North American Transmission Forum

Communauté Confidentialité Franchise Engagement

Guide d'application entériné par l'ERO

Guide d'application du NATF pour la norme CIP-013 : Plans de gestion des risques dans la chaîne d'approvisionnement

Version 1.1

Document nº 1605

Approbation 2023/10/23

Versionnage

Historique des versions

Date	Version	Remarques
2022/01/28	1.0	Version initiale
2023/10/23	1.1	Correction d'hyperliens défectueux

Exigences concernant la révision et la mise à jour

- Révision : tous les cinq ans
- Mise à jour : au besoin

Table des matières

Versionnage 2

Table des matières 3

1. Introduction 4

2. Énoncé de l'objectif ou du problème 7

3. Champ d'application 7

4. CIP-013 – Gestion des risques de cybersécurité dans la chaîne d'approvisionnement 7

5. Utilisation du modèle du NATF pour établir des plans de gestion des risques (E1) 9

6. Utilisation du modèle du NATF pour la conformité avec l'alinéa 1.1 de l'exigence E1 de la norme CIP 013 10

7. Utilisation du modèle du NATF pour la conformité avec l'alinéa 1.2 de l'exigence E1 de la norme CIP-013 16

8. Utilisation du modèle du NATF pour la conformité avec l'exigence E2 de la norme CIP-013 17

9. Recours à des évaluations indépendantes pour vérifier l'information des fournisseurs (E1) 18

10. Révisions périodiques de ce Guide d'application 19

Annexe 1 – Sources et ressources 21

1. Introduction

Ce Guide d'application décrit comment le modèle d'évaluation de la sécurité dans la chaîne d'approvisionnement du NATF (le modèle du NATF), utilisé adéquatement, constitue un des moyens de mise en conformité avec les exigences E1 et E2 des normes CIP-013-1 et CIP-013-2, qui prescrivent d'établir et de mettre en œuvre des plans de gestion des risques de cybersécurité dans la chaîne d'approvisionnement pour les *systèmes électroniques BES* à impact moyen ou élevé ainsi que les *systèmes de contrôle ou de surveillance des accès électroniques* (*EACMS*) et les *systèmes de contrôle des accès physiques* (*PACS*) associés (collectivement, les « systèmes visés par la norme CIP-013 »). Dans le présent document, les normes CIP-013-1 et CIP-013-2 seront appelées « norme CIP-013. »

> Pour être conforme à la norme CIP-013-2 selon l'exemple présenté dans ce document, l'entité responsable doit faire en sorte que ses « *systèmes de contrôle ou de surveillance des accès électroniques* (*EACMS*) et [ses] *systèmes de contrôle des accès physiques* (*PACS*) associés » soient couverts par son ou ses plans de gestion des risques de cybersécurité dans la chaîne d'approvisionnement au plus tard le 1er octobre 2022.

Le modèle du NATF intègre les critères de sécurité dans la chaîne d'approvisionnement du NATF (les critères du NATF) ainsi que le questionnaire ESSCR sur les risques dans la chaîne d'approvisionnement du secteur énergétique ; le présent Guide décrit l'utilisation de ces outils.

Le présent Guide est dérivé du Guide d'application du 14 juin 2019 entériné par l'ERO, intitulé *CIP-013-1 Supply Chain Risk Management Plans (NATF)*, qui porte sur la possibilité pour les entités responsables d'avoir recours aux services de tiers en ajoutant un processus qui améliore la visibilité de l'entité responsable sur les risques potentiels.

> Le modèle du NATF, les critères du NATF et le questionnaire ESSCR sont axés sur la sécurité. Le modèle du NATF présente un processus qui couvre l'ensemble du cycle d'acquisition.
>
> L'emploi de ces outils n'entraîne, ne suggère ni n'implique aucune amplification ni expansion des exigences de la norme.
>
> ***Les guides d'application n'ont pas pour effet d'élargir la portée des exigences de la norme de fiabilité[1]. Le fait pour une entité de ne pas mettre en œuvre des pratiques non exigées par la norme ne constitue pas une non-conformité.***

Ce Guide d'application a été créé dans le but d'assurer les entités responsables qu'un programme de sécurité dans la chaîne d'approvisionnement, s'il est mis en œuvre adéquatement, permettra de

1. La Politique de la NERC relative aux lignes directrices sur la conformité (5 novembre 2015) est disponible sur le site Web de la NERC à l'adresse https://www.nerc.com/pa/comp/guidance/Documents/Compliance%20Guidance%20Policy.pdf.

respecter les exigences de conformité, et pourra renforcer la confiance de l'ERO dans le programme de l'entité responsable.

Ce guide n'impose pas une démarche unique, mais décrit une démarche possible qui devrait permettre de gérer efficacement les risques dans la chaîne d'approvisionnement et de réaliser la conformité avec la norme. Il ne s'agit que d'un exemple, et les entités sont donc libres de choisir toute autre démarche plus adaptée à leur situation particulière[2].

Contexte

À la suite d'une proposition réglementaire (NOPR)[3] et d'une conférence technique subséquente[4], la Federal Energy Regulatory Commission (FERC) a publié le 21 juillet 2016 l'Ordonnance 829. La décision finale demandait à la NERC d'élaborer une norme de fiabilité nouvelle ou modifiée portant sur la gestion des risques dans la chaîne d'approvisionnement pour les équipements, les logiciels et les services informatiques et de réseau des systèmes de commande industrielle associés à l'exploitation du système de production-transport d'électricité. Cette norme devait exiger que chaque entité visée établisse et mette en œuvre un plan pour l'intégration de contrôles de sécurité dans la chaîne d'approvisionnement pour ces systèmes.

En réponse à cette ordonnance, le Conseil d'administration de la NERC a adopté en août 2017 des normes sur la chaîne d'approvisionnement (CIP-005-6, CIP-010-3 et CIP-013-1), et présenté une résolution demandant que la direction de la NERC, en collaboration avec les comités techniques appropriés de la NERC, des représentants de l'industrie et des experts, y compris des représentants de fournisseurs de l'industrie[5], étudie plus à fond la nature et la complexité des risques de cybersécurité dans la chaîne d'approvisionnement. La résolution du Conseil d'administration de la NERC demandait spécifiquement au North American Transmission Forum (NATF) et au North American Generation Forum (NAGF) « de rédiger des livres blancs décrivant les meilleures pratiques de gestion de la chaîne d'approvisionnement – notamment pour le processus d'acquisition, les spécifications et les exigences applicables aux fournisseurs, ainsi que pour la gestion des équipements existants – qui font l'objet d'une mise en commun parmi les membres de chaque forum, puis, dans la mesure permise par toute entente de confidentialité applicable, de diffuser ces livres blancs dans l'industrie[6]. » En réponse à la résolution du Conseil d'administration de la NERC, le NATF a publié en juin 2018 un livre blanc intitulé *Cyber Security Supply Chain Risk Management Guidance*, disponible sur le site Web de la NERC. Par la suite, le NATF a rédigé et soumis un guide d'application intitulé *CIP-013-1 Supply Chain Risk Management Plans (NATF)*.

2. *Idem*, p. 1.
3. 152 FERC ¶ 61,054 (juillet 2015).
4. La transcription de cette conférence technique, tenue le 28 janvier 2016, est disponible dans le dossier RM15-14-000.
5. Dans le présent Guide, le terme « fournisseur » est utilisé comme générique pour englober les équipementiers (OEM), les producteurs de logiciels, les revendeurs ou toute source de produits ou de services, par souci de cohérence avec les normes de fiabilité de la NERC. Dans la version anglaise, le terme utilisé est « *vendor* », lequel remplace le terme « *supplier* » utilisé dans le modèle du NATF ; dans le contexte du présent Guide et du modèle du NATF, ces deux termes sont interchangeables.
6. Les livres blancs du NATF et du NAGF de 2018 sont disponibles sur le site Web de la NERC à l'adresse https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx.

L'ERO a entériné en 2019 ce guide d'application, qui concernait la possibilité pour les entités responsables de recourir aux services de tiers.

Depuis, le NATF et l'Industry Organizations Team dirigée par le NATF, regroupant des entreprises d'électricité ainsi que divers intervenants de l'industrie de l'énergie (représentants d'organismes et de forums industriels, fournisseurs, vérificateurs indépendants et prestataires de solutions), ont produit – et partagé librement – des analyses qui répondent à la résolution du Conseil d'administration de la NERC demandant d'étudier les enjeux de gestion des risques dans la chaîne d'approvisionnement. Les objectifs du NATF et de l'Industry Organizations Team sont de renforcer la sécurité dans la chaîne d'approvisionnement par la détection des risques et leur atténuation ; d'harmoniser la position de l'industrie sur l'information jugée nécessaire à cette fin ; et d'établir des pratiques efficientes, efficaces et qui répondent aux exigences de conformité.

C'est en fonction de ces objectifs qu'ont été élaborés le modèle du NATF, les critères du NATF et le questionnaire ESSCR. L'Industry Organizations Team a aussi rédigé des guides pour aider les entités à comprendre les évaluations indépendantes et le recours à des prestataires de solutions pour la gestion des risques liés à des tiers. Une série de webinaires a permis de faire mieux connaître les méthodes des entités pour la conduite des évaluations des risques ; l'American Public Power Association (APPA), avec des apports d'autres membres de l'Industry Organizations Team, a rédigé un guide sur la gestion des risques dans la chaîne d'approvisionnement, comprenant des méthodes pour la conduite d'une évaluation des risques. Une autre série de webinaires a été donnée sur différents produits et services permettant de détecter et d'atténuer les risques. Enfin, le Groupe de travail sur les chaînes d'approvisionnement (SCWG) de la NERC a élaboré une série de directives de sécurité qui ont été reprises par le NATF et l'Industry Organizations Team.

Ces différents efforts visaient à établir des pratiques de sécurité permettant de respecter et de dépasser les exigences des normes de la NERC sur la chaîne d'approvisionnement. Il s'agit de fusionner les efforts de sécurisation et de conformité réglementaire, de telle sorte qu'une entité responsable qui sécurise sa chaîne d'approvisionnement se trouve à respecter du même coup les exigences de conformité. La NERC a travaillé diligemment avec l'industrie afin de répondre aux questions sur la conformité au moyen de rapports internes et par des séances de consultation en petits groupes sur la chaîne d'approvisionnement en 2018 et en 2021. En outre, le Comité de conformité et de certification (CCC) de la NERC, lui-même membre de l'Industry Organizations Team, a collaboré avec la NERC et les *entités régionales* pour établir une série de questions fréquentes, qu'on retrouve dans les documents de questions fréquentes sur le programme d'atténuation des risques dans la chaîne d'approvisionnement[7].

Le processus d'élaboration des Guides d'application « permet aux entités visées de suggérer des exemples ou des démarches, validés par l'industrie et entérinés par l'ERO, qui illustrent comment ces entités peuvent se mettre en conformité avec une norme [ou une de ses exigences]. Les exemples présentés dans les Guides d'application ne se veulent pas limitatifs, car il existe vraisemblablement d'autres moyens de mise en conformité[8] ». Le présent Guide d'application du NATF décrit une des méthodes possibles

7. Ces documents, en plus d'autres ressources, sont disponibles sur le site Web de la NERC à l'adresse https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx.
8. La Politique de la NERC relative aux lignes directrices sur la conformité (5 novembre 2015) est disponible sur le site Web de la NERC à l'adresse https ://www.nerc.com/pa/comp/guidance/Documents/Compliance%20Guidance%20Policy.pdf.

permettant à une entité responsable de satisfaire à l'exigence E1 de la norme CIP-013 et, par la suite, à son exigence E2.

2. Énoncé de l'objectif ou du problème

Le but visé par ce Guide d'application est d'unifier les efforts de sécurisation de la chaîne d'approvisionnement avec les efforts de mise en conformité, et de proposer ainsi aux entités responsables une méthode entérinée par l'ERO pour synchroniser la réalisation de ces objectifs.

3. Champ d'application

Ce Guide d'application du NATF présente une méthode qui permet à une entité responsable de satisfaire à l'exigence E1 de la norme CIP-013 et, de là, à son exigence E2.

Cet exemple ne s'applique pas à l'exigence E3 de la norme CIP-013 :

> **E3.** Chaque entité responsable doit réexaminer et faire approuver par le *cadre supérieur CIP* ou son délégataire, au moins une fois tous les 15 mois civils, le ou les plans de gestion des risques de cybersécurité dans la chaîne d'approvisionnement prescrits à l'exigence E1.
> *[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation]*

Comme le souligne la Politique de la NERC relative aux lignes directrices sur la conformité, le fait qu'un Guide d'application soit entériné ne garantit pas que l'entité responsable qui l'utilise répondra de ce fait aux exigences de la norme. Cette politique stipule que « l'entérinement par l'ERO signifie que l'ERO reconnaît que le Guide en question aidera à obtenir un jugement favorable le cadre des activités de surveillance de la conformité et d'application des normes (CMEP). Les entités visées pourront donc s'appuyer sur un Guide et être raisonnablement assurées que les exigences de conformité seront respectées, sans toutefois perdre de vue que la détermination de la conformité dépend aussi de la réalité, des circonstances et des configurations de réseau[9]. »

4. CIP-013 – Gestion des risques de cybersécurité dans la chaîne d'approvisionnement

La norme de fiabilité CIP-013 a pour objet d'« atténuer les risques de cybersécurité susceptibles de menacer la fiabilité du *système de production-transport d'électricité* (*BES*) en établissant des contrôles de sécurité axés sur la gestion des risques dans la chaîne d'approvisionnement des *systèmes électroniques BES* ». Le modèle du NATF présente un processus validé par l'industrie pour aider les entités responsables à établir des plans de gestion des risques de cybersécurité dans leur chaîne d'approvisionnement.

9 *Idem*.

Selon l'exigence E1, chaque entité responsable doit établir un ou des plans documentés de gestion des risques de cybersécurité dans la chaîne d'approvisionnement pour les systèmes visés par la norme CIP-013. Chaque plan doit comporter un ou des processus d'évaluation des risques liés à l'acquisition et à l'installation d'équipements et de logiciels de fournisseurs ainsi qu'à une transition entre fournisseurs, et doit inclure les six points énumérés sous l'alinéa 1.2.

Les exigences E1 et E2 de la norme[10] se lisent comme suit :

E1. Chaque entité responsable doit établir un ou des plans documentés de gestion des risques de cybersécurité dans la chaîne d'approvisionnement pour les *systèmes électroniques BES* à impact moyen ou élevé [ainsi que les *systèmes de contrôle ou de surveillance des accès électroniques* (*EACMS*) et les *systèmes de contrôle des accès physiques* (*PACS*) associés]. Ce ou ces plans doivent comprendre les éléments suivants :
[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation]

1.1. Un ou des processus utilisés dans la planification de l'acquisition de *systèmes électroniques BES* [ainsi que des *EACMS* et des *PACS* associés] afin de déterminer et d'évaluer les risques de cybersécurité pour le *BES* liés aux produits ou services de fournisseurs, résultant : i) de l'acquisition et de l'installation d'équipements et de logiciels de fournisseurs ; et ii) d'une transition entre fournisseurs.

1.2. Un ou des processus utilisés dans l'acquisition de *systèmes électroniques BES* [ainsi que des *EACMS* et des *PACS* associés], qui prévoient les mesures suivantes, selon le cas :

1.2.1. la notification par le fournisseur des incidents constatés par celui-ci relativement aux produits ou services livrés à l'entité responsable et qui présentent pour celle-ci un risque de cybersécurité ;

1.2.2. la coordination des réponses aux incidents constatés par le fournisseur relativement aux produits ou services livrés à l'entité responsable et qui présentent pour celle-ci un risque de cybersécurité ;

1.2.3. la notification par le fournisseur lorsqu'il n'y a plus lieu d'accorder à ses représentants un accès distant ou local ;

1.2.4. la divulgation par le fournisseur de vulnérabilités connues touchant des produits ou services livrés à l'entité responsable ;

1.2.5. la vérification de l'intégrité et de l'authenticité de tous les logiciels et correctifs livrés par le fournisseur et destinés à un *système électronique BES* [ainsi qu'aux *EACMS* et aux *PACS* associés] ; et

10. Les passages ajoutés dans la norme CIP-013-2 sont en caractères noirs et entre crochets.

1.2.6. la coordination des contrôles visant i) les accès distants interactifs commandés par un fournisseur, et ii) les accès distants par l'entremise de systèmes de fournisseurs.

E2. Chaque entité responsable doit mettre en œuvre le ou les plans de gestion des risques de cybersécurité dans la chaîne d'approvisionnement prescrits à l'exigence E1.
[Facteur de risque de non-conformité : moyen] [Horizon : planification de l'exploitation]

Remarque : La mise en œuvre d'un plan n'oblige pas l'entité responsable à renégocier ou à résilier des contrats existants (y compris les modifications aux ententes-cadres ou les bons de commande). En outre, l'exigence E2 ne s'étend pas : 1) aux modalités mêmes d'un contrat d'approvisionnement ; et 2) à l'exécution et au respect du contrat par le fournisseur.

5. Utilisation du modèle du NATF pour établir des plans de gestion des risques (E1)

Le modèle du NATF offre aux entités responsables un processus pour l'acquisition des systèmes visés par la norme CIP-013 ; mis en œuvre adéquatement, ce processus encadre la gestion des risques dans la chaîne d'approvisionnement au fil des étapes successives du cycle d'acquisition, en spécifiant une action particulière pour chaque étape du cycle. Les entités responsables qui appliquent le modèle du NATF cherchent à intégrer chacune de ces actions dans leurs plans de gestion des risques de cybersécurité dans la chaîne d'approvisionnement pour les systèmes visés par la norme CIP-013. Comme il existe différentes manières de réaliser l'action liée à chaque étape, les entités responsables doivent documenter les modalités propres à leur organisation.

Le modèle en cinq étapes du NATF présente un processus permettant de détecter, d'évaluer et d'atténuer les risques dans la chaîne d'approvisionnement. Ce modèle englobe les fournisseurs et les prestataires de solutions, et prévoit une certaine latitude dans la mise en œuvre par chaque entité responsable. En outre, le modèle du NATF, les critères du NATF, le questionnaire ESSCR et les produits complémentaires d'autres organisations participantes[11] proposent des outils qui favorisent de bonnes pratiques de sécurité dans la chaîne d'approvisionnement. S'il est mis en œuvre correctement et avec un souci de sécurité, le modèle du NATF aide les entités à se conformer aux exigences des normes de fiabilité de la NERC sur la chaîne d'approvisionnement[12]. Les cinq étapes du modèle du NATF sont illustrées ci-dessous à la figure 1 ; chaque étape est décrite en détail ci-après[13]. Les cinq étapes du modèle du NATF aident les entités responsables à atténuer les risques dans la chaîne d'approvisionnement en intégrant les actions nécessaires et les éléments de risque dans la chaîne d'approvisionnement, sans égard au fait que

11. Les produits complémentaires d'autres organisations sont présentés sur le site Web public du NATF à l'adresse https://www.natf.net/industry-initiatives/supply-chain-industry-coordination.
12. L'information sur la version la plus récente des normes sur la chaîne d'approvisionnement est disponible sur le site Web de la NERC à l'adresse https://www.nerc.com/Pages/default.aspx.
13. Une illustration détaillée des intrants des différentes étapes du modèle est présentée à la figure 6 de l'annexe 4 du modèle du NATF.

l'acquisition concerne des technologies informatiques ou opérationnelles ou qu'elle porte sur des logiciels, des micrologiciels, des équipements, des composants ou des services.

Figure 1 : Modèle d'évaluation de la sécurité dans la chaîne d'approvisionnement du NATF

6. Utilisation du modèle du NATF pour la conformité avec l'alinéa 1.1 de l'exigence E1 de la norme CIP 013

Les entités responsables établissent des plans de gestion des risques de cybersécurité dans la chaîne d'approvisionnement pour les systèmes visés par la norme CIP-013 en se guidant sur le modèle du NATF. Le processus de ce modèle couvre les exigences de conformité concernant la planification de l'acquisition de systèmes visés par la norme CIP-013, qui demandent de déterminer et d'évaluer les risques de cybersécurité pour le *BES* liés aux produits ou services de fournisseurs, résultant de l'acquisition et de l'installation d'équipements et de logiciels de fournisseurs ou d'une transition entre fournisseurs, en plus des six points énumérés sous l'alinéa 1.2 de l'exigence E1, selon le cas.

Collecte de l'information

L'entité responsable recueille l'information auprès des fournisseurs afin d'évaluer les risques liés à leurs pratiques de sécurité. La collecte de l'information consiste à recueillir l'information selon les critères du NATF ou au moyen du questionnaire ESSCR (ou les deux) et à valider l'exactitude de cette information.

6.1. Collecte de l'information

Les entités responsables obtiennent l'information sur les fournisseurs (auprès de ceux-ci ou autrement) selon les critères du NATF ou au moyen du questionnaire ESSCR, ou les deux[14].

14. Les critères du NATF et le questionnaire ESSCR peuvent être modifiés de temps en temps en vertu du *Processus de révision du NATF pour le questionnaire sur les risques dans la chaîne d'approvisionnement du secteur énergétique et les critères de cybersécurité du NATF relatifs aux fournisseurs* (le Processus de révision), processus ouvert aux parties prenantes de l'industrie et qui prévoit aussi une validation par l'ERO et l'E-ISAC.

Le modèle du NATF offre les outils suivants pour recueillir l'information :

1. ***les critères du NATF**, qui peuvent servir à recueillir l'information auprès d'un fournisseur, ou servir de base pour mesurer la posture et les pratiques de sécurité du fournisseur (p. ex. une liste de « pratiques exemplaires ») ; et*

2. ***le questionnaire ESSCR**, qui peut servir à obtenir une information plus fine sur la performance d'un fournisseur en matière de sécurité.*

*L'entité responsable utilise ces outils pour recueillir de l'information sur la gestion des risques par le fournisseur au **niveau corporatif**, pour un **produit ou service particulier** ou au **niveau du système de développement**.*

L'un ou l'autre de ces outils (ou les deux) peuvent être utilisés pour recueillir l'information sur la gestion des risques par le fournisseur au niveau corporatif, pour un produit ou service particulier, ou encore au niveau du système de développement. Les entités responsables utilisent ces outils pour détecter les risques. La connaissance de ces risques permet ensuite aux entités responsables d'établir des mesures d'atténuation en collaboration avec les fournisseurs.

En utilisant les critères du NATF ou le questionnaire ESSCR (ou les deux), l'entité responsable obtient les éléments d'information qu'elle juge nécessaires pour son évaluation des risques, en fonction du fournisseur et du risque lié aux produits ou services à acquérir. Au minimum, l'entité responsable incorpore à son évaluation des risques les réponses concernant les six points énumérés sous l'alinéa 1.2 de l'exigence E1.

6.2. Valider l'exactitude de l'information

L'entité responsable s'assure que l'information recueillie auprès du fournisseur est exacte. Pour réaliser une évaluation approfondie d'un fournisseur, l'entité responsable peut procéder à un examen complet des pièces justicatives du fournisseur ainsi qu'à des audits de ses installations. Cette méthode de vérification assure en principe le plus haut degré d'assurance quant à la posture de sécurité du fournisseur ; cependant, les entités responsables considèrent que souvent ce n'est pas là une utilisation efficiente des ressources et que cette méthode, compte tenu des ressources et des capacités de l'entité responsable, peut produire un résultat douteux. C'est pourquoi les entités responsables ont souvent recours aux services de tiers pour vérifier l'exactitude de l'information sur les fournisseurs.

Pour offrir aux entités responsables le plus haut degré d'assurance, la vérification par un tiers prend la forme d'une évaluation ou d'une certification indépendante par un évaluateur ou un vérificateur indépendant dûment qualifié et accrédité. On peut aussi s'adresser à d'autres organisations tierces qui embauchent des vérificateurs dûment formés, mais sans accréditation en matière d'audit ; ces organisations peuvent réaliser des vérifications crédibles de l'information sur le fournisseur, sur la foi de pièces justicatives attestant leurs méthodes de travail et leurs compétences. La section 9 présente des détails supplémentaires sur les actions des entités responsables lorsqu'elles ont recours aux services de tiers pour vérifier l'information sur des fournisseurs.

S'il est impossible d'obtenir des certifications, évaluations ou autres vérifications par des tiers, l'entité responsable peut devoir vérifier l'information en faisant appel à d'autres ressources disponibles, ce dont elle devra tenir compte dans son processus d'évaluation. En outre, si une certification, évaluation ou autre forme de vérification ne couvre pas tous les critères ou les questions applicables à une acquisition, l'entité responsable devra compléter la vérification par un autre moyen (ou une combinaison de moyens), par exemple effectuer son propre examen des pièces justificatives, recueillir des informations accessibles au public, ou encore obtenir un examen du fournisseur par une autre entité ayant utilisé les critères ou les questions du NATF.

Évaluation de l'information et détection des risques

L'entité responsable acquéreuse peut déterminer, d'après l'information et les assurances fournies, si certaines pratiques de sécurité du fournisseur soulèvent une inquiétude (constituent un risque), et si ce risque peut être atténué, ou encore toléré[15].

Lorsqu'elle évalue l'information recueillie, l'entité responsable détermine :

1. *si le **niveau de conformité du fournisseur** aux critères du NATF ou les réponses au questionnaire ESSCR révèlent des risques pertinents au produit ou service à acquérir ; et*
2. *si le **degré d'assurance ou de vérification de l'exactitude** de l'information sur le fournisseur est suffisant pour le produit ou service à acquérir ;*
3. *si **tout risque détecté peut être atténué** par le fournisseur ou par l'entité, ou si le risque peut être considéré comme tolérable.*

Parmi les points à considérer :

6.3. Évaluation de la conformité du fournisseur aux critères du NATF ou des réponses au questionnaire ESSCR (performance)

Le fournisseur effectue-t-il pleinement toutes les actions pertinentes spécifiées dans les critères du NATF ou dans le questionnaire ESSCR, ou certaines actions ne sont-elles effectuées que partiellement ? Pour toute action pertinente qui n'est pas exécutée complètement, l'entité responsable peut déterminer si ce manquement représente un risque.

15. Le Groupe de travail sur les chaînes d'approvisionnement (SCWG) de la NERC a rédigé une série de directives sur la sécurité dans la chaîne d'approvisionnement qui visent à encadrer l'évaluation de l'information sur les fournisseurs et la détermination des risques et des moyens de les atténuer. Ces directives sont de courts documents de trois pages qui présentent les grandes lignes des enjeux à connaître et des méthodes utilisables pour les gérer. Ces directives sont disponibles sur le site Web de la NERC à l'adresse https://www.nerc.com/comm/RSTC/Pages/SCWG.aspx, et des hyperliens vers ces documents sont donnés sur le site Web du NATF à l'adresse https://www.natf.net/industry-initiatives/supply-chain-industry-cooordination.

6.4. Évaluation du degré d'assurance donné par le fournisseur pour ses réponses (attestation)

Le fournisseur a-t-il été capable de fournir à l'entité responsable acquéreuse une assurance ou une attestation de sa performance déclarée ? Selon l'impact potentiel que le produit ou service à acquérir pourrait avoir sur le *système électrique interconnecté*, l'entité responsable acquéreuse pourra exiger un degré d'assurance plus élevé.

6.5. Évaluation de l'importance des risques détectés et des correctifs possibles[16]

L'entité responsable acquéreuse peut déterminer quels risques détectés nécessitent des mesures d'atténuation et s'il revient à l'entité ou au fournisseur de prendre des mesures ou de mettre en place des contrôles pour atténuer chaque risque, voire l'éliminer. Dans certains cas, l'entité responsable peut déterminer que le risque détecté ne nécessite pas de mesures d'atténuation : soit parce que le risque inhérent est faible, soit parce que le risque résiduel est faible compte tenu des contrôles internes déjà en place.

Grâce à la collaboration entre les entités responsables et les fournisseurs pour trouver des solutions applicables aux risques détectés, il est à prévoir qu'une détection récurrente des mêmes risques et la mise en place de mesures d'atténuation entraîneront un renforcement général de la sécurité, comme le résume la figure 2.

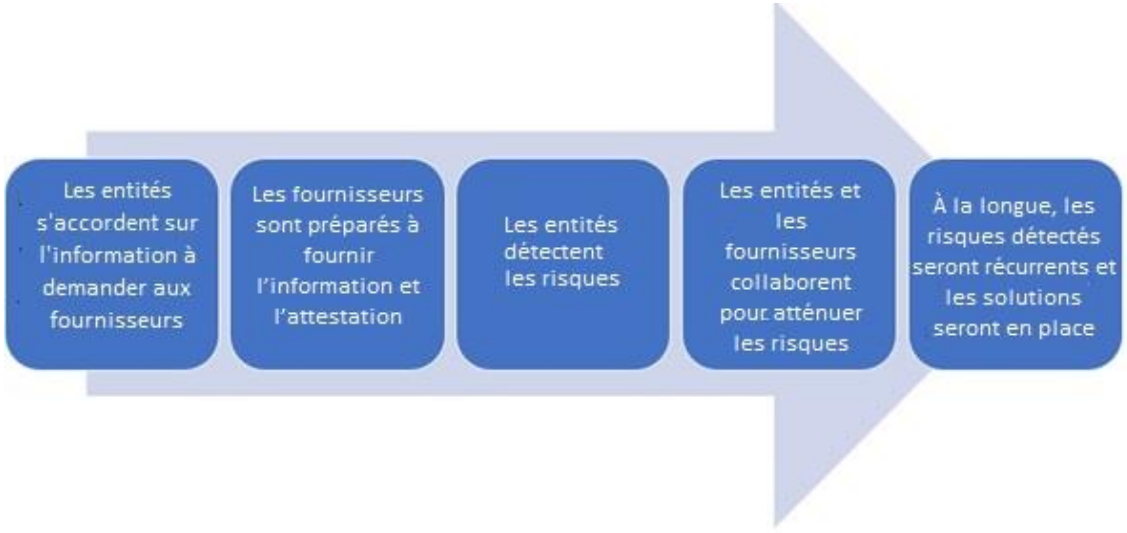


Figure 2 : Démarche collaborative entre entités et fournisseurs

6.6. Documentation des conclusions

L'entité responsable acquéreuse conserve en dossier les réponses du fournisseur et documente son évaluation, ce qui l'aidera à surveiller les risques après l'acquisition ainsi qu'à démontrer sa

16. La norme de fiabilité CIP-013 de la NERC stipule que « la documentation doit désigner et inclure une évaluation des risques de cybersécurité pour le *système de production-transport d'électricité* spécifiques à l'organisation de l'entité visée. »

conformité. Il incombe à l'entité responsable de sécuriser et de protéger les réponses du fournisseur désignées comme confidentielles.

La surveillance des risques après l'acquisition est une pratique de sécurité qui excède les exigences de conformité.

Conduite de l'évaluation des risques

Une fois l'information recueillie, l'entité responsable procède à une évaluation des risques afin de déterminer le degré relatif de risque résiduel parmi les fournisseurs qui offrent le produit ou service à acquérir.

6.7. Conduite de l'évaluation des risques

1. *L'entité responsable dispose d'une méthode pour évaluer les risques des fournisseurs*[17].
2. *L'entité responsable documente les résultats des évaluations de risques.*

Les méthodes utilisables pour l'évaluation des risques sont variées[18]. Certaines entités responsables soumettent les réponses des fournisseurs aux critères du NATF à une analyse selon la méthode des barrières et passages, qui consiste à établir quels critères du NATF sont les plus critiques pour le produit ou service, puis à évaluer les risques du fournisseur selon la séquence établie des critères. D'autres entités utilisent une méthode par cotation et classement, et d'autres encore une combinaison des deux.

Prise de la décision d'achat

Les résultats de l'évaluation des risques dans la chaîne d'approvisionnement, y compris les mesures d'atténuation pouvant être mises en œuvre et surveillées, constituent un des intrants du processus d'approvisionnement de l'entité responsable.

1. *L'entité responsable a mis en place un processus interfonctionnel permettant d'intégrer l'information sur l'évaluation des risques des fournisseurs dans la procédure d'acquisition de l'entité responsable.*
2. *L'entité responsable détermine d'autres facteurs à prendre en compte, notamment sa tolérance au*

17. L'American Public Power Association (APPA), membre actif de l'Industry Organizations Team, a publié un guide pour la conduite des évaluations des risques intitulé *Cyber Supply Chain Risk Management*, disponible sur le site Web de l'APPA à l'adresse https://www.publicpower.org/resource/cyber-supply-chain-risk-management ; un hyperlien vers ce guide est donné sur le site Web du NATF à l'adresse https://www.natf.net/industry-initiatives/supply-chain-industry- coordination/all-resources.

18. *Idem*.

risque, dans la sélection du fournisseur.

3. *Lorsqu'elle prend une décision d'acquisition et qu'elle établit une entente ou un contrat d'acquisition, l'entité responsable examine si des mesures d'atténuation déjà en place ou convenues peuvent être inscrites dans les modalités contractuelles.*

6.8. L'entité responsable a mis en place un processus interfonctionnel permettant d'intégrer l'information sur l'évaluation des risques des fournisseurs dans la procédure d'acquisition de l'entité responsable.

Des processus interfonctionnels sont requis pour l'évaluation des risques du fournisseur, l'atténuation de ces risques, l'établissement des modalités contractuelles, l'achat et enfin la surveillance. Souvent, l'ensemble de ces activités ne relève pas d'un seul service dans l'organisation ; l'entité responsable doit donc établir des contrôles pour faire en sorte que les processus soient déployés adéquatement dans plusieurs services.

6.9. Dans la sélection du fournisseur, l'entité responsable détermine d'autres facteurs à prendre en compte, notamment sa tolérance au risque.

L'information obtenue au moyen du modèle du NATF ne commande pas directement les décisions d'acquisition de l'entité responsable ; il s'agit plutôt d'une information sur les risques de sécurité dans la chaîne d'approvisionnement à prendre en compte et à pondérer avec divers autres facteurs.

L'entité responsable détermine ces autres facteurs et, pour chacun d'eux, établit son importance, ou sa pondération, dans le choix d'un fournisseur. L'entité responsable détermine si les facteurs varient d'une acquisition à l'autre. Les facteurs à considérer, en plus de l'information sur la sécurité dans la chaîne d'approvisionnement, peuvent être notamment les suivants :

- les considérations financières ;
- les aspects opérationnels ;
- les niveaux de soutien du fournisseur ;
- les enjeux réputationnels ;
- les exigences réglementaires ;
- les risques inhérents à l'entité responsable ;
- la tolérance au risque de l'entité responsable ;
- autres informations ou facteurs déteminés par l'entité responsable.

6.10. Lorsqu'elle prend une décision d'acquisition et qu'elle établit une entente ou un contrat d'acquisition, l'entité responsable examine si des mesures d'atténuation déjà en place ou convenues peuvent être inscrites dans les modalités contractuelles.

Mise en place de contrôles et surveillance des risques

Les risques dans la chaîne d'approvisionnement ne se limitent pas à l'acquisition, à la prestation du service ou à l'installation du produit ; ils doivent faire l'objet d'une surveillance tout au long du cycle de vie du produit ou service. La posture de sécurité du fournisseur en rapport avec la chaîne

d'approvisionnement peut être dynamique, ce qui demande à l'entité responsable d'avoir des contrôles en place et de surveiller les risques.

L'entité responsable établit un plan pour surveiller :

1. *les risques et les contrôles liés à l'acquisition sur tout le cycle de vie des produits ou services ;*
2. *le fournisseur afin de détecter tout changement pouvant se répercuter sur les produits ou services (changements corporatifs ou dans la chaîne d'approvisionnement du fournisseur, etc.) ainsi que tout manquement ou compromission.*

La surveillance des risques après l'acquisition est une pratique de sécurité qui excède les exigences de conformité.

6.11. L'entité responsable surveille les risques et les contrôles liés à l'acquisition sur tout le cycle de vie des produits ou services.

Il est nécessaire de surveiller si les mesures d'atténuation adoptées demeurent efficaces, et si l'installation ou la mise en place du produit ou service entraîne un changement dans le profil de risque. Par ailleurs, il convient d'être attentif à de nouveaux risques dans la chaîne d'approvisionnement (par exemple des préoccupations liées au pays d'origine). L'entité responsable peut devoir évaluer si ces risques touchent des équipements, composants, logiciels, etc., déjà installés ou en stock, et si ces risques peuvent être atténués.

6.12. L'entité responsable surveille le fournisseur afin de détecter tout changement pouvant se répercuter sur les produits ou services (changements corporatifs ou dans la chaîne d'approvisionnement du fournisseur, etc.) ainsi que tout manquement ou compromission.

La question de savoir à quelle fréquence l'entité responsable doit mettre à jour son évaluation des risques d'un fournisseur dépend de diverses considérations : selon le fournisseur, selon que des produits ou services acquis du fournisseur font l'objet d'une surveillance, ou selon qu'on envisage le fournisseur pour une nouvelle acquisition. L'entité responsable peut se charger elle-même de la surveillance des fournisseurs, ou peut avoir recours à un prestataire de solutions pour exercer une surveillance continue.

7. Utilisation du modèle du NATF pour la conformité avec l'alinéa 1.2 de l'exigence E1 de la norme CIP-013

Afin d'inclure les six points énumérés sous l'alinéa 1.2 de l'exigence E1 dans le processus d'acquisition des systèmes visés par la norme CIP-013, l'entité responsable qui utilise le modèle du NATF doit considérer les critères et les questions qui s'appliquent à chacun des points de l'alinéa. L'entité responsable intègre ces critères et ces questions, s'il y a lieu, dans les quatre premières étapes du processus du modèle du NATF – collecte de l'information, évaluation de l'information et analyse des risques, conduite de l'évaluation des risques et prise de la décision d'achat – et documente comment elle a traité chaque étape et comment les critères et les questions ont été considérés.

L'entité responsable, dans un souci de sécurité, met aussi en œuvre l'étape supplémentaire du modèle du NATF qui consiste à assurer une surveillance permanente des risques et des contrôles ainsi que du fournisseur.

La surveillance des risques après l'acquisition est une pratique de sécurité qui excède les exigences de conformité.

8. Utilisation du modèle du NATF pour la conformité avec l'exigence E2 de la norme CIP-013

La description des étapes décrites ci-après s'appuie sur le document intitulé *Guide d'application du NATF pour la norme CIP-013 : Recours à des évaluations indépendantes de fournisseurs* afin de clarifier de quelle manière l'entité responsable peut respecter les obligations des exigences E1 et E2 en utilisant le modèle du NATF, les critères du NATF et le questionnaire ESSCR. Ces trois documents sont disponibles (en anglais seulement) sur le site Web du NATF sous « Industry Initiatives/Supply Chain Industry Coordination[19] » ainsi que par les liens suivants :

- Modèle d'évaluation de la sécurité dans la chaîne d'approvisionnement du NATF
- Critères de sécurité dans la chaîne d'approvisionnement du NATF
- Questionnaire sur les risques dans la chaîne d'approvisionnement du secteur énergétique

L'entité responsable présente des pièces justicatives attestant qu'elle met en œuvre son plan de gestion des risques de cybersécurité dans la chaîne d'approvisionnement conformément à l'exigence E2 de la norme CIP-013. L'entité responsable peut présenter des pièces justificatives ou une preuve par démonstration indiquant comment elle applique le modèle du NATF pour chacune de ses cinq étapes.

Collecte de l'information

8.1. En vue d'une acquisition, l'entité responsable obtient les réponses des fournisseurs potentiels aux critères du NATF ou au questionnaire ESSCR (ou les deux), selon ce qu'elle juge nécessaire pour évaluer les pratiques de sécurité des fournisseurs en matière d'hygiène de sécurité générale et en rapport avec le produit ou service à acquérir.

8.2. L'entité responsable vérifie ou fait vérifier les différentes informations des fournisseurs (voir aussi la section 9).

Évaluation de l'information des fournisseurs

8.3. L'entité responsable évalue l'information des fournisseurs afin de déterminer :

8.3.1. les pratiques de sécurité de chaque fournisseur (degré de conformité avec les critères ou les questions) ;

8.3.2. le degré de confiance de l'entité responsable quant à la détermination des pratiques de sécurité de chaque fournisseur (degré d'assurance lié à la vérification) ;

8.3.3. pour chaque fournisseur, les risques qu'il est nécessaire d'atténuer ; et

8.3.4. si des actions ou des contrôles peuvent être mis en œuvre pour atténuer tout risque détecté pour chaque fournisseur.

Conduite de l'évaluation des risques

8.4. L'entité responsable utilise sa méthode documentée pour évaluer les risques.

8.5. Les résultats de l'évaluation des risques par l'entité responsable indiquent comment la méthode est appliquée aux fournisseurs du produit ou service à acquérir.

Prise de la décision d'achat

8.6. L'entité responsable appuie sa décision d'acquisition sur les résultats de l'évaluation des risques de sécurité dans la chaîne d'approvisionnement.

8.7. L'entité responsable détermine si des mesures d'atténuation des risques détectés, déjà en place ou convenues avec le fournisseur retenu, sont spécifiées dans des clauses contractuelles.

Mise en place de contrôles et surveillance des risques

8.8. L'entité responsable surveille les risques détectés et met en place des contrôles pour toute la durée du cycle de vie du produit ou service.

8.9. L'entité responsable surveille le fournisseur afin de détecter tout changement pouvant se répercuter sur les produits ou services (changements corporatifs ou dans la chaîne d'approvisionnement du fournisseur, etc.) ainsi que tout manquement ou compromission.

La surveillance des risques après l'acquisition est une pratique de sécurité qui excède les exigences de conformité.

9. Recours à des évaluations indépendantes pour vérifier l'information des fournisseurs (E1)

En se guidant sur le modèle du NATF, l'entité responsable élabore son ou ses plans de gestion des risques de cybersécurité dans la chaîne d'approvisionnement afin de répondre aux exigences de la norme CIP-013. Le processus du modèle du NATF aide l'entité responsable à évaluer les risques liés à l'acquisition et à l'installation de systèmes visés par la norme CIP-013, ou encore à une transition entre fournisseurs.

9.1. Afin d'encadrer le recours à des évaluations indépendantes de l'information sur les fournisseurs, le plan de gestion des risques de cybersécurité dans la chaîne d'approvisionnement d'une entité responsable, stipulé à l'exigence E1 de la norme CIP-013, doit décrire le processus à suivre par l'entité responsable pour :

9.1.1. demander au fournisseur de présenter une évaluation indépendante (avec la description de la méthode utilisée) par un vérificateur. Celui-ci évalue les contrôles du fournisseur, teste certaines activités de contrôle, ou valide par ailleurs que la posture de sécurité du fournisseur respecte, au minimum, les points énumérés sous l'alinéa 1.2 de l'exigence E1 de la norme CIP-013 ;

9.1.2. évaluer les qualifications du vérificateur ainsi que le référentiel de cybersécurité utilisé pour l'évaluation du fournisseur, en s'assurant que le vérificateur a une indépendance et des accréditations appropriées, ainsi qu'une compréhension adéquate des risques de cybersécurité dans la chaîne d'approvisionnement de l'industrie électrique ;

9.1.3. évaluer la portée ainsi que les résultats de l'évaluation indépendante ;

9.1.4. documenter son évaluation des qualifications du vérificateur indépendant, la méthode utilisée et la portée de l'évaluation ainsi que ses conclusions, afin de déterminer quelles mesures d'atténuation déjà en place ou supplémentaires permettent de gérer les risques, et documenter ces mesures. (Les mesures d'atténuation peuvent comprendre des contrôles physiques, des contrôles électroniques, ou encore des modifications contractuelles.)

L'évaluation indépendante se trouve ainsi intégrée dans le processus global établi par l'entité responsable pour l'acquisition de systèmes visés par la norme CIP-013, et couvre également chacun des points énumérés sous l'alinéa 1.2 de l'exigence E1.

10. Révisions périodiques de ce Guide d'application

La périodicité des révisions de ce document par le NATF ainsi qu'un historique des révisions sont présentés à la section Versionnage, au début de ce document.

Le *Processus de révision du questionnaire ESSCR sur les risques dans la chaîne d'approvisionnement du secteur énergétique et des critères de cybersécurité du NATF relatifs aux fournisseurs* (le Processus de révision), articulé sur un cycle annuel, permet de modifier ou de mettre à jour les critères du NATF et le questionnaire ESSCR à partir des commentaires de l'industrie. Ces commentaires peuvent provenir d'entités, de fournisseurs, d'évaluateurs et d'autres organisations de l'industrie, ainsi que des experts techniques de l'ERO et de l'E-ISAC. Le Processus de révision prévoit la publication des changements pour examen par les parties prenantes et par l'ERO. Lorsqu'elle reçoit une notification de changement par le NATF, l'ERO doit déterminer si le changement proposé risque de remettre en question son entérinement du présent Guide, et invitera alors le NATF à y remédier. Le Processus de révision et l'examen par l'ERO en vue du maintien de son entérinement font en sorte que les critères soient maintenus à jour et pertinents au fil du temps pour chacun des points énumérés sous l'alinéa 1.2 de l'exigence E1, en toute transparence.

Les critères du NATF, le questionnaire ESSCR et le Processus de révision sont publiés et tenus à jour sur le site Web public du NATF à l'adresse https://www.natf.net/industry-initiatives/supply-chain-industry-coordination.

Annexe 1 – Sources et ressources

Le modèle

Le modèle du NATF, les critères du NATF et le questionnaire ESSCR sont disponibles sur le site https://www.natf.net sous Industry Initiatives/Supply Chain Industry Coordination, à l'adresse https://www.natf.net/industry-initiatives/supply-chain-industry-coordination, et par les liens individuels suivants :

- Modèle d'évaluation de la sécurité dans la chaîne d'approvisionnement du NATF
- Critères de sécurité dans la chaîne d'approvisionnement du NATF
- Questionnaire sur les risques dans la chaîne d'approvisionnement du secteur énergétique
- Processus de révision du questionnaire sur les risques dans la chaîne d'approvisionnement du secteur énergétique et des critères de cybersécurité dans la chaîne d'approvisionnement du NATF

Ressources

La page Web du NATF sur la coordination de l'industrie en matière de chaîne d'approvisionnement (www.natf.net/industry-initiatives/supply-chain-industry-coordination) propose aussi des ressources d'organisations membres de l'Industry Organizations Team, d'entités, de fournisseurs, d'évaluateurs indépendants et de prestataires de solutions.

Documents

Organisations industrielles

- *APPA's Cyber Supply Chain Risk Management* (Gestion des risques de cybersécurité dans la chaîne d'approvisionnement – APPA) (externe)
- *EEI Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk V2* (Clauses contractuelles portant sur les risques de cybersécurité dans la chaîne d'approvisionnement – EEI) (externe)
- *NATF CIP-013-1 Implementation Guidance* (Guide d'application du NATF pour la norme CIP-013-1)
- *NATF Guidance for CIP-010-3 Software Integrity* (Directive du NATF sur l'intégrité des logiciels pour la norme CIP-010-3)
- *Advancing Supply Chain Security in Oil and Gas: An Industry Analysis* (Amélioration de la sécurité dans la chaîne d'approvisionnement du secteur pétrolier et gazier : analyse de l'industrie) (externe)

Évaluateurs indépendants

- *Understanding Third-party Assessments* (Guide sur le recours à des évaluations indépendantes)

Prestataires de solutions

- *NATF Industry Collaboration: Using Solution Providers for Third-party Risk Management* (Collaboration dans l'industrie : recours à des prestataires externes pour la gestion des risques – NATF)

Présentations

Industry Organizations Team et NATF

- *Industry Organizations Aligned Approach for Supply Chain Cyber Security Webinar 02242020* (Démarche commune des organisations de l'industrie pour la cybersécurité dans la chaîne d'approvisionnement – webinaire)
- *The Energy Sector Supply Chain Risk ESSCR Questionnaire Webinar 05192020* (Questionnaire ESSCR sur les risques dans la chaîne d'approvisionnement du secteur énergétique – webinaire)
- *Large Entity Use Case Webinar 06022020* (Cas d'utilisation dans les grandes entités – webinaire)
- *Large Entity Use Case Webinar – Exelon 09012020* (Cas d'utilisation dans les grandes entités : Exelon – webinaire)
- *NATF Criteria and ESSCR Questionnaire Overview Use and Revision Process 10022020* (Aperçu du processus d'utilisation et de révision des critères du NATF et du questionnaire ESSCR)
- *Identifying and Managing Potential Compromise of Network Interface Cards - NATF-RF-SERC Special Webinar 20201022* (Détection et gestion des compromissions potentielles des cartes d'interface réseau – webinaire spécial NATF-RF-SERC)
- *Supply Chain Compliance Joint ERO and CCC Webinar 08072021* (Conformité de la chaîne d'approvisionnement, webinaire mixte ERO et CCC – présentation en direct)
- *ESSCR Questionnaire and Criteria Revisions Overview 03192021* (Aperçu des révisions du questionnaire ESSCR et des critères)

Organisations industrielles

- *Securing Your Supply Chain – Designing and Implementing Supply Chain Security Programs – APPA 05082020* (Sécurisation de votre chaîne d'approvisionnement – Conception et mise en œuvre de programmes de sécurité dans la chaîne d'approvisionnement – APPA)
- *APPA Cyber Supply Chain Risk Management Webinar hosted by MRO 09222021* (Gestion des risques de cybersécurité dans la chaîne d'approvisionnement – webinaire APPA présenté par la Midwest Reliability Organization)

Fournisseurs

- *Suppliers: Responding to Requests for Cyber Security Information 12012020* (Fournisseurs : comment répondre aux demandes d'information sur la cybersécurité)

- *Suppliers: Responding to Requests for Cyber Security Information 01122021* (Fournisseurs : comment répondre aux demandes d'information sur la cybersécurité)

Prestataires de solutions

- *Technical Assessment Methodology for Cyber Security – EPRI 10142020* (Méthode d'évaluation technique de la cybersécurité – EPRI)
- *Solution Provider Webinar – EPRI 10142020* (Webinaire EPRI pour les prestataires de solutions)

Produits et services de soutien

Fournisseurs

- *PwC: Are you inundated with vendor management questionnaires? SOC 2 reporting can help* (Vous êtes inondé de questionnaires de gestion des fournisseurs ? Le modèle de rapport SOC 2 peut vous aider – PwC)

Évaluateurs indépendants

- *Understanding Third-party Assessments* (Guide sur le recours à des évaluations indépendantes)

Prestataires de solutions

- *NATF Industry Collaboration: Using Solution Providers for Third-party Risk Management* (Collaboration dans l'industrie : recours à des prestataires externes pour la gestion des risques)
- *Asset to Vendor Network (A2V) Supplier & Product Assessment Database / Compliance Technology* (Réseau A2V [Asset to Vendor] – Base de données d'évaluation de fournisseurs et de produits et technologie de conformité)
- *EPRI Technology Assessment Methodology (TAM) / Cyber Security Data Sheets (CSDS) for device and system supply chain risk assessment* (Méthode d'évaluation technologique [TAM] et fiches techniques de cybersécurité [CSDS] de l'EPRI pour l'évaluation des risques dans la chaîne d'approvisionnement en dispositifs et en systèmes)
- *IHS Markit KY3P – Know Your Third Party / Third Party Risk Management* (IHS Markit – Services KY3P d'information sur les tiers et de gestion des risques liés à des tiers)
- Directives de sécurité du Groupe de travail sur les chaînes d'approvisionnement (SCWG) de la NERC
    - *Cyber Security Risk Management Lifecycle* (Cycle de gestion des risques de cybersécurité)
    - *Supply Chain Procurement Language* (Clauses contractuelles relatives à la chaîne d'approvisionnement)
    - *Supply Chain Provenance* (Provenance dans la chaîne d'approvisionnement)
    - *Risk Considerations for Open Source Software* (Observations sur les risques liés aux logiciels libres)

- *Risks Related to Cloud Service Providers* (Risques liés aux fournisseurs de services infonuagiques)
- *Supply Chain Secure Equipment Delivery* (Livraison sécurisée des équipements dans la chaîne d'approvisionnement)
- *Vendor Identified Incident Response Measures* (Mesures d'intervention des fournisseurs en cas d'incident constaté par ceux-ci)
- *Vendor Risk Management Lifecycle* (Cycle de gestion des risques liés aux fournisseurs)

- *UL Supplier Cyber Trust Level* (Niveaux UL de cyberconfiance dans les fournisseurs)

North American Transmission

North American Transmission FORUM

Communauté Confidentialité Franchise Engagement

Guide d'application entériné par l'ERO

Guide d'application du NATF pour la norme CIP-013 : Recours à des évaluations indépendantes de fournisseurs

Version 3.1

Document n° 1097

Approbation 2023/10/23

Versionnage

Historique des versions

Date	Version	Remarques
2018/06/20	1.0	Version initiale
2019/04/03	2.0	Révisions d'après les commentaires de l'équipe d'examen de l'ERO. Ajouts concernant les qualifications des évaluateurs indépendants et la portée de l'examen. Éclaircissements sur les étapes du processus et les exigences de documentation. Entérinement par l'ERO.
2022/01/28	3.0	Mise à jour en fonction de la norme CIP-013-2 et intégration des critères du NATF, du questionnaire ESSCR et du Processus de révision, tels que définis dans le document.
2023/10/23	3.1	Correction d'hyperliens défectueux

Exigences concernant la révision et la mise à jour

- Révision : tous les cinq ans
- Mise à jour : au besoin

Table des matières

Versionnage **2**

Table des matières ..... **i**

1. Introduction **2**

2. Recours à des évaluations indépendantes de fournisseurs **3**

3. Révisions périodiques de ce Guide d'application **5**

Annexe A – Critères du NATF et questionnaire ESSCR **7**

Annexe B – Processus de révision et de mise à jour des critères du NATF et du questionnaire ESSCR **9**

1. Introduction

Le processus d'élaboration des Guides d'application « permet aux entités visées de suggérer des exemples ou des démarches, validés par l'industrie et entérinés par l'ERO, qui illustrent comment ces entités peuvent se mettre en conformité avec une norme [ou une de ses exigences]. Les exemples présentés dans les Guides d'application ne se veulent pas limitatifs, car il existe vraisemblablement d'autres moyens de mise en conformité »[1]. Ce Guide d'application du NATF présente une méthode qui permet à une entité responsable de satisfaire aux exigences E1 et E2 des normes CIP-013-1 et CIP-013-2. Dans le présent document, les normes CIP-013-1 et CIP-013-2 seront appelées « norme CIP-013 ».

Acceptabilité du recours à des évaluations indépendantes pour déceler et évaluer les risques des fournisseurs

L'ERO a entériné la pratique, pour les entités responsables, de recourir à une évaluation indépendante de la production par un fournisseur de *systèmes électroniques BES* ainsi que des *systèmes de contrôle ou de surveillance des accès électroniques* (*EACMS*) et des *systèmes de contrôle des accès physiques* (*PACS*) associés (collectivement, les « systèmes visés par la norme CIP-013 »), ou des services connexes, dans le but de se conformer à la norme CIP-013[2]. Le document créé par l'équipe de rédaction CIP-013 et entériné par l'ERO, intitulé *CIP-013-1 Supply Chain Risk Management Plans (2016-03 SDT)*, recommande que le processus d'évaluation des risques de l'entité responsable détecte et évalue les risques de cybersécurité potentiels, y compris les « risques potentiels liés aux contrôles de gestion des risques du fournisseur ». Afin d'évaluer les contrôles de gestion des risques d'un fournisseur, l'entité responsable peut obtenir un « résumé de tout essai de cybersécurité interne ou indépendant portant sur les produits du fournisseur afin d'assurer un fonctionnement sûr et fiable »[3].

Les entités responsables qui utilisent des évaluations indépendantes de fournisseurs s'appuient aussi sur la pratique entérinée par l'ERO de recourir aux « services de tiers » comme moyen d'étayer une assurance raisonnable que les objectifs de fiabilité et de sécurité définis sont atteints par les fournisseurs. Le document intitulé *ERO Enterprise Guide for Internal Controls*[4] invite les *responsables des mesures pour assurer la conformité* de l'ERO à évaluer l'indépendance, les capacités et les compétences du prestataire de « services de tiers » (tiers désintéressé ou service interne indépendant du service chargé d'une fonction de fiabilité) aux fins de la surveillance de la conformité[5].

---

1. Politique de la NERC relative aux lignes directrices sur la conformité (5 novembre 2015), disponible à l'adresse https://nerc.com/pa/comp/guidance/documents/compliance%20guidance%20policy.pdf.
2. Tableau synthèse des normes de fiabilité de la NERC, disponible à l'adresse https://www.nerc.com/pa/Stand/Pages/USRelStand.aspx.
3. CIP-013-1 Supply Chain Risk Management Plans (2016-03 SDT), p. 4 (juin 2017), disponible à l'adresse https://www.nerc.com/pa/comp/guidance/EROEndorsedImplementationGuidance/CIP-013-1-R1%20Implementation%20Guidance.pdf.
4. https://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Guide_for_Internal_Controls_Final12212016.pdf
5. *Idem*, section 2.2.2.

Tout comme l'ERO peut s'appuyer sur les « services de tiers » pour déterminer comment surveiller la conformité d'une entité visée, les entités responsables, dans le contexte de la gestion des risques dans leur chaîne d'approvisionnement, peuvent recourir à une évaluation indépendante compétente des contrôles de gestion des risques d'un fournisseur pour démontrer qu'elles ont évalué les risques de cybersécurité associés aux produits et services du fournisseur pour les systèmes visés par la norme CIP-013.

La description qui suit, qui s'appuie sur le document *CIP-013-1 Supply Chain Risk Management Plans (2016-03 SDT)*, précise de quelle manière l'entité responsable peut réaliser la conformité aux exigences E1 et E2 lorsqu'elle recourt à une évaluation indépendante. Toutefois, aucun ensemble de circonstances ne peut obliger l'entité responsable à opter pour une évaluation indépendante.

2. Recours à des évaluations indépendantes de fournisseurs

Lorsqu'elle établit son plan de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, l'entité responsable décrit l'option du recours à une évaluation indépendante (CIP 013 E1)

L'entité responsable élabore son ou ses plans de gestion des risques de cybersécurité dans la chaîne d'approvisionnement afin de répondre aux exigences de la norme CIP-013. Le plan en question comprend le processus établi par l'entité responsable pour évaluer les risques liés à l'acquisition et à l'installation de systèmes visés par la norme CIP-013, ou encore à une transition entre fournisseurs. Afin d'encadrer le recours à des évaluations indépendantes de l'information sur les fournisseurs, le plan de gestion des risques de cybersécurité dans la chaîne d'approvisionnement d'une entité responsable, stipulé à l'exigence E1 de la norme CIP-013, doit décrire le processus à suivre par l'entité responsable pour :

1. demander au fournisseur de présenter une évaluation indépendante (avec la description de la méthode utilisée) par un vérificateur[6]. Celui-ci évalue les contrôles du fournisseur, teste certaines activités de contrôle, ou valide par ailleurs que la posture de sécurité du fournisseur respecte, au minimum, les points énumérés sous l'alinéa 1.2 de l'exigence E1 de la norme CIP-013 ;

2. évaluer les qualifications du vérificateur ainsi que le référentiel de cybersécurité utilisé pour l'évaluation du fournisseur, en s'assurant que le vérificateur a une indépendance et des accréditations appropriées, ainsi qu'une compréhension adéquate des risques de cybersécurité dans la chaîne d'approvisionnement de l'industrie électrique ;

6. Les vérificateurs qui offrent des évaluations indépendantes doivent avoir des qualifications appropriées à cette fin. Des exemples de qualifications sont donnés aux pages 134 à 137 du document https://www.nerc.com/pa/comp/ERO%20Enterprise%20Compliance%20Auditor%20Manual%20DL/NERC_Compliance%20Monitoring%20and%20Enforcement%20Manual_v4_0.pdf. Autres exemples de qualifications pertinentes : titre de Certified Internal Auditor (CIA) ou de Certified Information Systems Auditor (CISA), et autres accréditations d'audit de sécurité et de contrôles.

3. évaluer la portée ainsi que les résultats de l'évaluation indépendante ;

4. documenter son évaluation des qualifications du vérificateur indépendant, la méthode utilisée et la portée de l'évaluation ainsi que ses conclusions, afin de déterminer quelles mesures d'atténuation déjà en place ou supplémentaires permettent de gérer les risques, et documenter ces mesures. (Les mesures d'atténuation peuvent comprendre des contrôles physiques, des contrôles électroniques, ou encore des modifications contractuelles.)

L'évaluation indépendante se trouve ainsi intégrée dans le processus global établi par l'entité responsable pour l'acquisition de systèmes visés par la norme CIP-013, et couvre également chacun des points énumérés sous l'alinéa 1.2 de l'exigence E1.

L'évaluation indépendante dans la mise en œuvre du plan de gestion des risques de cybersécurité dans la chaîne d'approvisionnement (CIP-013 E2)

Pour les systèmes visés par la norme CIP-013 et les services connexes pour lesquels l'entité responsable juge approprié de recourir à une évaluation indépendante, l'entité responsable peut montrer qu'elle a mis en œuvre son plan conformément à l'exigence E2 de la norme CIP-013 en documentant qu'elle a :

1. demandé et obtenu une évaluation indépendante et documenté sa conclusion que l'évaluateur indépendant avait les qualifications appropriées ;

2. examiné les résultats de l'évaluation indépendante et confirmé (comme au moyen d'une liste de contrôle préétablie) qu'ils confirment le respect des points énumérés sous l'alinéa 1.2 de l'exigence E1 de la norme CIP-013 ;

   Annexe A – Les critères de sécurité dans la chaîne d'approvisionnement du NATF (les critères du NATF), décrits à l'annexe A, présentent des critères validés par l'industrie et les fournisseurs qu'une entité responsable peut utiliser pour mesurer la posture de sécurité d'un fournisseur, et qui couvrent tous les points énumérés sous l'alinéa 1.2 de l'exigence E1 de la norme CIP-013. Le questionnaire ESSCR sur les risques dans la chaîne d'approvisionnement du secteur énergétique (le questionnaire ESSCR) présente des questions pour aider les entités responsables à obtenir l'information nécessaire pour leurs évaluations. Les critères du NATF établissent des renvois à différents référentiels de sécurité pour les points énumérés sous l'alinéa 1.2 de l'exigence E1 de la norme CIP-013.

   L'un ou l'autre de ces outils (ou les deux) peuvent être utilisés pour recueillir l'information sur la gestion des risques par le fournisseur au niveau corporatif, pour un produit ou service particulier, ou encore au niveau du système de développement[7]. En utilisant les critères du NATF ou le questionnaire ESSCR (ou les deux), l'entité responsable obtient les éléments d'information qu'elle

7. Les critères du NATF et le questionnaire ESSCR peuvent être modifiés de temps en temps en vertu du *processus de révision du NATF pour le questionnaire sur les risques dans la chaîne d'approvisionnement du secteur énergétique et les critères de cybersécurité du NATF relatifs aux fournisseurs* (processus de révision), processus ouvert aux parties prenantes de l'industrie et qui prévoit aussi une validation par l'ERO et l'E-ISAC.

juge nécessaires pour son évaluation des risques, en fonction du fournisseur et du risque lié aux produits ou services à acquérir. Au minimum, l'entité responsable incorpore à son évaluation des risques les réponses concernant les six points énumérés sous l'alinéa 1.2 de l'exigence E1.

Annexe B – Le *Processus de révision du questionnaire ESSCR sur les risques dans la chaîne d'approvisionnement du secteur énergétique et des critères de cybersécurité du NATF relatifs aux fournisseurs* (le Processus de révision), décrit à l'annexe B, est articulé sur un cycle annuel ; il permet de modifier ou de mettre à jour les critères du NATF et le questionnaire ESSCR à partir des commentaires des parties prenantes de toute l'industrie. Ces commentaires peuvent provenir d'entités, de fournisseurs, d'évaluateurs et d'autres organisations de l'industrie, ainsi que des experts techniques de l'ERO et de l'E-ISAC. Le Processus de révision fait en sorte que les critères soient maintenus à jour et pertinents pour chacun des points énumérés sous l'alinéa 1.2 de l'exigence E1, et en toute transparence.

Les critères du NATF, le questionnaire ESSCR et le Processus de révision sont publiés et tenus à jour sur le site Web public du NATF à l'adresse https://www.natf.net/industry-initiatives/supply-chain-industry-coordination.

3. examiné et évalué les résultats de l'évaluation indépendante afin de confirmer que les mesures et les contrôles de sécurité du fournisseur ou de l'entité responsable (ou les deux) atténuent les risques de cybersécurité dans l'acquisition des systèmes visés par la norme CIP-013. Cette étape comprend l'utilisation de l'évaluation indépendante pour informer les mesures prises par l'entité responsable pour se conformer aux points énumérés sous l'alinéa 1.2 de l'exigence E1.

Puisque l'entité responsable porte la responsabilité ultime de la conformité avec les normes de cybersécurité dans la chaîne d'approvisionnement, il lui incombe de conserver les pièces justificatives attestant sa conformité avec la norme CIP-013, notamment la documentation de son plan de gestion des risques de cybersécurité dans la chaîne d'approvisionnement, de ses réexamens périodiques et de son exécution. L'exécution comprend la détection des risques, les conclusions de l'évaluation des risques, ainsi que les mesures d'atténuation et l'état de leur mise en œuvre.

3. Révisions périodiques de ce Guide d'application

La périodicité des révisions de ce document par le NATF ainsi qu'un historique des révisions sont présentés à la section Versionnage, au début de ce document.

Le Processus de révision, articulé sur un cycle annuel, permet de modifier ou de mettre à jour les critères du NATF et le questionnaire ESSCR à partir des commentaires de toute l'industrie. Ces commentaires peuvent provenir d'entités, de fournisseurs, d'évaluateurs et d'autres organisations de l'industrie, ainsi que des experts techniques de l'ERO et de l'E-ISAC. Le Processus de révision prévoit la publication des changements pour examen par les parties prenantes et par l'ERO. Lorsqu'elle reçoit une notification de changement par le NATF, l'ERO doit déterminer si le changement proposé risque de remettre en question son entérinement du présent Guide, et invitera alors le NATF à y remédier. Le Processus de révision ainsi que l'examen par l'ERO en vue du maintien de son entérinement font en sorte que les critères soient maintenus à jour et pertinents pour chacun des points énumérés sous l'alinéa 1.2 de l'exigence E1, en toute transparence.

Les critères du NATF, le questionnaire ESSCR et le Processus de révision sont publiés et tenus à jour sur le site Web public du NATF à l'adresse https://www.natf.net/industry-initiatives/supply-chain-industry-coordination.

Annexe A – Critères du NATF et questionnaire ESSCR

Le modèle du NATF offre aux entités responsables un processus pour l'acquisition des systèmes visés par la norme CIP-013 ; mis en œuvre adéquatement, ce processus encadre la gestion des risques dans la chaîne d'approvisionnement au fil des étapes successives du cycle d'acquisition, en spécifiant une action particulière pour chaque étape du cycle. Les entités responsables qui appliquent le modèle du NATF cherchent à intégrer chacune de ces actions dans leurs plans de gestion des risques de cybersécurité dans la chaîne d'approvisionnement pour les systèmes visés par la norme CIP-013. Comme il existe différentes manières de réaliser l'action liée à chaque étape, les entités responsables doivent documenter les modalités propres à leur organisation.

Le modèle en cinq étapes du NATF présente un processus permettant de détecter, d'évaluer et d'atténuer les risques dans la chaîne d'approvisionnement. Ce modèle englobe les fournisseurs et les prestataires de solutions, et prévoit une certaine latitude dans la mise en œuvre par chaque entité responsable. En outre, le modèle du NATF, les critères du NATF, le questionnaire ESSCR et les produits complémentaires d'autres organisations participantes[8] proposent des outils qui favorisent de bonnes pratiques de sécurité dans la chaîne d'approvisionnement. S'il est mis en œuvre correctement et avec un souci de sécurité, le modèle du NATF aide les entités à se conformer aux exigences des normes de fiabilité de la NERC sur la chaîne d'approvisionnement[9, 10]. Les cinq étapes du modèle du NATF sont illustrées ci-dessous à la figure 1. Ces cinq étapes aident les entités responsables à atténuer les risques dans la chaîne d'approvisionnement en intégrant les actions nécessaires et les éléments de risque dans la chaîne d'approvisionnement, sans égard au fait que l'acquisition concerne des technologies informatiques ou opérationnelles ou qu'elle porte sur des logiciels, des micrologiciels, des équipements, des composants ou des services.

8. Les produits complémentaires d'autres organisations sont présentés sur le site Web public du NATF à l'adresse https://www.natf.net/industry-initiatives/supply-chain-industry-coordination.
9. En réponse à l'Ordonnance 829 de la FERC, l'équipe du projet 2016-03 sur les normes de fiabilité de la NERC, portant sur la gestion des risques de cybersécurité dans la chaîne d'approvisionnement, a élaboré la norme de fiabilité CIP-013-1 et modifié les normes de fiabilité CIP-005-6 et CIP-010-3 ; ces trois normes, collectivement, sont connues sous l'appellation « normes sur la chaîne d'approvisionnement ».
10. L'information sur la version la plus récente des normes sur la chaîne d'approvisionnement est disponible sur le site Web de la NERC à l'adresse https://www.nerc.com/Pages/default.aspx.

Figure 1 : Modèle d'évaluation de la sécurité dans la chaîne d'approvisionnement du NATF

Le modèle du NATF, les critères du NATF et le questionnaire ESSCR sont disponibles sur le site https://www.natf.net sous Industry Initiatives/Supply Chain Industry Coordination, et par les liens individuels suivants :

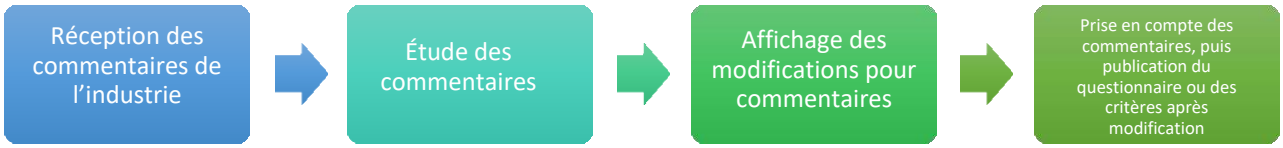
- Modèle d'évaluation de la sécurité dans la chaîne d'approvisionnement du NATF
- Critères de sécurité dans la chaîne d'approvisionnement du NATF
- Questionnaire sur les risques dans la chaîne d'approvisionnement du secteur énergétique

Annexe B – Processus de révision et de mise à jour des critères du NATF et du questionnaire ESSCR

Le Processus de révision vise à faciliter les réexamens et les modifications périodiques des critères du NATF et du questionnaire ESSCR[11]. Ces documents évolutifs ont été créés afin de favoriser dans l'ensemble de l'industrie l'harmonisation des informations obtenues des fournisseurs d'équipements, de logiciels et de services destinés au *système électrique interconnecté*.

Cette procédure porte sur les modifications et la tenue à jour des critères du NATF et du questionnaire ESSCR. Les modifications découlent des commentaires des parties prenantes de toute l'industrie, notamment les entités, les fournisseurs, les évaluateurs et d'autres organisations de l'industrie, ainsi que les experts techniques de l'ERO et de l'E-ISAC. Ces modifications consistent à ajouter, à supprimer ou à modifier des questions dans le questionnaire ESSCR ou des critères dans le document de critères du NATF ainsi qu'à ajouter, à supprimer ou à modifier les renvois aux référentiels de sécurité (SOC 2, ISO 27001, etc.). Le Processus de révision est ouvert aux membres du NATF ainsi qu'aux non-membres, et n'est donc pas soumis aux politiques de confidentialité du NATF.

Étapes principales



Aperçu du processus

Le processus, articulé sur un cycle annuel, permet de modifier ou de mettre à jour les critères du NATF et le questionnaire ESSCR à partir des commentaires de l'industrie. Ces commentaires peuvent provenir d'entités, de fournisseurs, d'évaluateurs et d'autres organisations de l'industrie, ainsi que des experts techniques de l'ERO et de l'E-ISAC. Le processus prévoit un traitement accéléré pour des modifications ou mises à jour jugées plus urgentes : l'examen mensuel des commentaires de l'industrie permet de repérer et d'intégrer de telles modifications ou mises à jour. Comme l'objectif des critères du NATF et du questionnaire ESSCR est de présenter un ensemble uniforme de questions à poser par les entités aux fournisseurs, il importe que les critères du NATF et le questionnaire ESSCR demeurent aussi stables que possible. Dans cette démarche de convergence qui s'appuie sur l'utilisation de ces outils, les commentaires de l'industrie peuvent aider à :

- réduire le nombre de questions dans le questionnaire ;
- obtenir toute l'information nécessaire pour évaluer les risques des fournisseurs ;

11. Les critères du NATF et le questionnaire ESSCR sont disponibles à l'adresse https://www.natf.net/industry-initiatives/supply-chain-industry-coordination.

- présenter des renvois à des référentiels de sécurité utiles.

Les modifications aux critères du NATF et au questionnaire ESSCR seront étudiées simultanément, par souci de concordance entre les deux documents. Il existe en effet des cas où une même modification touche les deux documents, par exemple une mise à jour de renvois à des référentiels de sécurité, ou encore une révision dans un des documents qui nécessite une adaptation dans le texte de l'autre document. Au début du mois de mars de chaque année, l'équipe de révision du questionnaire et des critères publie les changements envisagés au questionnaire et aux critères.

La description du Processus de révision est consultable sur le site https://www.natf.net sous Industry Initiatives/Supply Chain Industry Coordination.