

A. Introduction

1. **Titre :** Cybersécurité – Gestion des risques dans la chaîne d’approvisionnement
2. **Numéro :** CIP-013-~~12~~
3. **Objet :** 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*.
4. **Applicabilité :**
 - 4.1. **Entités fonctionnelles :** Dans le contexte de la présente norme, les entités fonctionnelles indiquées ci-après sont appelées collectivement « entités responsables ». Si certaines exigences visent plus spécifiquement une entité fonctionnelle ou un sous-ensemble 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 systèmes, *installations* et équipements suivants pour la protection ou la remise en charge du *BES* :
 - 4.1.2.1. Système de délestage de charge en sous-fréquence (DSF) ou 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 des délestages automatiques de *charge* de 300 MW ou plus sous la commande d’un système commun détenu par l’entité responsable, sans intervention humaine.
 - 4.1.2.2. *Automatisme de réseau (RAS)* visé par une ou plusieurs exigences d’une norme de fiabilité de la NERC ou de l’*entité régionale*.
 - 4.1.2.3. *Système de protection* de réseau de *transport* (à l’exclusion des systèmes de DSF et de DST) visé par une ou plusieurs exigences d’une norme de fiabilité de la NERC ou de l’*entité régionale*.
 - 4.1.3. **Exploitant d’installation de production**
 - 4.1.4. **Propriétaire d’installation de production**
 - 4.1.5. **Coordonnateur de la fiabilité**
 - 4.1.6. **Exploitant de réseau de transport**
 - 4.1.7. **Propriétaire d’installation de transport**

4.2. Installations : Dans le contexte de la présente norme, les systèmes, *installations* et équipements suivants détenus par une entité responsable indiquée à la section 4.1 sont visés par les exigences. Si certaines exigences visent plus spécifiquement un type ou un sous-ensemble de systèmes, d’*installations* ou d’équipements, ceux-ci sont précisés explicitement.

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

4.2.1.1. 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 des délestages de *charge* automatiques de 300 MW ou plus sous la commande d’un système commun détenu par l’entité responsable, sans intervention humaine.

4.2.1.2. *Automatisme de réseau (RAS)* visé par une ou plusieurs exigences d’une norme de fiabilité de la NERC ou de l’*entité régionale*.

4.2.1.3. *Système de protection* de réseau de *transport* (à l’exclusion des systèmes de DSF et de DST) visé par une ou plusieurs exigences d’une norme de fiabilité de la NERC ou de l’*entité régionale*.

4.2.1.4. *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-013-~~12~~ :

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 *périmètres de sécurité électronique (ESP)* 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 ont déterminé n’avoir aucun *système électronique BES* classé dans les catégories « impact élevé » ou « impact moyen » selon le processus d’inventaire et de catégorisation ~~prescrit dans la~~ de la norme ~~de fiabilité~~ CIP-002-~~5~~ ou toute version postérieure.

5. **Date d’entrée en vigueur** : Voir le plan de mise en œuvre du projet ~~2016~~2019-03.

B. Exigences et mesures

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

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.~~ la coordination des contrôles visant les accès distants commandés par un fournisseur.

M1. 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.

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.

- M2.** 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.
- 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]
- M3.** 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.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité

Le terme « *responsable des mesures pour assurer la conformité* » (CEA) désigne la NERC ou l’*entité régionale*, ou toute entité désignée par un organisme gouvernemental pertinent, dans leurs rôles respectifs visant à surveiller et à assurer la conformité avec les normes de fiabilité obligatoires et exécutoires de la NERC dans leurs territoires respectifs.

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 afin de démontrer sa conformité. Dans les cas où la période de conservation indiquée est plus courte que le temps écoulé depuis ~~l’audit le plus récent~~ 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 ~~l’audit le plus récent~~ le dernier audit.

Chaque 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 ~~chacune des exigences~~ chaque exigence de la présente norme pendant trois années civiles.
- Si une entité responsable est jugée non conforme ~~à une exigence~~, 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 dossiers de l’audit le plus récent ainsi que tous les dossiers d’audit ~~subéquents demandés et présentés~~ demandés et soumis par la suite.

1.3. Programme de surveillance ~~et de mise en application~~ de la conformité et d’application des normes

Selon la définition des règles de procédure de la NERC, l’expression « programme de surveillance ~~et de mise en application~~ de la conformité et d’application des normes » désigne la liste des processus qui serviront à évaluer les données ou l’information afin de déterminer les résultats de conformité avec la norme de fiabilité.

Niveaux de gravité de la non-conformité (VSL)

Ex.	Niveaux de gravité de la non-conformité			
	VSL faible	VSL modéré	VSL élevé	VSL critique
E1.	<p>L’entité responsable a établi un ou des plans documentés de gestion des risques de cybersécurité dans la chaîne d’approvisionnement, qui comprennent un ou des processus utilisés dans la planification de l’acquisition de <i>systèmes électroniques BES</i> <u>ainsi que des EACMS et des PACS associés</u> afin de déterminer et d’évaluer les risques de cybersécurité pour le <i>BES</i> conformément à l’alinéa 1.1, et comprenant un ou des processus utilisés dans l’acquisition de <i>systèmes électroniques BES</i> <u>ainsi que des EACMS et des PACS associés</u> conformément à l’alinéa 1.2, mais ce ou ces plans omettent une des prescriptions des alinéas 1.2.1 à 1.2.6.</p>	<p>L’entité responsable a établi un ou des plans documentés de gestion des risques de cybersécurité dans la chaîne d’approvisionnement, qui comprennent un ou des processus utilisés dans la planification de l’acquisition de <i>systèmes électroniques BES</i> <u>ainsi que des EACMS et des PACS associés</u> afin de déterminer et d’évaluer les risques de cybersécurité pour le <i>BES</i> conformément à l’alinéa 1.1, et comprenant un ou des processus utilisés dans l’acquisition de <i>systèmes électroniques BES</i> <u>ainsi que des EACMS et des PACS associés</u> conformément à l’alinéa 1.2, mais ce ou ces plans omettent au moins deux des prescriptions des alinéas 1.2.1 à 1.2.6.</p>	<p>L’entité responsable a établi un ou des plans documentés de gestion des risques de cybersécurité dans la chaîne d’approvisionnement, mais ce ou ces plans ne comprennent pas de processus utilisé dans la planification de l’acquisition de <i>systèmes électroniques BES</i> <u>ainsi que des EACMS et des PACS associés</u> afin de déterminer et d’évaluer les risques de cybersécurité pour le <i>BES</i> conformément à l’alinéa 1.1, ou ne comprennent pas de processus utilisé dans l’acquisition de <i>systèmes électroniques BES</i> <u>ainsi que des EACMS et des PACS associés</u> conformément à l’alinéa 1.2.</p>	<p>L’entité responsable a établi un ou des plans documentés de gestion des risques de cybersécurité dans la chaîne d’approvisionnement, mais ce ou ces plans ne comprennent pas de processus utilisé dans la planification de l’acquisition de <i>systèmes électroniques BES</i> <u>ainsi que des EACMS et des PACS associés</u> afin de déterminer et d’évaluer les risques de cybersécurité pour le <i>BES</i> conformément à l’alinéa 1.1, et ne comprennent pas non plus de processus utilisé dans l’acquisition de <i>systèmes électroniques BES</i> <u>ainsi que des EACMS et des PACS associés</u> conformément à l’alinéa 1.2.</p> <p>OU</p> <p>L’entité responsable n’a établi aucun plan documenté de gestion des risques de cybersécurité dans la chaîne d’approvisionnement, en contravention avec l’exigence.</p>

Ex.	Niveaux de gravité de la non-conformité			
	VSL faible	VSL modéré	VSL élevé	VSL critique
E2.	<p>L’entité responsable a mis en œuvre son ou ses plans documentés de gestion des risques de cybersécurité dans la chaîne d’approvisionnement, comprenant un ou des processus utilisés dans la planification de l’acquisition de <i>systèmes électroniques BES</i> <u>ainsi que des EACMS et des PACS associés</u> afin de déterminer et d’évaluer les risques de cybersécurité pour le <i>BES</i> conformément à l’alinéa 1.1 de l’exigence E1, et comprenant un ou des processus utilisés dans l’acquisition de <i>systèmes électroniques BES</i> <u>ainsi que des EACMS et des PACS associés</u> conformément à l’alinéa 1.2 de l’exigence E1, mais cette mise en œuvre a omis une des prescriptions des alinéas 1.2.1 à 1.2.6.</p>	<p>L’entité responsable a mis en œuvre son ou ses plans documentés de gestion des risques de cybersécurité dans la chaîne d’approvisionnement, comprenant un ou des processus utilisés dans la planification de l’acquisition de <i>systèmes électroniques BES</i> <u>ainsi que des EACMS et des PACS associés</u> afin de déterminer et d’évaluer les risques de cybersécurité pour le <i>BES</i> conformément à l’alinéa 1.1 de l’exigence E1, et comprenant un ou des processus utilisés dans l’acquisition de <i>systèmes électroniques BES</i> <u>ainsi que des EACMS et des PACS associés</u> conformément à l’alinéa 1.2 de l’exigence E1, mais cette mise en œuvre a omis au moins deux des prescriptions des alinéas 1.2.1 à 1.2.6.</p>	<p>L’entité responsable a mis en œuvre son ou ses plans documentés de gestion des risques de cybersécurité dans la chaîne d’approvisionnement, mais sans mettre en œuvre un ou des processus utilisés dans la planification de l’acquisition de <i>systèmes électroniques BES</i> <u>ainsi que des EACMS et des PACS associés</u> afin de déterminer et d’évaluer les risques de cybersécurité pour le <i>BES</i> conformément à l’alinéa 1.1 de l’exigence E1, ou sans mettre en œuvre un ou des processus utilisés dans l’acquisition de <i>systèmes électroniques BES</i> <u>ainsi que des EACMS et des PACS associés</u> conformément à l’alinéa 1.2 de l’exigence E1.</p>	<p>L’entité responsable a mis en œuvre son ou ses plans documentés de gestion des risques de cybersécurité dans la chaîne d’approvisionnement, mais sans mettre en œuvre un ou des processus utilisés dans la planification de l’acquisition de <i>systèmes électroniques BES</i> <u>ainsi que des EACMS et des PACS associés</u> afin de déterminer et d’évaluer les risques de cybersécurité pour le <i>BES</i> conformément à l’alinéa 1.1 de l’exigence E1, et sans non plus mettre en œuvre un ou des processus utilisés dans l’acquisition de <i>systèmes électroniques BES</i> <u>ainsi que des EACMS et des PACS associés</u> conformément à l’alinéa 1.2 de l’exigence E1.</p> <p>OU</p> <p>L’entité responsable n’a mis en œuvre aucun plan documenté de gestion des risques de cybersécurité dans la chaîne d’approvisionnement, en contravention avec l’exigence.</p>

Ex.	Niveaux de gravité de la non-conformité			
	VSL faible	VSL modéré	VSL élevé	VSL critique
E3.	L’entité responsable a réexaminé et fait approuver par le <i>cadre supérieur CIP</i> ou son délégataire son ou ses plans de gestion des risques de cybersécurité dans la chaîne d’approvisionnement, mais dans un délai de plus de 15 mois civils et d’au plus 16 mois civils suivant le réexamen précédent.	L’entité responsable a réexaminé et fait approuver par le <i>cadre supérieur CIP</i> ou son délégataire son ou ses plans de gestion des risques de cybersécurité dans la chaîne d’approvisionnement, mais dans un délai de plus de 16 mois civils et d’au plus 17 mois civils suivant le réexamen précédent.	L’entité responsable a réexaminé et fait approuver par le <i>cadre supérieur CIP</i> ou son délégataire son ou ses plans de gestion des risques de cybersécurité dans la chaîne d’approvisionnement, mais dans un délai de plus de 17 mois civils et d’au plus 18 mois civils suivant le réexamen précédent.	L’entité responsable n’a pas réexaminé et fait approuver par le <i>cadre supérieur CIP</i> ou son délégataire son ou ses plans de gestion des risques de cybersécurité dans la chaîne d’approvisionnement dans un délai de 18 mois civils suivant le réexamen précédent.

D. Différences régionales

Aucune.

E. Documents connexes

~~Lien vers le plan de mise en œuvre et d’autres documents connexes importants.~~

- Plan de mise en œuvre du projet 2019-03.
- Justification technique de la norme CIP-013-2.

Historique des versions

Version	Date	Intervention	Suivi des modifications
1	20 juillet 2017	Mise en œuvre de l’Ordonnance 829 de la FERC.	
1	10 août 2017	Approbation par le Conseil d’administration de la NERC.	
1	18 octobre 2018	Ordonnance de la FERC approuvant la norme CIP-013-1. Dossier RM17-13-000.	
<u>2</u>	<u>1^{er} août 2019</u>	<u>Modifications visant à répondre à certaines prescriptions de l’Ordonnance 850 de la FERC.</u>	<u>Révision</u>
<u>2</u>	<u>5 novembre 2020</u>	<u>Adoption par le Conseil d’administration de la NERC.</u>	

Justification

Exigence E1

~~L’exigence proposée met en œuvre les prescriptions de l’Ordonnance 829 de la FERC concernant la mise en œuvre par les entités d’un ou de plans spécifiant un processus d’atténuation des risques de cybersécurité dans la chaîne d’approvisionnement. Ce ou ces plans doivent répondre aux quatre objectifs suivants (Ordonnance 829, paragraphe 45):~~

- ~~1) intégrité et authenticité des logiciels ;~~
- ~~2) accès distant par les fournisseurs ;~~
- ~~3) planification des systèmes d’information ; et~~
- ~~4) gestion des risques liés aux fournisseurs et contrôles d’approvisionnement.~~

~~Le ou les plans de gestion des risques de cybersécurité prescrits à l’exigence E1 s’appliquent aux systèmes électroniques BES à impact moyen ou élevé.~~

~~La mise en œuvre d’un plan de gestion des risques de cybersécurité 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), comme le précise l’Ordonnance 829 (paragraphe 36).~~

~~L’alinéa 1.1 de l’exigence E1 met en œuvre la prescription de l’Ordonnance 829 qui demande de déterminer et de documenter les risques de cybersécurité au cours du processus de planification et de préparation en amont de l’acquisition de systèmes électroniques BES (paragraphe 56). L’objectif de sécurité est d’une part d’amener les entités à envisager les risques de cybersécurité pour le BES liés aux produits et 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. D’autre part, les entités doivent être amenées à envisager les moyens d’atténuer ces risques à l’étape de planification des systèmes électroniques BES.~~

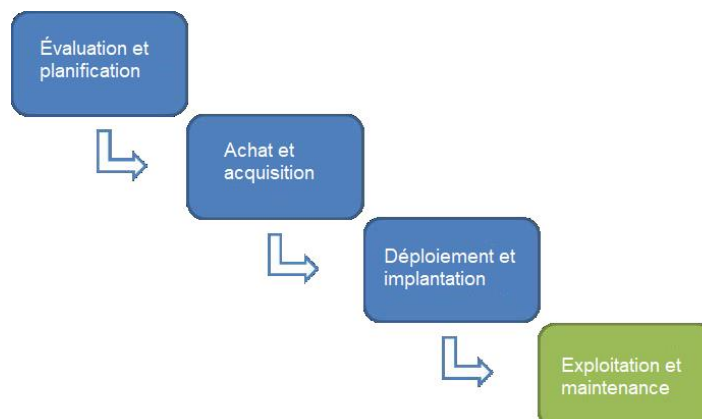
L’alinéa 1.2 de l’exigence E1 met en œuvre la prescription de l’Ordonnance 829 qui demande que des contrôles d’approvisionnement assurent l’intégration et l’application des concepts de sécurité dans les contrats futurs de systèmes électroniques BES (paragraphe 59). L’objectif visé est que les entités incorporent ces concepts dans leurs plans de manière que les risques pertinents soient pris en compte dans le processus d’acquisition et dans les négociations contractuelles. La mise en œuvre du plan de gestion des risques prescrit à l’alinéa 1.2 peut être réalisée dans le cadre des processus d’acquisition et de négociation contractuelle de l’entité. Par exemple, l’entité responsable peut intégrer les critères pertinents de son plan dans les appels de propositions, les négociations avec les fournisseurs, ou encore les demandes transmises à des entités chargées de négocier en son nom (ententes d’achat coopératif, etc.). L’intégration de certains contrôles dans le contrat négocié n’est pas toujours possible ; dans de tels cas, on ne considère pas que la mise en œuvre du plan de l’entité a échoué. Par ailleurs, bien qu’on s’attende à ce que l’entité responsable veille à faire respecter les dispositions contractuelles relatives à la sécurité, la mise en exécution du contrat et le respect de celui-ci par le fournisseur ne sont pas visés par cette norme de fiabilité.

L’exigence de vérifier l’intégrité et l’authenticité des logiciels (alinéa 1.2.5) vise à ce que les logiciels installés dans des systèmes électroniques BES ne soient pas modifiés à l’insu de leur fournisseur avant l’installation, et qu’ils ne soient pas contrefaits. L’alinéa 1.2.5 n’est pas une exigence opérationnelle qui oblige l’entité à effectuer une telle vérification ; il demande plutôt à l’entité de tenir compte de l’enjeu de l’intégrité et de l’authenticité des logiciels dans son processus contractuel, afin d’avoir ensuite les moyens de réaliser cette vérification dans le cadre de la norme CIP-010-3.

Le terme « fournisseur » utilisé dans cette norme désigne uniquement les personnes, entreprises ou autres organisations avec lesquelles l’entité responsable, ou une société affiliée, est en relation contractuelle en vue de la fourniture de systèmes électroniques BES et de services connexes. Ce terme exclut les autres entités inscrites auprès de la NERC qui fournissent des services de fiabilité (par exemple, des services de responsable de l’équilibrage ou de coordonnateur de la fiabilité dans le cadre des normes de fiabilité de la NERC). Un fournisseur, selon l’emploi de ce terme dans la norme, peut comprendre : i) des créateurs de logiciels ou de systèmes d’information, des fabricants de composants de système ou des prestataires de services informatiques ; ii) des revendeurs de produits ; ou iii) des intégrateurs de systèmes.

Collectivement, les dispositions de la norme CIP-013-1 concernent les contrôles d’une entité visant à gérer les risques de cybersécurité pour les systèmes électroniques BES pendant les phases de planification, d’acquisition et de déploiement du cycle de vie du système, selon le schéma ci-après.

Schéma du cycle de vie d’un système électronique BES



Exigence E2

~~L’exigence proposée met en œuvre les prescriptions de l’Ordonnance 829 qui demandent aux entités de réévaluer périodiquement certains contrôles de gestion des risques de cybersécurité dans la chaîne d’acquisition (paragraphe 46).~~

~~Ces réévaluations périodiques permettent aux entités de tenir leurs plans à jour et de répondre aux inquiétudes et aux vulnérabilités, existantes ou émergentes, concernant la chaîne d’approvisionnement. Les entités peuvent, par exemple, prendre en compte les directives ou autres informations provenant :~~

- ~~• de la NERC ou de l’E-ISAC ;~~
- ~~• de l’ICS-CERT ;~~
- ~~• du Centre canadien de réponse aux incidents cybernétiques (CCRIC).~~

~~Les entités responsables ne sont pas obligées de renégocier ou de résilier des contrats existants (y compris des modifications aux ententes-cadres ou des bons de commande) lorsqu’elles mettent en œuvre un plan mis à jour ; la note de l’exigence E2 s’applique à la mise en œuvre non seulement des nouveaux plans, mais aussi des plans mis à jour).~~