## A. Introduction

**1. Titre :** Cybersécurité — Plans de rétablissement des systèmes électroniques BES

**2. Numéro :** CIP-009-6

**3. Objet :** Rétablir les fonctions de fiabilité exercées par les *systèmes électroniques BES* en définissant les exigences relatives aux plans de rétablissement en vue du maintien de la stabilité, de l'exploitabilité et de la fiabilité du *système de production-transport d'électricité* (*BES*).

**4. Applicabilité :**

**4.1. Entités fonctionnelles :** Dans le contexte des exigences de la présente norme, les entités fonctionnelles indiquées ci-après seront appelées collectivement « les entités responsables ». Dans le cas des exigences de cette norme qui visent une entité fonctionnelle particulière ou un sous-ensemble particulier d'entités fonctionnelles, la ou les entités fonctionnelles sont précisées explicitement.

**4.1.1 Responsable de l'équilibrage**

**4.1.2 Distributeur** qui possède un ou plusieurs des *installations*, systèmes et équipements suivants pour la protection ou la remise en charge du BES :

**4.1.2.1** Chaque système de délestage de charge en sous-fréquence (DSF) ou de délestage de charge en sous-tension (DST) qui :

**4.1.2.1.1** fait partie d'un programme de délestage de *charge* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale ; et

**4.1.2.1.2** effectue du délestage automatique de *charge* de 300 MW ou plus par un système de commande commun détenu par l'entité responsable, sans déclenchement par un exploitant.

**4.1.2.2** Chaque *automatisme de réseau* ou *plan de défense* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale.

**4.1.2.3** Chaque *système de protection* applicable au *transport* (à l'exclusion des systèmes DSF et DST) visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale.

**4.1.2.4** Chaque *chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des groupes prochains groupes de production à démarrer.

***4.1.3 Exploitant d'installation de production***

**4.1.4** ***Propriétaire d'installation de production***

**4.1.5** ***Coordonnateur des échanges ou responsable des échanges***

**4.1.6** ***Coordonnateur de la fiabilité***

**4.1.7** ***Exploitant de réseau de transport***

**4.1.8** ***Propriétaire d'installation de transport***

**4.2.** **Installations :** Dans le contexte des exigences de la présente norme, les *installations*, systèmes et équipements suivants détenus par chaque entité responsable indiquée à la section 4.1 sont ceux auxquels ces exigences sont applicables. Dans le cas des exigences de cette norme qui visent un type particulier d'*installations*, de système ou d'équipements, ou un sous-ensemble d'*installations*, de systèmes ou d'équipements, ceux-ci sont précisés explicitement.

**4.2.1** **Distributeur :** Un ou plusieurs des *installations*, systèmes et équipements suivants détenus par le distributeur pour la protection ou la remise en charge du *BES* :

**4.2.1.1** Chaque système de DSF ou de DST qui :

**4.2.1.1.1** fait partie d'un programme de délestage de *charge* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale ; et

**4.2.1.1.2** effectue du délestage automatique de *charge* de 300 MW ou plus au moyen d'un système de commande commun détenu par l'entité responsable, sans déclenchement par un exploitant.

**4.2.1.2** Chaque *automatisme de réseau* ou *plan de défense* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale.

**4.2.1.3** Chaque *système de protection* applicable au *transport* (à l'exclusion des systèmes DSF et DST) dans le cas où le *système de protection est* visé par une ou plusieurs exigences d'une norme de fiabilité de la NERC ou de l'entité régionale.

**4.2.1.4** Chaque *chemin de démarrage* et groupe d'*éléments* respectant les exigences relatives aux manœuvres initiales depuis une *ressource à démarrage autonome* jusqu'au premier point de raccordement, inclusivement, d'alimentation des services auxiliaires du ou des prochains groupes de production à démarrer.

**4.2.2** **Entités responsables indiquées en 4.1, sauf les distributeurs :**

Toutes les *installations* du BES.

**4.2.3** **Exemptions :** Sont exemptés de la norme CIP-009-6 :

**4.2.3.1** les *actifs électroniques* aux *installations* réglementées par la Commission canadienne de sûreté nucléaire ;

**4.2.3.2** les *actifs électroniques* associés aux réseaux de communication et aux liaisons d'échange de données entre des *périmètres de sécurité électroniques* distincts ;

**4.2.3.3** les systèmes, structures et composants régis par la U.S. Nuclear Regulatory Commission en vertu d'un plan de cybersécurité conforme au règlement CFR 10, section 73.54 ;

**4.2.3.4** dans le cas des distributeurs, les systèmes et les équipements non mentionnés à la section 4.2.1 ci-dessus ;

**4.2.3.5** les entités responsables qui déterminent qu'elles n'ont pas de *systèmes électroniques BES* classés dans les catégories « impact élevé » ou « impact moyen » selon le processus de désignation et de catégorisation de la norme CIP-002-5.1.

## 5. Dates d'entrée en vigueur

Voir le plan de mise en œuvre de la norme CIP-009-6.

## 6. Contexte :

La norme CIP-009 fait partie d'une série de normes CIP sur la cybersécurité qui exigent la détermination et la catégorisation initiales des *systèmes électroniques BES*. Ces normes exigent aussi un niveau minimal de mesures organisationnelles, opérationnelles et administratives pour réduire les risques aux *systèmes électroniques BES*.

La plupart des exigences commencent ainsi : « Chaque entité responsable doit mettre en œuvre un ou plusieurs [processus, plans, etc.] documentés qui couvrent tous les alinéas applicables du tableau [référence au tableau]. » Le tableau en référence précise les éléments qui doivent être inclus dans les procédures pour le thème commun de l'exigence.

L'expression « processus documenté » désigne un ensemble de consignes spécifiques à l'entité responsable et visant à produire un résultat particulier. Cette expression n'implique pas de structure de nommage ou d'approbation au-delà de la formulation des exigences. Une entité doit inclure tout ce qu'elle juge nécessaire dans ses processus documentés, en s'assurant de bien couvrir les exigences pertinentes.

Les mots « programme » et « plan » sont parfois utilisés au lieu de « processus documenté », dans la mesure où la compréhension relève du bon sens. Par exemple, les processus documentés qui décrivent une réponse sont généralement appelés « plans » (plan d'action en cas d'incident, plan de rétablissement, etc.). De plus, un plan de sécurité peut décrire une approche comportant plusieurs procédures couvrant un thème étendu.

De même, le mot « programme » peut désigner la mise en œuvre générale par l'organisation de ses politiques, plans et procédures portant sur un thème donné. Le programme d'évaluation des risques liés au personnel et le programme de formation du personnel sont des exemples qui figurent dans les normes. La mise en œuvre complète des normes de fiabilité CIP sur la cybersécurité pourrait aussi être appelée « programme ». Toutefois, les mots « programme » et « plan » n'impliquent pas d'exigences supplémentaires au-delà de ce qui est indiqué dans les normes.

Les entités responsables peuvent mettre en œuvre des moyens communs qui répondent aux besoins de plusieurs *systèmes électroniques BES* à impact élevé et moyen. Par exemple, un même programme de formation pourrait répondre aux exigences en formation du personnel concernant plusieurs *systèmes électroniques BES*.

Les mesures auxquelles renvoie l'énoncé initial de l'exigence correspondent simplement aux processus documentés eux-mêmes. La colonne « Mesures » présente des exemples de pièces justificatives attestant la documentation et la mise en œuvre des éléments pertinents dans les processus documentés ; ces exemples sont présentés à titre indicatif, et leur liste ne doit pas être considérée comme exhaustive.

Dans l'ensemble des normes, sauf indication particulière, les éléments présentés à la section Exigences et mesures sous forme de liste à puces sont liés par l'opérateur « ou », et les éléments présentés sous forme de liste numérotée sont liés par l'opérateur « et ».

Plusieurs références de la section Applicabilité utilisent un seuil de 300 MW pour les systèmes DSF et DST. Ce seuil particulier de 300 MW pour les systèmes DSF et le DST provient de la version 1 des normes CIP sur la cybersécurité. Le seuil demeure à 300 MW puisqu'il concerne spécifiquement les systèmes DST et DSF, qui constituent des efforts de dernier recours pour sauver le BES. Un examen des tolérances des systèmes DSF définies dans les normes de fiabilité régionales pour les exigences des programmes de DSF à ce jour indique que la valeur historique de 300 MW représente une valeur de seuil adéquate et raisonnable pour les tolérances d'exploitation admissibles des systèmes DSF.

**Colonne « Systèmes visés » des tableaux**

Chaque tableau comporte une colonne intitulée « Systèmes visés » qui définit plus précisément les systèmes auxquels s'applique l'exigence. La SDT (équipe de rédaction) CSO706 a adapté ce concept à partir du cadre de gestion des risques du National Institute of Standards and Technology (NIST) en vue d'établir une méthode d'application des exigences qui tient compte plus adéquatement de l'impact et des caractéristiques de connectivité. La colonne « Systèmes visés » repose sur les conventions suivantes :

- ***Systèmes électroniques BES* à impact élevé –** Désigne les *systèmes électroniques BES* classés dans la catégorie « impact élevé », selon les processus de désignation et de catégorisation de la norme CIP-002-5.1.
- ***Systèmes électroniques BES* à impact moyen –** Désigne les *systèmes électroniques BES* classés dans la catégorie « impact moyen », selon les processus de désignation et de catégorisation de la norme CIP-002-5.1.
- ***Systèmes électroniques BES* à impact moyen situés aux centres de contrôle –** Désigne uniquement les *systèmes électroniques BES* situés aux *centres de*

*contrôle* et classés dans la catégorie « impact moyen », selon les processus de désignation et de catégorisation de la norme CIP-002-5.1.

- ***Systèmes de contrôle ou de surveillance des accès électroniques*** **(EACMS)** – Désigne tout *système de contrôle ou de surveillance des accès électroniques* associé à un *système électronique BES* à impact élevé ou moyen visé. Exemples non limitatifs : pare-feu, serveurs d'authentification et systèmes de surveillance de registre d'événements et d'alerte.
- ***Systèmes de contrôle des accès physiques*** **(PACS)** – Désigne tout *système de contrôle des accès physique*s associés à un *système électronique BES* à impact élevé ou moyen visé à *connectivité externe routable*.

## B. Exigences et mesures

**E1.** Chaque entité responsable doit avoir un ou plusieurs plans de rétablissement documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-009-6) – Caractéristiques d'un plan de rétablissement.
*[Facteur de risque de la non-conformité : moyen] [Horizon : planification à long terme]*

**M1.** Les pièces justificatives doivent inclure le ou les plans de rétablissement documentés qui, collectivement, couvrent tous les alinéas applicables du tableau E1 (CIP-009-6) – Caractéristiques d'un plan de rétablissement.

| Tableau E1 (CIP-009-6) – Caractéristiques d'un plan de rétablissement | | | |
|---|---|---|---|
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 1.1 | *Systèmes électroniques BES* à impact élevé et :<br>1. les EACMS associés ; et<br>2. les PACS associés.<br><br>*Systèmes électroniques BES* à impact moyen et :<br>1. les EACMS associés ; et<br>2. les PACS associés. | Conditions de déclenchement du ou des plans de rétablissement. | Exemples non limitatifs de pièces justificatives : un ou plusieurs plans de rétablissement où sont énoncées les conditions de déclenchement du ou des plans. |
| 1.2 | *Systèmes électroniques BES* à impact élevé et :<br>1. les EACMS associés ; et<br>2. les PACS associés.<br><br>*Systèmes électroniques BES* à impact moyen et :<br>1. les EACMS associés ; et<br>2. les PACS associés. | Rôles et responsabilités des intervenants. | Exemples non limitatifs de pièces justificatives : un ou plusieurs plans de rétablissement où sont énoncés les rôles et responsabilités des intervenants. |

| Tableau E1 (CIP-009-6) – Caractéristiques d'un plan de rétablissement | | | |
|---|---|---|---|
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 1.3 | *Systèmes électroniques BES* à impact élevé et :<br>1. les EACMS associés ; et<br>2. les PACS associés.<br><br>*Systèmes électroniques BES* à impact moyen et :<br>1. les EACMS associés ; et<br>2. les PACS associés. | Un ou plusieurs processus pour la sauvegarde et le stockage de l'information nécessaire au rétablissement des *systèmes électroniques BES*. | Exemples non limitatifs de pièces justificatives : processus documentés pour la sauvegarde et le stockage de l'information nécessaire au rétablissement des *systèmes électroniques BES*. |
| 1.4 | *Systèmes électroniques BES* à impact élevé et :<br>1. les EACMS associés ; et<br>2. les PACS associés.<br><br>*Systèmes électroniques BES* à impact moyen situés aux *centres de contrôle* et :<br>1. les EACMS associés ; et<br>2. les PACS associés. | Un ou plusieurs processus de vérification du bon déroulement des processus de sauvegarde énoncés à l'alinéa 1.3 et de prise en compte des échecs de sauvegarde. | Exemples non limitatifs de pièces justificatives : journaux, preuves d'activité ou autres documents attestant le bon déroulement du processus de sauvegarde et la prise en compte des échecs de sauvegarde, le cas échéant. |
| 1.5 | *Systèmes électroniques BES* à impact élevé et :<br>1. les EACMS associés ; et<br>2. les PACS associés.<br><br>*Systèmes électroniques BES* à impact moyen et :<br>1. les EACMS associés ; et<br>2. les PACS associés. | Un ou plusieurs processus de conservation des données, selon les capacités des *actifs électroniques*, permettant de déterminer la cause d'un *incident de cybersécurité* qui déclenche le ou les plans de rétablissement. La conservation des données ne doit pas nuire au rétablissement ni le limiter. | Exemples non limitatifs de pièces justificatives : procédures de conservation des données, comme la conservation d'un périphérique de stockage victime de corruption de données ou la copie miroir des données du système avant d'entreprendre le rétablissement. |

**E2.** Chaque entité responsable doit mettre en œuvre son ou ses plans de rétablissement documentés, qui, collectivement, couvrent tous les alinéas applicables du tableau E2 (CIP-009-6) – Mise en œuvre et essais du plan de rétablissement. *[Facteur de risque de la non-conformité : faible] [Horizon : planification de l'exploitation et exploitation en temps réel]*

**M2.** Les pièces justificatives doivent comprendre notamment des documents qui, collectivement, attestent la mise en œuvre de tous les alinéas applicables du tableau E2 (CIP-009-6) – Mise en œuvre et essais du plan de rétablissement.

| Tableau E2 (CIP-009-6) – Mise en œuvre et essais du plan de rétablissement | | | |
|---|---|---|---|
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 2.1 | *Systèmes électroniques BES* à impact élevé et :<br>1. les EACMS associés ; et<br>2. les PACS associés.<br><br>*Systèmes électroniques BES* à impact moyen situés aux *centres de contrôle* et :<br>1. les EACMS associés ; et<br>2. les PACS associés. | Tester chacun des plans de rétablissement visés par l'exigence E1 au moins une fois tous les 15 mois civils :<br>• par un rétablissement après un incident réel ;<br>• avec un exercice sur papier ou sur table ; ou<br>• avec un exercice opérationnel. | Exemples non limitatifs de pièces justificatives : preuve datée d'un essai du plan de rétablissement (rétablissement après un incident réel, exercice sur papier ou sur table, ou exercice opérationnel) au moins une fois tous les 15 mois civils. Dans le cas d'un exercice sur papier ou d'un exercice opérationnel complet : avis de réunion, procès-verbaux ou autres documents consignant les résultats des exercices peuvent constituer des pièces justificatives. |

| Tableau E2 (CIP-009-6) – Mise en œuvre et essais du plan de rétablissement | | | |
|---|---|---|---|
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 2.2 | *Systèmes électroniques BES* à impact élevé et :<br>1. les EACMS associés ; et<br>2. les PACS associés.<br><br>*Systèmes électroniques BES* à impact moyen situés aux *centres de contrôle* et :<br>1. les EACMS associés ; et<br>2. les PACS associés. | Tester un échantillon représentatif de l'information nécessaire pour rétablir la fonctionnalité du *système électronique BES* au moins une fois tous les 15 mois civils afin de s'assurer que l'information est utilisable et compatible avec les configurations courantes.<br><br>Ce test peut être remplacé par un rétablissement suivant un incident réel utilisant l'information nécessaire pour rétablir la fonctionnalité du *système électronique BES*. | Exemples non limitatifs de pièces justificatives : journaux d'exploitation ou résultats du test ainsi que les critères de vérification que l'information est utilisable (charger une bande de données, parcourir le contenu de la bande, etc.) et de sa compatibilité avec les configurations courantes des systèmes (points de comparaison manuels ou automatisés entre le contenu des supports de sauvegarde et la configuration courante, etc.). |
| 2.3 | *Systèmes électroniques BES* à impact élevé | Tester chacun des plans de rétablissement visés par l'exigence E1 au moins une fois tous les 36 mois civils, en effectuant un exercice opérationnel des plans de rétablissement dans un environnement représentatif de l'environnement de production.<br><br>Les mesures de rétablissement prises après un incident réel peuvent remplacer l'exercice opérationnel. | Exemples non limitatifs de pièces justificatives :<br>• preuve documentée et datée d'un exercice opérationnel effectué au moins une fois tous les 36 mois civils, qui démontre le rétablissement dans un environnement représentatif ; ou<br>• preuve documentée et datée de mesures de rétablissement prises, dans la fenêtre de 36 mois civils, après un incident réel ayant déclenché les plans de rétablissement. |

**E3.** Chaque entité responsable doit tenir à jour chacun de ses plans de rétablissement conformément à chacun des alinéas applicables du tableau E3 (CIP-009-6) – Examen, mise à jour et communication d'un plan de rétablissement. *[Facteur de risque de la non-conformité : faible] [Horizon : évaluation des activités d'exploitation]*

**M3.** Les pièces justificatives acceptables doivent notamment attester la conformité à chacun des alinéas applicables du tableau E3 (CIP-009-6) – Examen, mise à jour et communication d'un plan de rétablissement.

| Tableau E3 (CIP-009-6) – Examen, mise à jour et communication d'un plan de rétablissement | | | |
|---|---|---|---|
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| 3.1 | *Systèmes électroniques BES* à impact élevé et :<br>1. les EACMS associés ; et<br>2. les PACS associés.<br><br>*Systèmes électroniques BES* à impact moyen situés aux *centres de contrôle* et :<br>1. les EACMS associés ; et<br>2. les PACS associés. | Au plus tard 90 jours civils après la réalisation d'un test de plan de rétablissement ou un rétablissement réel :<br><br>3.1.1. documenter toutes les leçons apprises se rapportant au test de plan de rétablissement ou au rétablissement réel, ou documenter l'absence de leçons apprises ;<br><br>3.1.2. mettre à jour le plan de rétablissement en tenant compte des leçons apprises documentées associées au plan ; et<br><br>3.1.3. aviser chaque personne ou groupe qui joue un rôle défini dans le plan de rétablissement des mises à jour qui ont été apportées au plan de rétablissement en tenant compte des leçons apprises documentées. | Exemples non limitatifs de pièces justificatives :<br><br>1. documents datés consignant les lacunes relevées ou les leçons apprises pour chaque test de plan de rétablissement ou chaque rétablissement suivant un incident réel, ou documents datés attestant l'absence de leçons apprises ;<br><br>2. plan de rétablissement daté et révisé indiquant toutes les modifications apportées en tenant compte des leçons apprises ; et<br><br>3. preuve de distribution de plan révisé, par exemple :<br>• courriels ;<br>• US Postal Service ou autre service postal ;<br>• système de distribution électronique ; ou |

| Tableau E3 (CIP-009-6) – Examen, mise à jour et communication d'un plan de rétablissement | | | |
|---|---|---|---|
| **Alinéa** | **Systèmes visés** | **Exigences** | **Mesures** |
| | | | • feuilles de présence aux formations. |
| 3.2 | *Systèmes électroniques BES* à impact élevé et :<br>1. les EACMS associés ; et<br>2. les PACS associés.<br><br>*Systèmes électroniques BES* à impact moyen situés aux *centres de contrôle* et :<br>1. les EACMS associés ; et<br>2. les PACS associés. | Au plus tard 60 jours civils après un changement aux rôles ou responsabilités, aux intervenants ou à une technologie que l'entité responsable juge qu'il pourrait avoir un impact sur la capacité d'exécuter le plan de rétablissement :<br>3.2.1. mettre à jour le plan de rétablissement ; et<br>3.2.2. aviser des mises à jour chaque personne ou groupe jouant un rôle défini dans le plan de rétablissement. | Exemples non limitatifs de pièces justificatives :<br>1. plan de rétablissement, révisé et daté, comprenant les changements apportés aux rôles ou responsabilités, aux intervenants ou à une technologie ; et<br>2. preuve de distribution du plan révisé, par exemple :<br>• courriels ;<br>• US Postal Service ou autre service postal ;<br>• système de distribution électronique ; ou<br>• feuilles de présence aux formations. |

## C. Conformité

### 1. Processus de surveillance de la conformité

#### 1.1. Responsable des mesures pour assurer la conformité

Selon la définition des règles de procédure de la NERC, le terme « *responsable de la surveillance de l'application des normes* » (CEA) désigne la NERC ou l'entité régionale dans leurs rôles respectifs de surveillance de la conformité aux normes de fiabilité de la NERC.

#### 1.2. Conservation des pièces justificatives

Les périodes de conservation des pièces justificatives indiquées ci-après établissent la durée pendant laquelle une entité est tenue de conserver certaines pièces justificatives afin de démontrer sa conformité. Dans les cas où la période de conservation des pièces justificatives indiquée est plus courte que le temps écoulé depuis le dernier audit, le CEA peut demander à l'entité de fournir d'autres pièces justificatives attestant sa conformité pendant la période complète écoulée depuis le dernier audit.

L'entité responsable doit conserver les données ou pièces justificatives attestant sa conformité selon les modalités indiquées ci-après, à moins que son CEA lui demande de conserver certaines pièces justificatives plus longtemps dans le cadre d'une enquête :

- Chaque entité responsable doit conserver des pièces justificatives pour chaque exigence de la présente norme pendant trois années civiles.
- Si une entité responsable est jugée non conforme, elle doit conserver l'information relative à cette non-conformité jusqu'à ce que les correctifs aient été appliqués et approuvés ou pendant la période indiquée ci-dessus, selon la durée la plus longue.
- Le CEA doit conserver les derniers dossiers d'audit ainsi que tous les dossiers d'audit demandés et soumis par la suite.

#### 1.3. Processus de surveillance et de mise en application des normes

Audits de conformité

Déclarations sur la conformité

Contrôles ponctuels

Enquêtes de conformité

Déclarations de non-conformité

Plaintes

#### 1.4. Autres informations sur la conformité

Aucune.

## 2. Tableau des éléments de conformité

| Ex. | Horizon | VRF | Niveaux de gravité de la non-conformité (CIP-009-6) | | | |
|---|---|---|---|---|---|---|
| | | | VSL faible | VSL modéré | VSL élevé | VSL critique |
| **E1** | **Planification à long terme** | **Moyen** | Sans objet | L'entité responsable a créé un ou des plans de rétablissement, mais en omettant une des exigences des alinéas 1.2 à 1.5. | L'entité responsable a créé un ou des plans de rétablissement, mais en omettant deux des exigences des alinéas 1.2 à 1.5. | L'entité responsable n'a pas créé de plans de rétablissement pour les *systèmes électroniques BES*.<br>OU<br>L'entité responsable a créé un ou des plans de rétablissement pour les *systèmes électroniques BES*, mais en omettant les conditions de déclenchement de l'alinéa 1.1.<br>OU<br>L'entité responsable a créé un ou des plans de rétablissement pour les *systèmes électroniques BES*, mais en omettant au moins trois des exigences des alinéas 1.2 à 1.5. |
| **E2** | **Planification de l'exploitation**<br>**Exploitation en temps réel** | **Faible** | L'entité responsable a testé le ou les plans de rétablissement conformément à l'alinéa 2.1 (E2) dans un intervalle de plus de 15 mois civils et d'au plus 16 mois civils | L'entité responsable a testé le ou les plans de rétablissement conformément à l'alinéa 2.1 (E2) dans un intervalle de plus de 16 mois civils et d'au plus 17 mois civils | L'entité responsable a testé le ou les plans de rétablissement conformément à l'alinéa 2.1 (E2) dans un intervalle de plus de 17 mois civils et d'au plus 18 mois civils | L'entité responsable n'a pas testé le ou les plans de rétablissement conformément à l'alinéa 2.1 (E2) dans un intervalle de 18 mois civils entre les tests. (2.1) |

| Ex. | Horizon | VRF | Niveaux de gravité de la non-conformité (CIP-009-6) | | | |
|---|---|---|---|---|---|---|
| | | | VSL faible | VSL modéré | VSL élevé | VSL critique |
| | | | entre les tests. (2.1)<br>OU<br>L'entité responsable a testé un échantillon représentatif de l'information utilisée pour le rétablissement de la fonctionnalité du *système électronique BES* conformément à l'alinée 2.2 (E2) dans un intervalle de plus de 15 mois civils et d'au plus 16 mois civils entre les tests. (2.2)<br>OU<br>L'entité responsable a testé le plan de rétablissement conformément à l'alinéa 2.3 (E2) dans un intervalle de plus de 36 mois civils et d'au plus 37 mois civils entre les tests. (2.3) | entre les tests. (2.1)<br>OU<br>L'entité responsable a testé un échantillon représentatif de l'information utilisée pour le rétablissement de la fonctionnalité du *système électronique BES* conformément à l'alinéa 2.2 (E2) dans un intervalle de plus de 16 mois civils et d'au plus 17 mois civils entre les tests. (2.2)<br>OU<br>L'entité responsable a testé le plan de rétablissement conformément à l'alinéa 2.3 (E2) dans un intervalle de plus de 37 mois civils et d'au plus 38 mois civils entre les tests. (2.3) | entre les tests. (2.1)<br>OU<br>L'entité responsable a testé un échantillon représentatif de l'information utilisée pour le rétablissement de la fonctionnalité du *système électronique BES* conformément à l'alinéa 2.2 (E2) dans un intervalle de plus de 17 mois civils et d'au plus 18 mois civils entre les tests. (2.2)<br>OU<br>L'entité responsable a testé le plan de rétablissement conformément à l'alinéa 2.3 (E2) dans un intervalle de plus de 38 mois civils et d'au plus 39 mois civils entre les tests. (2.3) | OU<br>L'entité responsable n'a pas testé un échantillon représentatif de l'information utilisée pour le rétablissement de la fonctionnalité du *système électronique BES* conformément à l'alinéa 2.2 (E2) dans un intervalle de 18 mois civils entre les tests. (2.2)<br>OU<br>L'entité responsable n'a pas testé le ou les plans de rétablissement conformément à l'alinéa 2.3 (E2) dans un intervalle de 39 mois civils entre les tests. (2.3) |
| **E3** | **Évaluation des activités d'exploitation** | **Faible** | L'entité responsable a avisé chaque personne ou groupe jouant un rôle défini dans le ou les plans de rétablissement des mises à jour dans un délai de plus de 90 jours civils et de moins de 120 jours civils suivants la réalisation | L'entité responsable a mis à jour le ou les plans de rétablissement en tenant compte de toutes les leçons apprises documentées dans un délai de plus de 90 jours civils et de moins de 120 jours civils suivants chaque test de plan de | L'entité responsable a documenté les leçons apprises ou leur absence dans un délai de plus de 90 jours civils et de moins de 120 jours civils suivant chaque test de plan de rétablissement ou rétablissement réel. (3.1.1) | L'entité responsable n'a documenté ni les leçons apprises ni leur absence dans un délai de 120 jours civils suivant chaque test de plan de rétablissement ou rétablissement réel. (3.1.1) |

| Ex. | Horizon | VRF | Niveaux de gravité de la non-conformité (CIP-009-6) | | | |
|---|---|---|---|---|---|---|
| | | | VSL faible | VSL modéré | VSL élevé | VSL critique |
| | | | complète de la mise à jour. (3.1.3) | rétablissement ou rétablissement réel. (3.1.2)<br><br>OU<br><br>L'entité responsable n'a pas avisé chaque personne ou groupe jouant un rôle défini dans le ou les plans de rétablissement des mises à jour dans un délai de 120 jours civils suivant la réalisation complète de la mise à jour. (3.1.3)<br><br>OU<br><br>L'entité responsable a mis à jour le ou les plans de rétablissement et avisé chaque personne ou groupe jouant un rôle défini dans un délai de plus de 60 jours civils et de moins de 90 jours civils suivants un des changements ci-après que l'entité responsable juge susceptible d'avoir un impact sur la capacité d'exécuter le plan : (3.2)<br>• rôles et responsabilités<br>• intervenants, ou<br>• changements | OU<br><br>L'entité responsable n'a pas mis à jour le ou les plans de rétablissement en tenant compte de toutes les leçons apprises documentées dans un délai de 120 jours civils suivant chaque test de plan de rétablissement ou rétablissement réel. (3.1.2)<br><br>OU<br><br>L'entité responsable n'a pas mis à jour le ou les plans de rétablissement ou avisé chaque personne ou groupe jouant un rôle défini dans un délai de 90 jours civils suivants un des changements ci-après que l'entité responsable juge susceptible d'avoir un impact sur la capacité d'exécuter le plan : (3.2)<br>• rôles et responsabilités<br>• intervenants, ou<br>• changements technologiques. | |

| Ex. | Horizon | VRF | Niveaux de gravité de la non-conformité (CIP-009-6) | | | |
|---|---|---|---|---|---|---|
| | | | VSL faible | VSL modéré | VSL élevé | VSL critique |
| | | | | technologiques. | | |

### D. Différences régionales

Aucune.

### E. Interprétations

Aucune.

### F. Documents connexes

Aucun.

## Historique des versions

| Version | Date | Modification apportée | Suivi des modifications |
|---|---|---|---|
| 1 | 16 janvier 2006 | E3.2 — Remplacement de « Control Center » par « control center ». | 24 mars 2006 |
| 2 | 30 septembre 2009 | Modifications visant à clarifier les exigences et à mettre les éléments de conformité en concordance avec les plus récentes directives sur l'établissement des éléments de conformité des normes.<br><br>Suppression de la mention sur la prise en compte des considérations d'affaires.<br><br>Remplacement de l'organisation régionale de fiabilité par l'entité régionale comme entité responsable.<br><br>Reformulation de la date d'entrée en vigueur.<br><br>Remplacement de « Responsabilité de la surveillance de la conformité » par « Responsable de la surveillance de l'application des normes ». | |

| Version | Date | Modification apportée | Suivi des modifications |
|---|---|---|---|
| 3 | | Changement du numéro de version de -2 à -3.<br>À l'exigence 1.6, suppression de la phrase traitant de la mise hors service d'un composant ou d'un système en vue d'effectuer la vérification conformément à l'ordonnance de la FERC du 30 septembre 2009. | |
| 3 | 16 décembre 2009 | Approbation par le Conseil d'administration de la NERC. | |
| 3 | 31 mars 2010 | Approbation par la FERC. | |
| 4 | 24 janvier 2011 | Approbation par le Conseil d'administration de la NERC. | |
| 5 | 26 novembre 2012 | Adoption par le Conseil d'administration de la NERC. | Modification en coordination avec les autres normes CIP et révision du format selon le modèle RBS. |
| 5 | 22 novembre 2013 | Ordonnance de la FERC approuvant la norme CIP-009-5. | |
| 6 | 13 novembre 2014 | Adoption par le Conseil d'administration de la NERC. | Mise en œuvre de prescriptions de l'ordonnance 791. |
| 6 | 21 janvier 2016 | Ordonnance de la FERC émise approuvant CIP-003-6. Dossier no. RM15-14-000 | |

## Principes directeurs et fondements techniques

### Section 4 – Portée de l'applicabilité des normes CIP sur la cybersécurité

La section 4 (Applicabilité) des normes présente de l'information importante pour aider les entités responsables à déterminer la portée d'application des exigences CIP sur la cybersécurité.

La section 4.1 (Entités fonctionnelles) présente la liste des entités fonctionnelles de la NERC auxquelles s'applique la norme. Si l'entité est enregistrée au titre d'une ou de plusieurs des entités fonctionnelles énumérées à la section 4.1, les normes CIP sur la cybersécurité de la NERC s'y appliquent. Il est à noter qu'en ce qui concerne les *distributeurs*, la section 4.1 limite l'applicabilité à ceux qui détiennent certains types de systèmes et d'équipements énumérés à la section 4.2.

La section 4.2 (Installations) définit la portée des *installations*, systèmes et équipements détenus par l'entité responsable qui, selon la section 4.1, est visée par les exigences de la norme. Comme il est indiqué à la section d'exemption 4.2.3.5, la présente norme ne s'applique pas aux entités responsables qui n'ont pas de *systèmes électroniques BES* à impact élevé ou moyen selon la catégorisation de la norme CIP-002-5.1. Outre l'ensemble des *installations* du *BES*, des *centres de contrôle* et des autres systèmes et équipements, la liste comprend l'ensemble des systèmes et équipements détenus par les *distributeurs*. Bien que le terme « *installations* » dans le glossaire de la NERC indique déjà qu'il s'agit d'*éléments* du *BES*, l'utilisation additionnelle du terme « *BES* » vise ici à renforcer la portée d'applicabilité pour ces *installations*, en particulier dans cette section sur l'applicabilité. Cela aide à clarifier quels sont les *installations*, systèmes et équipements visés par les normes.

### Exigence E1

Les directives suivantes servent de guide pour les éléments que doit comporter un plan de rétablissement :

- North American Electric Reliability Corporation (NERC). *Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions*. Septembre 2011. En ligne à l'adresse suivante : http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf.
- National Institute of Standards and Technology (NIST). *Contingency Planning Guide for Federal Information Systems*. Special Publication 800-34 Revision 1. Mai 2010. En ligne à l'adresse suivante : http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf.

Le terme « plan de rétablissement » est utilisé dans la présente norme de fiabilité pour désigner un ensemble documenté d'instructions et de ressources nécessaires au rétablissement des fonctions de fiabilité exercées par les *systèmes électroniques BES*. Le plan de rétablissement peut s'inscrire dans un plan global de continuité des activités ou de reprise après sinistre, mais ce terme n'implique pas d'autres obligations associées aux disciplines non visées par les exigences.

Un plan de rétablissement documenté peut ne pas être nécessaire pour chaque *système électronique BES* visé. Par exemple, le plan de rétablissement à court terme d'un *système électronique BES* situé dans un poste électrique donné peut être géré quotidiennement à l'aide d'applications avancées pour les réseaux électriques (estimation d'état, contingences et : http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order_RBR_ROP_10152015_RR15-4.pdf

mesures correctives, gestion prévisionnelle des retraits, etc.). Un seul plan de rétablissement de *systèmes électroniques BES* devrait être suffisant pour plusieurs installations similaires, comme celles qu'on trouve dans les postes électriques ou les centrales.

Selon l'alinéa 1.1, les conditions de déclenchement du plan de rétablissement doivent tenir compte de menaces viables pour le *système électronique BES*, comme une catastrophe naturelle, une panne de matériel ou d'environnement informatique ou un *incident de cybersécurité*. Une analyse des incidences opérationnelles pour le *système électronique BES* peut s'avérer utile en vue de déterminer ces conditions.

Selon l'alinéa 1.2, les entités doivent désigner les personnes chargées des mesures de rétablissement du *système électronique BES* visé.

Selon l'alinéa 1.3, les entités doivent tenir compte des types d'information suivants lors du rétablissement des *systèmes électroniques BES* :

1. fichiers et supports d'installation ;
2. bandes de sauvegarde courantes et autres paramètres de configuration documentés ;
3. procédures documentées d'assemblage ou de restauration ; et
4. stockage de duplication entre les sites.

Selon l'alinéa 1.4, les processus de vérification du bon déroulement des processus de sauvegarde doivent comprendre notamment : 1) la vérification de l'intégrité des supports de sauvegarde, 2) la vérification des journaux ou une inspection attestant que l'information du système de production courant peut être lue, et 3) la vérification des journaux ou une inspection attestant que l'information a été écrite sur le support de sauvegarde. Cet alinéa de l'exigence n'impose pas l'exécution d'essais de restauration. Les scénarios de sauvegarde suivants donnent des exemples de processus efficaces pour vérifier le bon déroulement des sauvegardes et déceler les échecs de sauvegarde :

- Processus de sauvegarde périodique (p. ex., quotidienne ou hebdomadaire) – Examen des journaux générés ou des rapports d'état des travaux et mise en place d'avis d'échec de sauvegarde.
- Processus de sauvegarde non périodique – Essai initial et essais périodiques (tous les 15 mois) seulement si une sauvegarde unique est fournie durant la mise en service du système. Essais supplémentaires effectués au besoin, par exemple dans le cadre du programme de gestion des changements de configuration.

- Écriture de données miroir – Configuration d'alertes en cas d'échec de transfert de données pendant un délai précisé par l'entité (p. ex., 15 minutes), après lequel l'information miroir n'est peut-être plus utile aux fins de rétablissement.
- Données de configuration manuelle – Inspection initiale et périodique (tous les 15 mois) des données utilisées pour le rétablissement avant leur stockage. Inspections supplémentaires effectuées au besoin, par exemple dans le cadre du programme de gestion des changements de configuration.

Le plan doit aussi inclure des processus de prise en compte des échecs de sauvegarde, qui précisent les mesures à prendre en cas d'avis d'échec ou de toute autre indication d'un échec.

Selon l'alinéa 1.5, le plan de rétablissement doit inclure des modalités de conservation des données permettant de déterminer la cause d'un *incident de cybersécurité*. Puisqu'il n'est pas toujours possible de savoir initialement si un *incident de cybersécurité* constitue la cause du déclenchement du plan de rétablissement, les procédures de conservation des données doivent être suivies tant et aussi longtemps que la possibilité d'un *incident de cybersécurité* n'est pas écartée. La norme CIP-008 traite de la conservation des données associées à ce type d'incident.

**Exigence E2**

Une entité responsable doit tester chaque plan de rétablissement des *systèmes électroniques BES* tous les 15 mois. Toutefois, cela ne veut pas nécessairement dire que l'entité doit mettre à l'essai chaque plan individuellement. Les *systèmes électroniques BES* qui sont répartis et en grand nombre, comme ceux qu'on trouve dans les postes électriques, peuvent ne pas nécessiter un plan de rétablissement individuel et les installations redondantes connexes si les mesures à prendre en cas d'événement grave consistent généralement à reconfigurer et à reconstruire ces systèmes. Inversement, chaque zone de production-transport d'électricité comporte habituellement un centre de contrôle nécessitant une installation redondante ou de repli. Étant donné ces différences, les plans de rétablissement associés aux centres de contrôle diffèrent grandement de ceux qui sont associés aux centrales et aux postes électriques.

Le test d'un plan de rétablissement ne porte pas nécessairement sur tous les aspects du plan ou des scénarios de panne, mais il doit suffire pour faire en sorte que le plan soit à jour et il doit porter sur au moins un processus de restauration des systèmes électroniques visés.

Les entités peuvent remplacer un test du plan aux 15 mois par un rétablissement suivant un incident réel. Autrement, elles doivent mettre à l'essai le plan au moyen d'un exercice sur papier, d'un exercice sur table ou d'un exercice opérationnel. Le programme *Homeland Security Exercise and Evaluation Program (HSEEP*) de la Federal Emergency Management Agency (FEMA) présente d'autres types d'exercices, dont les quatre types suivants d'exercices axés sur les discussions : séminaires, ateliers, exercices sur table et jeux. Il définit, en particulier, l'exercice sur table, à savoir « un exercice où des membres clés du personnel se réunissent pour discuter de scénarios de simulation dans un contexte informel. On peut avoir recours à des exercices sur table pour évaluer des plans, des politiques ou des procédures. »

Le programme HSEEP énumère les trois types suivants d'exercices axés sur les opérations : exercice d'entraînement, exercice fonctionnel et exercice à grand déploiement. Il définit, en

particulier, l'exercice à grand déploiement, à savoir « un exercice multidisciplinaire, intergouvernemental et multi-agences qui donne lieu à des interventions fonctionnelles (bureaux locaux conjoints, centres des opérations d'urgence, etc.) et sur le terrain (pompiers décontaminant des mannequins, etc.). »

Selon l'alinéa 2.2, les entités doivent se reporter aux exigences de sauvegarde et de stockage de l'information nécessaire au rétablissement des *systèmes électroniques BES* précisées à l'alinéa 1.3. Cela permet d'offrir une assurance supplémentaire que cette information permettra effectivement de rétablir le *système électronique BES*, le cas échéant. Dans le cas d'équipement informatique complexe, un essai complet de l'information est irréaliste. Les entités doivent alors déterminer l'échantillon représentatif de l'information qui offre une assurance dans les processus mentionnés à l'alinéa 1.3. Cet essai doit comprendre les étapes nécessaires pour s'assurer que l'information est à la fois utilisable et à jour. Dans le cas des supports de sauvegarde, il peut s'agir d'en mettre à l'essai un échantillon représentatif pour s'assurer que l'information peut être chargée et d'en vérifier le contenu pour s'assurer que l'information reflète la configuration courante des *actifs électroniques* visés.

**Exigence E3 :**

Cette exigence prescrit la tenue à jour par les entités de leurs plans de rétablissement. Deux alinéas de cette exigence déclenchent la mise à jour d'un plan : 1) les leçons apprises et 2) les changements organisationnels ou technologiques.

La documentation des leçons apprises concerne chaque déclenchement de plan de rétablissement, et comprend les activités illustrées à la figure 1 ci-dessous. Elle débute à la fin des activités de rétablissement, en reconnaissance du fait que les activités de rétablissement complexes peuvent prendre des jours sinon des semaines à réaliser. Durant le processus d'intégration des leçons apprises, l'équipe de rétablissement peut être amenée à discuter de l'incident en vue de déterminer les lacunes ou les points à améliorer dans le plan. Il est possible qu'aucune leçon apprise documentée ne soit associée à un déclenchement de plan de rétablissement. Dans un tel cas, l'entité doit conserver les documents attestant l'absence de leçons apprises associées à ce déclenchement.

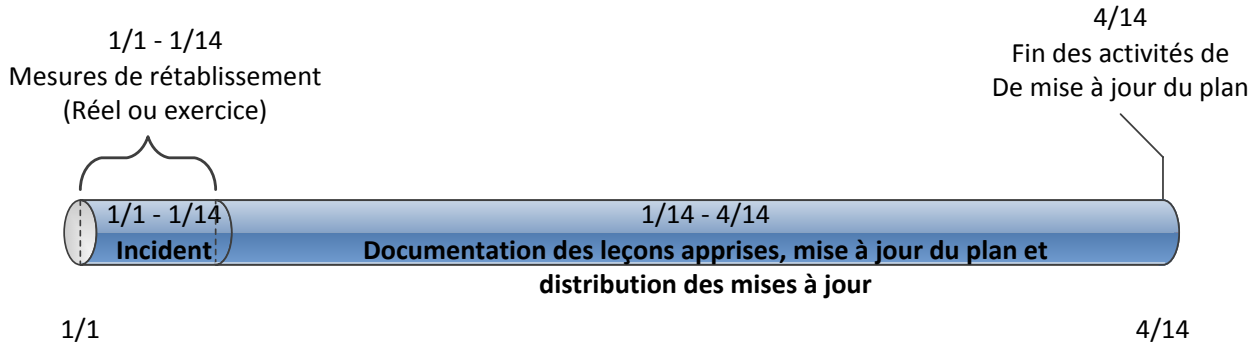


**Figure 1 : Calendrier pour l'exigence E3 de la norme CIP-009-6**

Les activités nécessaires pour intégrer les leçons apprises au plan comprennent notamment la mise à jour du plan et la distribution de ces mises à jour. Les entités doivent envisager de

rencontrer toutes les personnes concernées par le plan de rétablissement et de documenter les leçons apprises aussitôt que possible après qu'il a été déclenché. On disposera ainsi d'un plus long délai pour mettre à jour le plan, obtenir les approbations requises et distribuer ces mises à jour à l'équipe de rétablissement.

L'exigence portant sur la révision du plan concerne les changements organisationnels et technologiques aux éléments touchés par le plan et vise les activités illustrées à la figure 2 ci-dessous. Parmi les changements organisationnels, on compte les changements apportés aux rôles et responsabilités des personnes définis dans le plan et aux groupes ou personnes chargés de l'intervention. Il peut s'agir de changements apportés à des noms ou à des coordonnées cités dans le plan. Les changements technologiques qui ont une incidence sur le plan peuvent être des changements apportés à des sources d'information, à des systèmes de communication ou à des systèmes d'établissement de tickets.

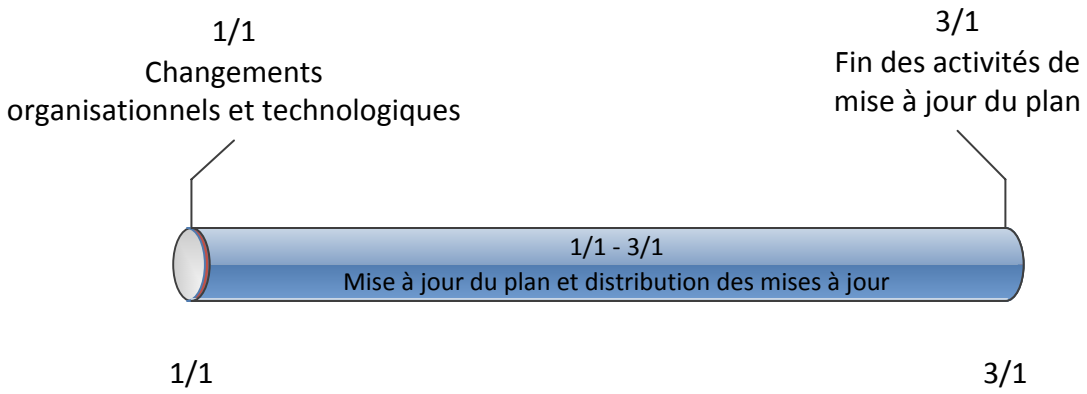


**Figure 2 : Calendrier pour les changements au plan de l'alinéa 3.2.**

Au moment d'aviser les personnes de changements apportés au plan d'intervention, les entités doivent garder à l'esprit que les plans de rétablissement peuvent être considérés comme de l'information de *système électronique BES*. Elles doivent donc prendre les mesures qui s'imposent pour empêcher la divulgation non autorisée de l'information contenue dans ces plans. Par exemple, le plan de rétablissement lui-même et toute autre information sensible concernant le plan doivent être retranchés des courriels et autres communications non cryptées.

## Justification

Pendant l'élaboration de cette norme, des zones de texte ont été incorporées à celle-ci pour exposer la justification de ses diverses parties. Après l'approbation par le Conseil d'administration, le contenu de ces zones de texte a été transféré ci-après.

**Justification de l'exigence E1**

Les activités de prévention peuvent limiter le nombre d'incidents, sans toutefois les prévenir tous. Il est donc nécessaire de se doter de moyens pour assurer un rétablissement rapide après

les incidents, limiter les pertes et la destruction, combler les lacunes exploitées et rétablir les services informatiques afin que la restauration des fonctionnalités des *systèmes électroniques BES* se fasse de manière cohérente et organisée.

**Justification de l'exigence E2**

La mise en œuvre d'un plan de rétablissement efficace réduit les risques posés au fonctionnement fiable du *BES* en réduisant le délai de rétablissement après différents types d'incidents nuisibles pour les *systèmes électroniques BES*. Cette exigence encadre la mise en œuvre continue des plans d'intervention.

L'alinéa 2.2 de cette exigence offre une assurance supplémentaire quant à l'information (bandes de sauvegarde, centres miroirs, etc.) nécessaire au rétablissement des *systèmes électroniques BES*. Dans la plupart des cas, une mise à l'épreuve complète du plan est irréaliste en raison de la grande quantité d'information nécessaire au rétablissement. L'entité responsable doit donc déterminer un échantillon qui offre l'assurance que l'information est utilisable.

**Justification de l'exigence E3**

Améliorer l'efficacité du ou des plans de rétablissement des *systèmes électroniques BES* après un essai et assurer la tenue à jour et la distribution de ces plans. Pour ce faire, les entités responsables doivent i) passer en revue les leçons apprises, selon l'alinéa 3.1, et ii) réviser le plan, selon l'alinéa 3.2, à la suite de changements organisationnels ou technologiques spécifiques qui pourraient avoir un impact sur l'exécution du plan. Dans les deux cas, l'entité responsable doit mettre à jour et distribuer le plan si celui-ci nécessite des modifications.

Annexe QC-CIP-009-6
Dispositions particulières de la norme CIP-009-6 applicables au Québec

Cette annexe établit les dispositions particulières d'application de la norme au Québec. Les dispositions de la norme et de son annexe doivent obligatoirement être lues conjointement pour fins de compréhension et d'interprétation. En cas de divergence entre la norme et l'annexe, l'annexe aura préséance.

## A. Introduction

**1. Titre :** Cybersécurité — Plans de rétablissement des systèmes électroniques BES

**2. Numéro :** CIP-009-6

**3. Objet :** Aucune disposition particulière

**4. Applicabilité :**

**4.1. Entités fonctionnelles**

**4.2. Installations**

La présente norme s'applique seulement aux installations du *réseau de transport principal* (RTP) et aux installations spécifiées pour le *distributeur*. Dans l'application de cette norme, toute référence aux termes « *système de production-transport d'électricité* » ou « BES » doit être remplacée par les termes « *réseau de transport principal* » ou « RTP » respectivement.

**Exemptions additionnelles**

Sont exemptés de l'application de la présente norme :

- Toute installation de production qui répond aux deux conditions suivantes : (1) la puissance nominale de l'installation est de 300 MVA ou moins et (2) aucun groupe de l'installation ne peut être synchronisé avec un réseau voisin.
- Postes élévateurs des installations de production identifiées au point précédent.

**5. Date d'entrée en vigueur au Québec :**

**5.1.** Adoption de la norme par la Régie de l'énergie : 31 octobre 2017

**5.2.** Adoption de l'annexe par la Régie de l'énergie : 31 octobre 2017

**5.3.** Date d'entrée en vigueur de la norme et de l'annexe au Québec : 1er janvier 2018

| Norme | Date de mise en application au Québec | | |
|---|---|---|---|
| | Entités visées par la version 1 des normes CIP adoptées par la Régie | Entités exemptées de l'application de la version 1 des normes CIP en vertu des dispositions particulières associées à ces normes | Entités qui possèdent des installations de production à vocation industrielle |
| CIP-009-6 | 2018-01-01 | 2018-10-01 | 2019-04-01 |

**6. Contexte :**

Aucune disposition particulière

## B. Exigences et mesures

Aucune disposition particulière

## C. Conformité

**1. Processus de surveillance de la conformité**

**1.1. Responsable des mesures pour assurer la conformité**

La Régie de l'énergie est responsable, au Québec, de la surveillance de l'application de la norme de fiabilité et de son annexe qu'elle adopte.

**1.2. Conservation des pièces justificatives**

Aucune disposition particulière

**1.3. Processus de surveillance et de mise en application des normes**

Aucune disposition particulière

**1.4. Autres informations sur la conformité**

Aucune disposition particulière

**2. Tableau des éléments de conformité**

Aucune disposition particulière

## D. Différences régionales

Aucune disposition particulière

## E. Interprétations

Aucune disposition particulière

## F. Documents connexes

Aucune disposition particulière

## Principes directeurs et fondements techniques

Aucune disposition particulière

## Justification

Aucune disposition particulière

## Historique des versions

| Révision | Date | Intervention | Suivi des modifications |
|---|---|---|---|
| 0 | 31 octobre 2017 | Nouvelle annexe. | Nouvelle |