**Formulaire d’audit de la norme de fiabilité au Québec**

# CIP-013-2 — Cybersécurité – Gestion des risques dans la chaîne d’approvisionnement

***Cette section doit être complétée par le NPCC.***

|  |  |
| --- | --- |
| **Numéro de l’audit:** | NPCC-NIRnnnn-YYYYMMDD |
| **Entité visée:** | Nom de l’entité visée |
| **Numéro d’identification à la Régie:** | NIRnnnn |
| **Responsable des mesures pour assurer la conformité:** | Régie de l’énergie |
| **Date(s)**[[1]](#footnote-1) **d’évaluation de la conformité:** | Du jour mois année au jour mois année |
| **Processus de surveillance de la conformité:** | [Audit sur place | Audit hors site | Contrôle ponctuel] |
| **Noms des auditeurs:** | Fournis par le NPCC |

Applicabilité des exigences:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **BA** | **DP** | **GO** | **GOP** | **LSE** | **PA** | **RC** | **RP** | **TO** | **TOP** | **TP** | **TSP** |
| **E1** | X | X[[2]](#footnote-2) | X | X |  |  | X |  | X | X |  |  |
| **E2** | X | X2 | X | X |  |  | X |  | X | X |  |  |
| **E3** | X | X2 | X | X |  |  | X |  | X | X |  |  |

**Légende:**

|  |  |
| --- | --- |
| Texte avec fond bleu: | Texte figé – ne pas modifier |
| Zone d’entrée de texte avec fond vert: | Information fournie par l’entité |
| Zone d’entrée de texte avec fond blanc: | Information fournie par l’auditeur |

**Clause de non-responsabilité**

Ce formulaire d’audit de la norme de fiabilité au Québec (formulaire) a été conçu pour faciliter l’évaluation, par le NPCC, de la conformité à cette norme de fiabilité et son annexe Québec (l’Annexe) d’une entité visée. Ce formulaire contient toutes les questions et tous les sujets pertinents du formulaire correspondant de la NERC utilisé aux États-Unis. Le texte du formulaire est adapté aux versions spécifiques de chaque norme de fiabilité et son Annexe. Les entités qui utilisent ce formulaire devraient choisir la version du formulaire qui s’applique à la norme de fiabilité qui est évaluée. Bien que l’information contenue dans ce formulaire dévoile en partie la méthodologie que le NPCC a choisie pour évaluer la conformité aux exigences de la norme de fiabilité, ce document ne doit pas remplacer la norme de fiabilité ou ne doit pas être vu comme un ajout d’exigences à la norme de fiabilité. Dans tous les cas, l’entité régionale doit se baser sur le texte de la norme de fiabilité elle-même et non sur le texte de ce formulaire, pour déterminer la conformité à la norme de fiabilité. Les normes de fiabilité peuvent être consultées [sur le site internet de la Régie](https://www.regie-energie.qc.ca/fr). Par ailleurs, les normes de fiabilité sont fréquemment mises à jour et il se peut que ce formulaire ne soit pas mis à jour à la même fréquence. Par conséquent, il est impératif que les entités visées considèrent ce formulaire comme un document de référence seulement et non comme un suppléant ou remplaçant de la norme de fiabilité. Il est de la responsabilité de l’entité visée de vérifier si elle est conforme à la dernière version approuvée, par l’autorité gouvernementale applicable, de la norme de fiabilité, en fonction de son inscription [au registre des entités](https://www.regie-energie.qc.ca/fr/entites-visees/registre-des-entites-visees-par-les-normes-de-fiabilite).

Ce formulaire fournit, à titre d’information seulement, une liste non-exclusive d’exemples de types de pièces justificatives qu’une entité visée pourrait devoir fournir ou pourrait être demandée de fournir pour démontrer la conformité à la norme de fiabilité. Les pièces justificatives soumises par l’entité visée pour répondre aux exemples de ce formulaire n’assurent pas nécessairement la conformité à la norme de fiabilité, et le NPCC se réserve le droit de demander des pièces justificatives additionnelles, non contenue dans le formulaire, de la part de l’entité visée.

Constats

**(Cette section doit être complétée par le NPCC)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Exig.** | **Constat** | **Résumé et documentation** | **Fonctions surveillées** |
| **E1** |  |  |  |
| **E2** |  |  |  |
| **E3** |  |  |  |

|  |  |
| --- | --- |
| **Exig.** | **Sujets de préoccupation** |
|  |  |
|  |  |
|  |  |

|  |  |
| --- | --- |
| **Exig.** | **Recommandations** |
|  |  |
|  |  |
|  |  |

|  |  |
| --- | --- |
| **Exig.** | **Observations positives** |
|  |  |
|  |  |
|  |  |

**Experts en la matière**

Identifier le ou les experts en la matière, responsables de la norme de fiabilité.

**Réponse de l’entité visée (Requise; Veuillez insérez des lignes supplémentaires, si nécessaire) :**

|  |  |  |  |
| --- | --- | --- | --- |
| **Nom de l’expert en la matière** | **Titre** | **Organisation** | **Exigence(s)** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**E1 Documentation et pièces justificatives à l’appui**

1. 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. 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.
  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. 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 ;
     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 ;
     3. la notification par le fournisseur lorsqu’il n’y a plus lieu d’accorder à ses représentants un accès distant ou local ;
     4. la divulgation par le fournisseur de vulnérabilités connues touchant des produits ou services livrés à l’entité responsable ;
     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
     6. la coordination des contrôles visant les accès distants commandés par un fournisseur.

1. Les pièces justificatives doivent comprendre un ou des plans documentés de gestion des risques de cybersécurité dans la chaîne d’approvisionnement, conformément à l’exigence.

**Réponse de l’entité visée (Requise):**

**Description narrative de la conformité:**

Fournir une brève explication, en vos propres termes, de votre conformité à cette exigence. Il est recommandé de fournir les références aux pièces justificatives, y compris les liens vers la page appropriée.

**Pièces justificatives de l’entité visée (Requise):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L’information suivante est demandée pour chaque document fourni comme pièce justificative. Les pièces justificatives présentées doivent être mises en évidence et signées, le cas échéant, afin d’identifier l’endroit exact où la pièce justificative attestant de la conformité peut être trouvée.** | | | | | |
| **Nom du dossier** | **Titre du document** | **Révision ou Version** | **Date du document** | **Page(s) ou section(s) pertinentes** | **Description de l’applicabilité du document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Pièces justificatives passées en revue par l’équipe d’audit (Cette section doit être complétée par le NPCC):**

|  |
| --- |
|  |
|  |
|  |

**Démarche d’évaluation de la conformité spécifique à la norme CIP-013-2, E1**

***Cette section doit être complétée par le NPCC***

|  |  |
| --- | --- |
|  | [E1] Vérifier que l’entité responsable a établi 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 *EACMS* et les *PACS* associés. |
|  | [Alinéa 1.1] Vérifier que les plans contiennent un ou des processus utilisés dans la planification de l’acquisition de *systèmes électroniques BES* ainsi que des *EACMS* et des *PACS* associés. Vérifier que ces processus permettent, collectivement, de déterminer et d’évaluer les risques de cybersécurité pour le *BES* liés aux produits ou services de fournisseurs, résultant :   1. de l’acquisition et de l’installation d’équipements et de logiciels de fournisseurs ; et 2. d’une transition entre fournisseurs. |
|  | [Alinéa 1.2] Vérifier que les plans contiennent collectivement un ou des processus utilisés dans l’acquisition de *systèmes électroniques BES* ainsi que des *EACMS* et des *PACS* associés et que ces processus prévoient, selon le cas, les mesures décrites dans les alinéas 1.2.1 à 1.2.6. Si l’une des mesures décrites dans les alinéas 1.2.1 à 1.2.6 ne s’applique pas, vérifier que l’entité a documenté la raison pour laquelle elle ne s’applique pas. |

**Notes des auditeurs:**

**E2 Documentation et pièces justificatives à l’appui**

1. 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.

1. Les pièces justificatives doivent comprendre une documentation attestant la mise en œuvre du ou des plans de gestion des risques de cybersécurité dans la chaîne d’approvisionnement. Exemples non limitatifs de pièces justificatives : documents de correspondance, de politique ou de travail témoignant de l’utilisation de tels plans.

**Réponse de l’entité visée (Requise):**

**Description narrative de la conformité:**

Fournir une brève explication, en vos propres termes, de votre conformité à cette exigence. Il est recommandé de fournir les références aux pièces justificatives, y compris les liens vers la page appropriée.

**Pièces justificatives de l’entité visée (Requise):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L’information suivante est demandée pour chaque document fourni comme pièce justificative. Les pièces justificatives présentées doivent être mises en évidence et signées, le cas échéant, afin d’identifier l’endroit exact où la pièce justificative attestant de la conformité peut être trouvée.** | | | | | |
| **Nom du dossier** | **Titre du document** | **Révision ou Version** | **Date du document** | **Page(s) ou section(s) pertinentes** | **Description de l’applicabilité du document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Pièces justificatives passées en revue par l’équipe d’audit (Cette section doit être complétée par le NPCC):**

|  |
| --- |
|  |
|  |
|  |

**Démarche d’évaluation de la conformité spécifique à la norme CIP-013-2, E2**

***Cette section doit être complétée par le NPCC***

|  |  |
| --- | --- |
|  | Pour les achats des *systèmes électroniques BES* à impact moyen ou élevé initiés à compter de la date de mise en vigueur de la norme CIP-013-1 ou après cette date, vérifier que l’entité responsable a mis en œuvre les plans documentés de gestion des risques de cybersécurité dans la chaîne d’approvisionnement prescrits à l’exigence E1. |
|  | Pour les achats des *EACMS* et des *PACS* associés aux *systèmes électroniques BES* à impact moyen ou élevé à compter de la date de mise en vigueur de la norme CIP-013-2 ou après cette date, vérifier que l’entité responsable a mis en œuvre les plans documentés de gestion des risques de cybersécurité dans la chaîne d’approvisionnement prescrits à l’exigence E1. |

**Notes des auditeurs:**

**E3 Documentation et pièces justificatives à l’appui**

1. 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]*

1. Les pièces justificatives doivent comprendre le ou les plans datés de gestion des risques de cybersécurité dans la chaîne d’approvisionnement approuvés par le *cadre supérieur CIP* ou son délégataire ainsi que des pièces justificatives supplémentaires attestant le réexamen de ce ou ces plans. Exemples non limitatifs de pièces justificatives : documents de politique, historique de révisions, dossiers de réexamen ou preuves de flux de travail provenant d’un système de gestion documentaire attestant que chaque plan de gestion des risques de cybersécurité dans la chaîne d’approvisionnement a fait l’objet d’un réexamen au moins une fois tous les 15 mois civils, ainsi que l’approbation documentée par le *cadre supérieur CIP* ou son délégataire.

**Réponse de l’entité visée (Requise):**

**Description narrative de la conformité:**

Fournir une brève explication, en vos propres termes, de votre conformité à cette exigence. Il est recommandé de fournir les références aux pièces justificatives, y compris les liens vers la page appropriée.

**Pièces justificatives de l’entité visée (Requise):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L’information suivante est demandée pour chaque document fourni comme pièce justificative. Les pièces justificatives présentées doivent être mises en évidence et signées, le cas échéant, afin d’identifier l’endroit exact où la pièce justificative attestant de la conformité peut être trouvée.** | | | | | |
| **Nom du dossier** | **Titre du document** | **Révision ou Version** | **Date du document** | **Page(s) ou section(s) pertinentes** | **Description de l’applicabilité du document** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Pièces justificatives passées en revue par l’équipe d’audit (Cette section doit être complétée par le NPCC):**

|  |
| --- |
|  |
|  |
|  |

**Démarche d’évaluation de la conformité spécifique à la norme CIP-013-2, E3**

***Cette section doit être complétée par le NPCC***

|  |  |
| --- | --- |
|  | Vérifier que l’entité responsable a réexaminé ses plans documentés de gestion des risques de cybersécurité dans la chaîne d’approvisionnement prescrits à l’exigence E1, à la date d’entrée en vigueur de la norme CIP-013-1 ou avant cette date, et au moins une fois tous les 15 mois civils par la suite. |
|  | Vérifier que l’entité responsable a fait approuver par le *cadre supérieur CIP* ou son délégataire, ses plans de gestion des risques de cybersécurité dans la chaîne d’approvisionnement prescrits à l’exigence E1 à la date d’entrée en vigueur de la norme CIP-013-1 ou avant cette date, et au moins une fois tous les 15 mois civils par la suite. |

**Notes des auditeurs:**

**Information supplémentaire**

**Norme de fiabilité**

Le texte complet de la norme CIP-013-2 peut être consulté sur le site internet de la Régie de l’énergie, à la section [Entités visées - Normes de fiabilité](https://www.regie-energie.qc.ca/fr/entites-visees).



**Historique des révisions**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Réviseurs** | **Description de la révision** |
| 1 | Décembre 2023 | Document initial | Document créé à partir du formulaire « RSAW » de la NERC |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. Date(s) d’évaluation de la conformité: la ou les dates auxquelles l’évaluation de la conformité réelle (audit sur place, audit hors site, contrôle ponctuel, etc.) a lieu. [↑](#footnote-ref-1)
2. La norme CIP-013-2 est applicable aux *distributeurs* qui possèdent certains systèmes de délestage de *charge* en sous-fréquence (DSF) ou en sous-tension (DST), des *automatismes de réseau* (*RAS*), des *systèmes de protection*, ou des *chemins de démarrage*. Consulter la section 4, Applicabilité de la norme CIP-013-2 pour des informations supplémentaires. [↑](#footnote-ref-2)