to industry adoption.
	Sure it would help but we have to maintain our tie to our Corp policies
	These endorsements would not necessarily be a determining factor for continued use, but would certainly strengthen our position on its use.
	We use selected questions from the NATF criteria and has established procedures. An endorsement would not be a determining factor in modifying our procedures.
	The criteria and questionnaire contain a solid basis for assessing risk, with or without an endorsement.
	While not a determining factor since we are already using it, we would like to see an endorsement by as many agencies as possible.
	Our company does not need convincing of the value of the NATF questionnaire. The problem is it's magnitude and vendors' reluctance to complete it.
	Prefer to use a third party due to resource constraints
	NATF and DOE SCRM alignment would be very beneficial.
	We are committed to our risk assessment program, which has been heavily influenced by the NATF Criteria and Questionnaire, so additional endorsement wouldn't cause this to change.

26. If your organization doesn't use the NATF Criteria or Questionnaire, please describe any barriers or reasons why and if there are any modifications that would encourage use of these tools.

ResponseID	Response
35	One major barrier is that the questionnaire is too complex/long to expect responses from vendors. As a smaller organization we have little buying power and have failed to secure responses to even our own smaller questionnaire that contains similar questions. However; we have had a lot of success negotiating our supply chain terms, so they have become the primary vehicle for establishing responses from vendors. The barrier above, absent the portal hosting the vendor responses to take the burden of getting answers off of us, then also becomes the primary barrier for using the NATF Criteria.
36	We developed tools based on the NATF criteria and questionnaire that are tailored to our specified risks. Our tool has less criteria than the NATF developed criteria.
44	The topic hasn't come up and we have been slow to adopt new criteria
58	N/A
64	There are no barriers to using the NATF criteria or questionnaire. Our company had a third party risk review process in place corporate-wide prior to the implementation of CIP-014 that could be easily modified to capture CIP-013 requirements.
67	Too long and cumbersome, and it requires an SME to interpret responses to long answer questions. Depending on the SME, the same answer can be acceptable or deficient. Our existing VCSA is more objective and easier for vendors to complete; it's just a series of a little over 40 Yes or No questions. The Y/N nature of the VCSA lends itself toward automated scoring as well.
69	N/A
72	Prefer to use a third party due to resource constraints
74	N/A

27. Please provide any further information that your company believes would be helpful for the NATF/Industry Organizations Team to increase the adoption of the Model?

ResponseID	Response
23	we have been using the NATF questionnaire but are moving away from it in the next version of our program in favor of a pared-down risk assessment that has a greater aperture for inputs (i.e. things other than "just" the questionnaire); the questionnaire is good and well thought out but it is cumbersome to use and frankly, "scares" folks both inside and outside the organization with its depth/detail, making adoption difficult...we are therefore changing to a simpler method - until/if directed to use a specific product/form by NERC in future versions of the standard (which I support for standardization to both implementation and audit)...
34	The amount of effort NATF and NERC SCWG have done on behalf of utilities (and vendors) is amazing, and we are extremely grateful for everything you've produced. Thanks!
39	We would appreciate a list of prospect service providers in this space. The typical Vendor Risk Assessment service providers are not up to speed yet on CIP-013, nor the NATF model. Additionally, since this is a relatively new space for the Electricity Sub-Sector, there are often no current utility customers to provide references.
44	Just taking time to get up to speed
48	If there was a database that all electric providers would be able to use to review existing vendor responses. This would minimize the burden on each entity and allow for better collaboration amongst industry.
69	A centralized repository for all of the answers to the NATF questionnaire is critical for both the vendor and utility communities
76	NATF could possibly educate and implore vendors (even industry specific vendors) to adopt the Model. This may help encourage more vendor participation so that when entities request vendors to complete the questionnaire the vendors might either be willing to complete the questionnaire or have a questionnaire already completed.