

Séminaire annuel sur la fiabilité

6^e édition

6 octobre 2026



Table des matières

1. Le secteur de l'énergie face aux cybermenaces
2. Élaboration d'un programme de défense pour la cybersécurité et la sécurité physique
3. Faire le lien entre la gestion des risques et la fiabilité
4. Évaluation des risques inhérents et plans de surveillance de la conformité : Comment les risques influencent la surveillance
5. Au-delà des normes de fiabilité : ressources supplémentaires
6. Mise à jour des normes de fiabilité du Québec : Principaux changements pour 2026-2027
7. Participation des entités visées au processus de consultations publiques
8. Changements finaux du PSCAQ révisé et documentation des processus de surveillance et d'application
9. L'audit réglementaire : un levier d'amélioration continue
10. Plan d'action de la NERC relatif aux grands volumes de charge
11. Valeur stratégique du partage d'informations de l'E-ISAC pour la résilience de l'industrie mondiale
12. Survol des initiatives du comité d'utilisation des sanctions pécuniaires

Le secteur de l'énergie face aux cybermenaces

Jean-Philippe Racicot

Responsable de la présence nationale – Montréal

Séminaire annuel sur la fiabilité 2026
Régie de l'énergie

Mardi, 6 octobre 2026



Centre de la sécurité des
télécommunications Canada
Centre canadien
pour la cybersécurité

Communications Security
Establishment Canada
Canadian Centre
for Cyber Security

Canada

Centre de la sécurité des télécommunications Canada

Agence nationale de cryptologie du Canada

Centre canadien pour la cybersécurité (CCC)

Autorité technique du Canada en matière de cybersécurité



Nous utilisons notre expertise pour protéger les renseignements et les systèmes sur lesquels les Canadiens comptent tous les jours.



Nous travaillons à protéger et à défendre les actifs cybernétiques précieux du pays et à diriger la réponse fédérale du Canada aux événements de cybersécurité.

Nous élevons le niveau de la cybersécurité au Canada afin que les Canadiens puissent vivre et travailler en ligne en toute sécurité et avec confiance.

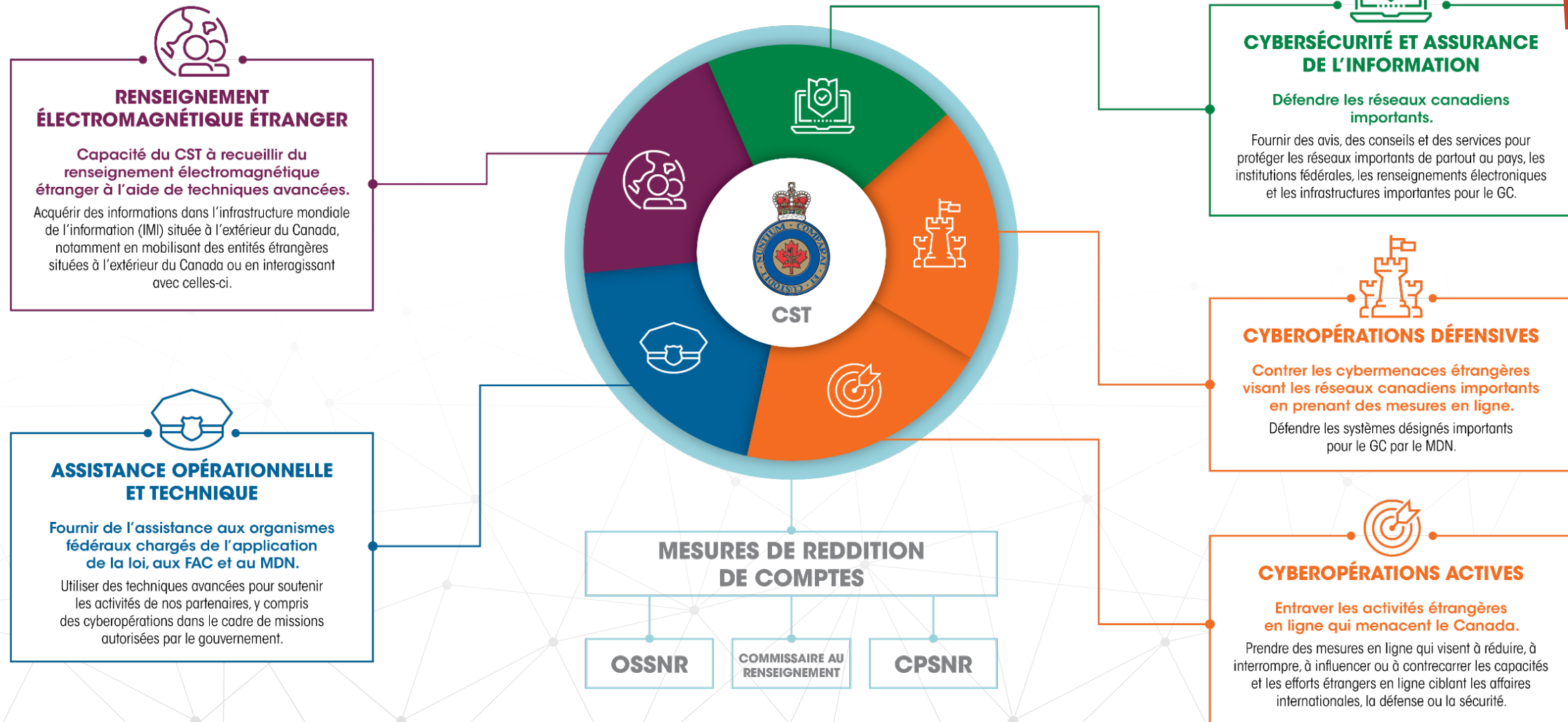


Centre de la sécurité des
télécommunications Canada
Centre canadien
pour la cybersécurité

Communications Security
Establishment Canada
Canadian Centre
for Cyber Security

Canada

LA LOI SUR LE CST | UN MANDAT EN CINQ VOILETS



Centre de la sécurité des
télécommunications Canada
Centre canadien
pour la cybersécurité

Communications Security
Establishment Canada
Canadian Centre
for Cyber Security

Canada

Écosystème fédéral de cybersécurité



Exécute des opérations cybernétiques pour protéger les réseaux militaires et soutenir les opérations.



Fournit une expertise nationale en cybersécurité en tant qu'autorité technique, répond aux incidents et défend les réseaux gouvernementaux.

- Centre canadien pour la cybersécurité (CCC)



Se concentre sur l'investigation et l'atténuation des menaces cybernétiques et la conduite d'opérations humaines pour protéger la sécurité nationale



Mène les enquêtes sur la cybercriminalité au Canada.

- Centre antifraude du Canada (CAFC)
- Centre national de coordination contre la cybercriminalité (NC3).
- CyberAide—Centre canadien de protection de l'enfance (C3P)



Se concentre sur les politiques, les orientations et l'allocation des ressources pour les efforts de cybersécurité militaire.

Leadership stratégique et gestion de l'information

- Bureau du dirigeant principal de l'information

Joue un rôle stratégique et de facilitation dans l'avancement de la cybersécurité au Canada.

- Réseau d'innovation en cybersécurité
- CyberSécuritaire Canada

Sécurise l'infrastructure TI du gouvernement du Canada et protège les données.

Se concentre sur la politique internationale en matière de cybersécurité, l'engagement diplomatique, le renforcement des capacités et l'attribution publique des menaces cybernétiques.

Dirige l'élaboration des politiques et stratégies nationales en tant qu'autorité des politiques sur la cybersécurité.



Centre de la sécurité des télécommunications Canada
Centre canadien pour la cybersécurité

Communications Security Establishment Canada
Canadian Centre for Cyber Security

Canada

Nos 16 secteurs d'infrastructures essentielles



21 (1) Le ministre peut, par arrêté, désigner comme étant **importante pour le gouvernement fédéral** de l'information électronique, des infrastructures de l'information ou des catégories d'information électronique ou d'infrastructures de l'information.



*Loi sur le CST - Section 21 :
Désignation d'un système
d'importance*



Centre de la sécurité des
télécommunications Canada
Centre canadien
pour la cybersécurité

Communications Security
Establishment Canada
Canadian Centre
for Cyber Security

Canada

L'année en revue

1er avril 2025 au 31 mars 2026

Le CCC a publié:

- Publications de conseils en matière de cybersécurité: 41
- Publications conjointes : 28
- Évaluations de menaces non classifiées: 7

9 Autorisations ministérielles approuvées durant l'année fiscale 2025-26.

6585

Personnes ayant participé aux cours du Carrefour de l'apprentissage.

14 700

Demandes générales reçues, triées et gérées

23

Séances d'information bimensuelles sur les menaces

3216

Incidents auquel le Centre pour la cybersécurité a aidé à répondre

4

Exercices de simulation auprès des infrastructures essentielles

67

Notifications de signes avant-coureurs d'une attaque par rançongiciel

1 772

Évaluations des risques liés à la chaîne d'approvisionnement complétées.

120

Allocutions données par des représentants et représentantes du Centre pour la cybersécurité.



Centre de la sécurité des
télécommunications Canada
Centre canadien
pour la cybersécurité

Communications Security
Establishment Canada
Canadian Centre
for Cyber Security

Canada

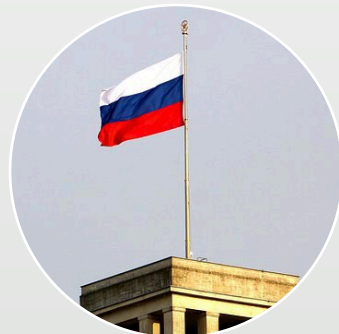
Principaux avis – ÉCMN 2025-26



Les États adversaires du Canada recourent à des cyberopérations pour causer des perturbations et créer des divisions.



Le programme de cyberactivité de la République populaire de Chine représente pour le Canada à l'heure actuelle la cybermenace la plus active et la plus sophistiquée.



Le programme de cyberactivité de la Russie renforce l'ambition de Moscou de vouloir confronter et déstabiliser le Canada et ses alliés.



L'Iran se sert de son programme de cyberactivité pour contraindre, harceler et réprimer ses adversaires et gérer les risques d'escalade.



Le modèle opérationnel de cybercriminalité comme service (CaaS) contribue sans doute au fait que la cybercriminalité se poursuit au Canada et dans le monde.



Les rançongiciels constituent la principale menace émanant de la cybercriminalité à laquelle font face les infrastructures essentielles du Canada.



Centre de la sécurité des
télécommunications Canada
Centre canadien
pour la cybersécurité

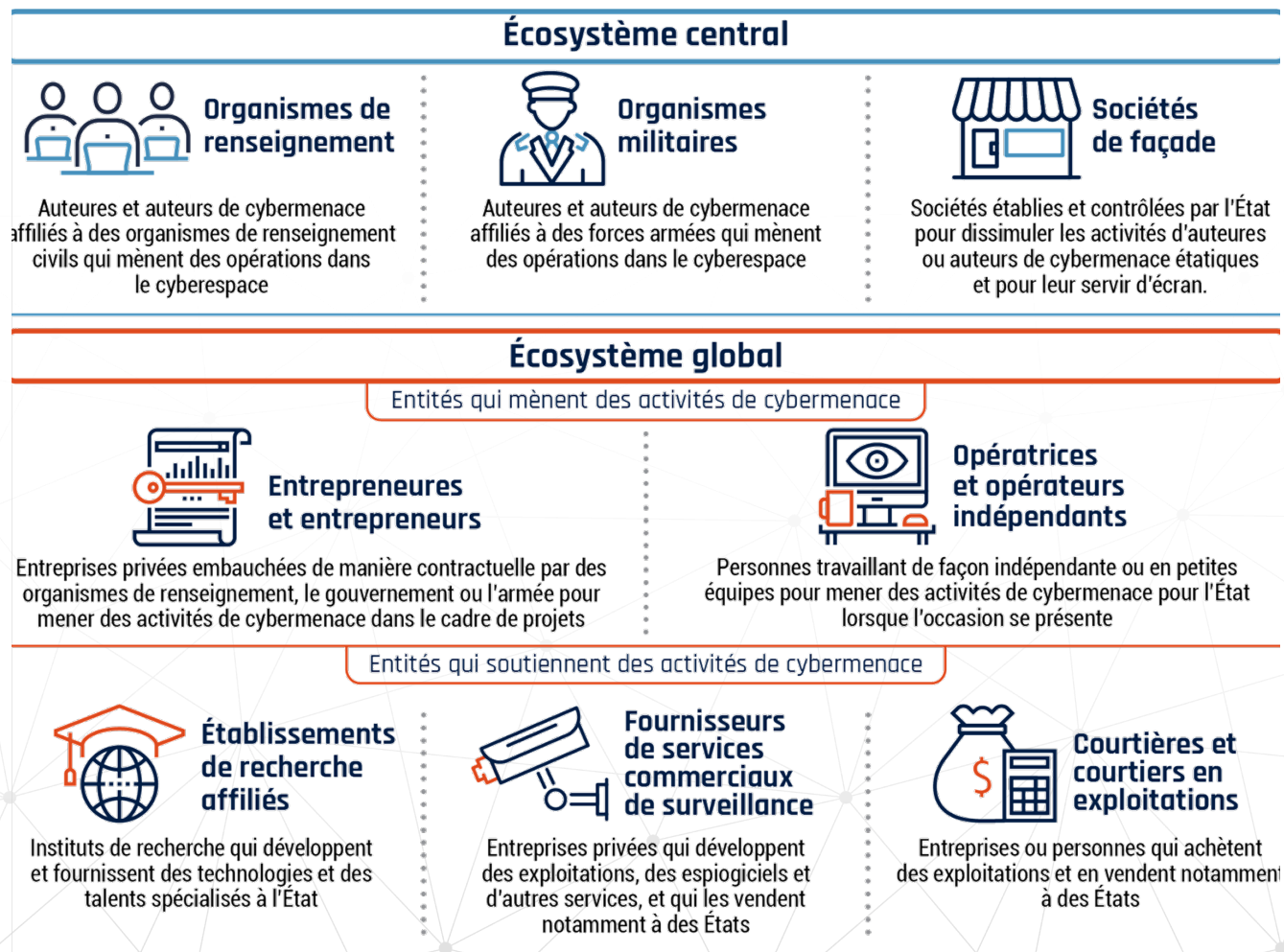
Communications Security
Establishment Canada
Canadian Centre
for Cyber Security

Canada

Cybermenace provenant d'États adversaires

« Les États avancés et émergents tirent parti d'un écosystème complexe de fournisseurs de services commerciaux de surveillance, d'entrepreneurs et entrepreneurs et d'établissements de recherche affiliés pour soutenir ou exécuter des activités de cybermenace ».

Écosystème des programmes de cyberactivité étatiques



RPC: Volt Typhoon et Salt Typhoon

○ Volt Typhoon

- Utilise les techniques d'exploitation des ressources locales (LOTL)
- Persiste et se pré-positionne
- A compromis des infrastructures essentielles américaines

○ Salt Typhoon

- Cible les appareils de périphérie
- A compromis plusieurs fournisseurs de services de télécommunications américains
- **A vraisemblablement compromis des dispositifs réseau canadiens**



Exemples notables d'activités de cybermenace non étatiques pro-Russie

Février 2023

Des groupes d'auteurs et auteurs de cybermenace non étatiques pro-Russie participent à une campagne visant à saboter les infrastructures essentielles de pays qui prêtent assistance à l'Ukraine, y compris le Canada.

Avril 2023

Un groupe d'auteurs et auteurs de cybermenace non étatique pro-Russie revendique une campagne par DDoS contre des sites Web canadiens, notamment le site Web public du Cabinet du Premier ministre.

Septembre 2023

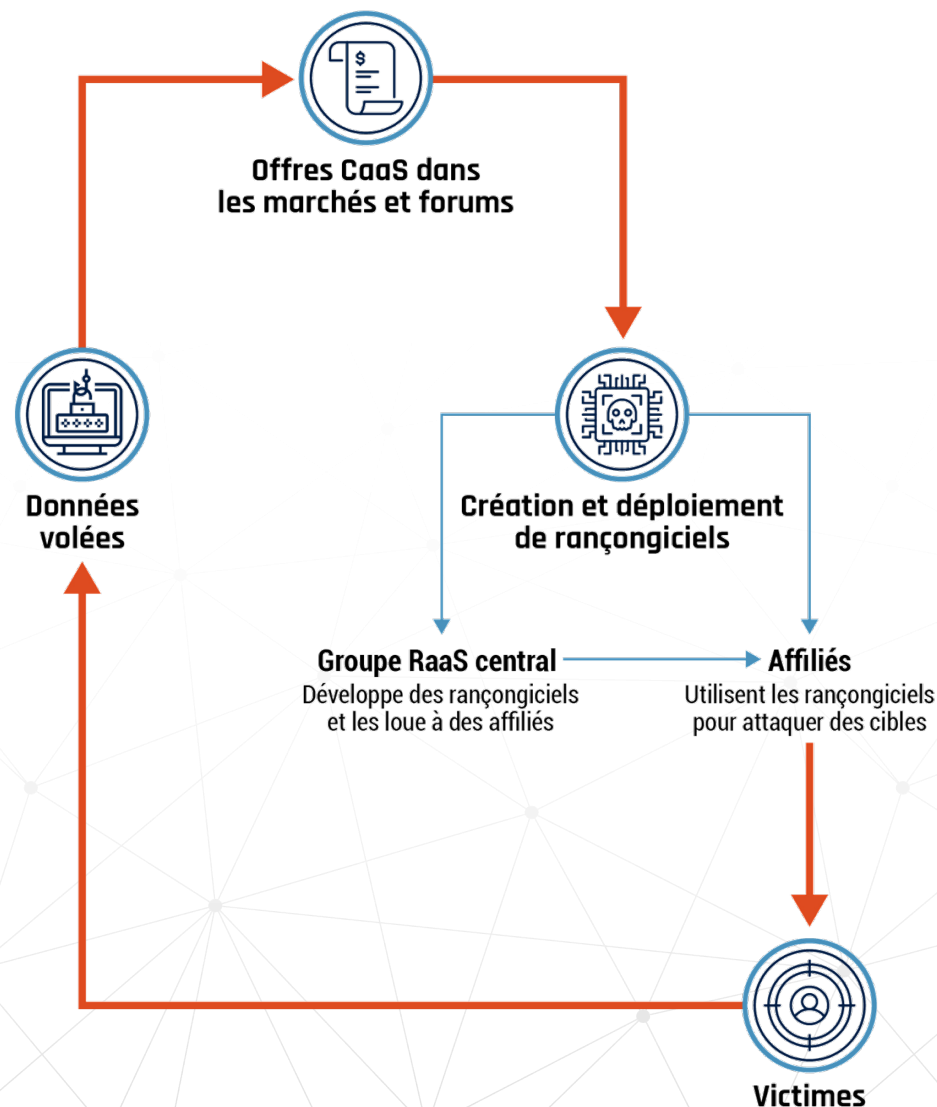
Un groupe d'auteurs et auteurs de cybermenace non étatique pro-Russie revendique une campagne par DDoS contre des sites Web canadiens, notamment des sites Web du gouvernement provincial du Québec.



Cybercriminalité

« L'écosystème de *Ransomware-as-a-Service* fait partie de l'écosystème plus vaste de *Cybercrime-as-a-Service*. Il est alimenté par une chaîne d'approvisionnement complexe composée de divers intervenants qui offrent différents services de CaaS pouvant servir à mener des attaques par rançongiciel. Cela comprend les services de soutien qui sont à la base du fonctionnement de l'écosystème. »

Écosystème du rançongiciel comme service (RaaS)



Services de soutien

Infrastructure d'hébergement

Les auteurs et auteurs de menace louent une infrastructure d'hébergement Internet capable d'offrir une protection raisonnable contre les forces de l'ordre.

Services financiers

Les auteurs et auteurs de menace utilisent des cryptomonnaies pseudo-anonymes pour faire l'achat d'outils de rançongiciel et de divers services illicites de blanchiment de fonds recueillis dans le cadre d'opérations.

Communications

Les auteurs et auteurs de menace emploient différentes plateformes pour communiquer de façon anonyme entre eux et avec leurs victimes pour négocier des demandes de rançon.



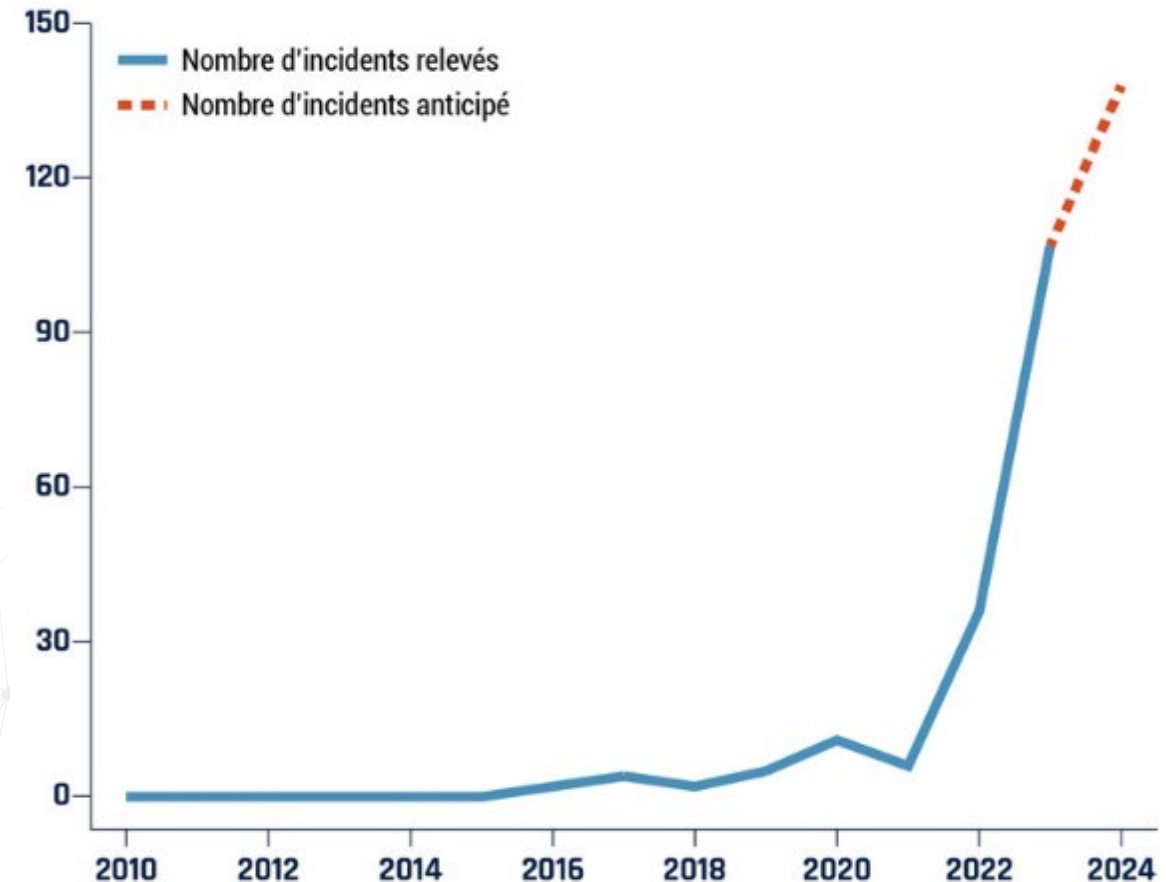
Cybermenaces et intelligence artificielle

Les technologies d'intelligence artificielle amplifient les menaces dans le cyberspace.

- L'IA améliore la personnalisation et le pouvoir de persuasion des attaques par piratage psychologique
- Les technologies d'IA augmentent la qualité et l'ampleur des campagnes d'influence étrangères en ligne
- L'IA prédictive améliore les capacités d'analyse des mégadonnées

Source: NCTA 2025-26

Incidents liés à l'IA générative à l'échelle mondiale ayant été signalés publiquement et ayant causé un préjudice ou quasi-préjudice



Événements notables - secteur de l'énergie

2026 à aujourd'hui

Le centre canadien pour la cybersécurité documente en 2026 un incident de rançongiciel dans le secteur de l'énergie et plusieurs expositions TO/SCI.

INCIDENT RAPPORTÉ

2026 • Rançongiciel - entité canadienne du secteur de l'énergie

Fuite de renseignements personnels et bancaires de nombreux clients actuels et anciens. L'entité n'a pas payé la rançon; elle a activé son intervention, évalué les impacts et reconstruit/rétabli les systèmes touchés.

[1]

ALERTE SCI / ÉNERGIE

2 mars 2026 • Recharge de véhicules électriques et contrôles industriels

Le centre canadien pour la cybersécurité relaie plusieurs avis de la CISA concernant notamment; EV Energy, SWITCH EV, Chargemap, CloudCharge, Frick Controls Quantum HD et Yokogawa CENTUM VP. Il s'agit de vulnérabilités à corriger. Il n'y a pas d'attaques confirmées.

[2]

ALERTE SCI / ÉNERGIE

7 avril 2026 • Hitachi Energy et systèmes industriels

Avis concernant notamment Hitachi Energy Ellipse ainsi que des composants Siemens et Yokogawa. Le CCC recommande l'application des mesures d'atténuation et mises à jour disponibles.

[3]

ALERTE SCI / ÉNERGIE

8 juin 2026 • Hitachi Energy – environnement OT

Avis touchant Hitachi Energy ITT600 Explorer, MACH HiDraw et RTU500. Ces produits sont associés à des environnements industriels/énergétiques; pour l'instant aucune compromission n'est affirmée par le CCC dans le cadre de cet avis.

[4]

ALERTE SCI / ÉNERGIE

13 juillet 2026 • Hydro-Québec / Hitachi Energy / Schneider Electric

Avis visant notamment le système de gestion des bornes de recharge du Circuit électrique d'Hydro-Québec, Hitachi Energy e-mesh EMS et PROMOD V, ainsi que Schneider Electric Easergy MiCOM Px40.

[5]



Centre de la sécurité des
télécommunications Canada
Centre canadien
pour la cybersécurité

Communications Security
Establishment Canada
Canadian Centre
for Cyber Security

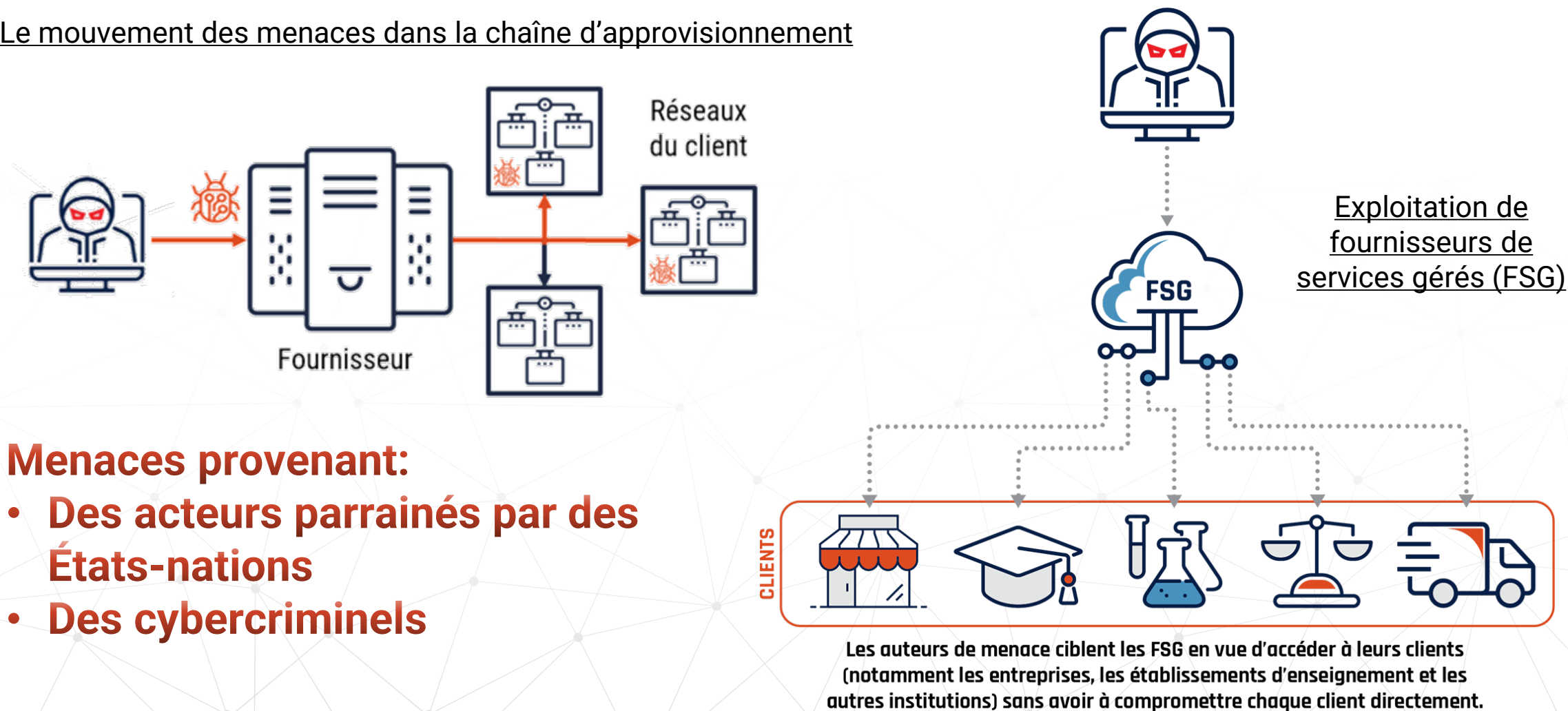
Canada

Où les menaces peuvent-elles s'introduire?



État de la menace à l'intégrité de la chaîne d'approvisionnement

Le mouvement des menaces dans la chaîne d'approvisionnement



Étude de cas: Jaguar Land Rover



DATA BREACHES

Jaguar Land Rover Admits Data Breach Caused by Recent Cyberattack

Jaguar Land Rover admet à une fuite de données suite à la plus récente cyberattaque



GOVERNMENT

Cyberattack on JLR Prompts £1.5 Billion UK Government Intervention

Une cyberattaque contre JLR entraîne une intervention gouvernementale britannique de 1,5 milliard.

Bulletin de cybersécurité conjoint: Scattered Spider est un groupe cybercriminel qui cible de grandes organisations et les services d'assistance des technologies de l'information qu'elles embauchent en sous-traitance. (Juillet 2025)

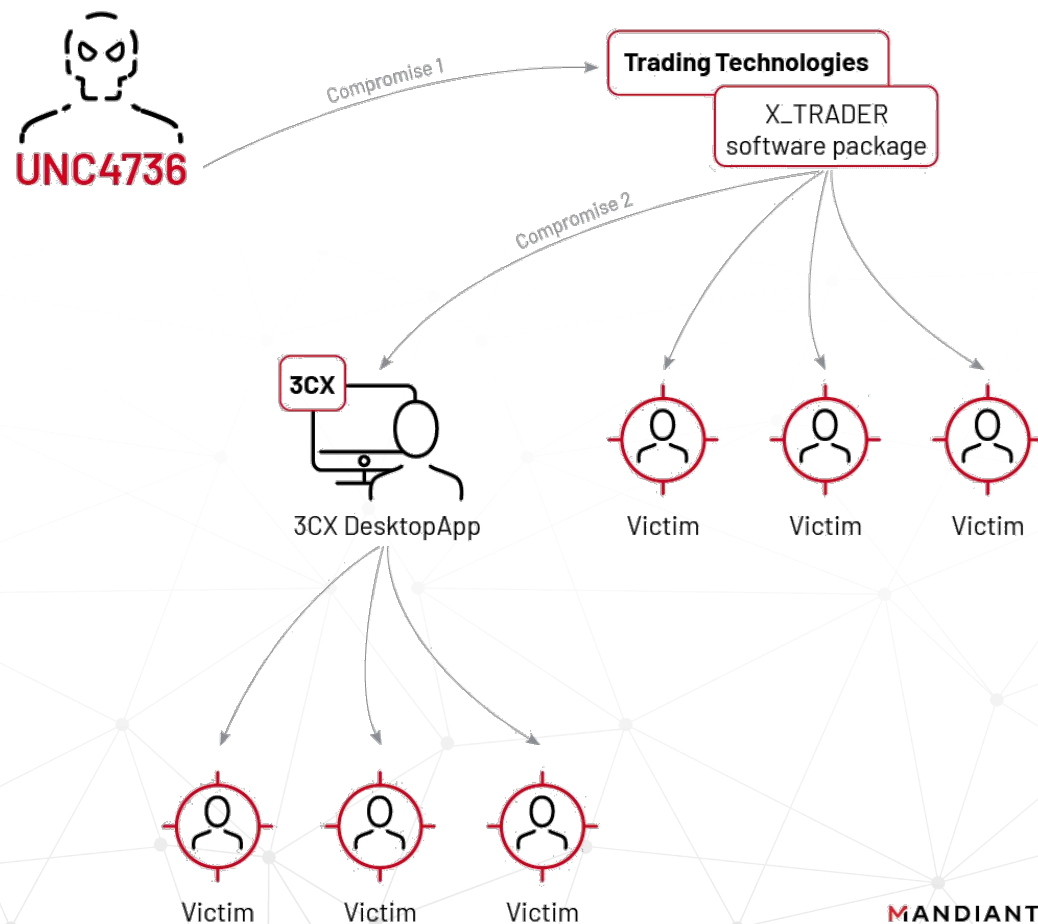


Centre de la sécurité des
télécommunications Canada
Centre canadien
pour la cybersécurité

Communications Security
Establishment Canada
Canadian Centre
for Cyber Security

Canada

Étude de cas: 3CX Desktop App



Source: Mandiant. [3CX Software Supply Chain Compromise Initiated by a Prior Software Supply Chain Compromise; Suspected North Korean Actor Responsible](#). Avril 2023.

- **3CX Desktop App**: logiciel d'entreprise fournissant une plateforme pour **le clavardage, les appels vidéo et les appels vocaux**.
- **Trading Technologies**: Fournisseur de plateforme technologique **SaaS** pour l'industrie mondiale des **marchés de capitaux**.
- Pas une, mais bien **deux compromissions** de l'intégrité de la chaîne d'approvisionnement.
- Attaquants soupçonnés: **UNC4736, un groupe nord-coréen**.
 - Le groupe avait **introduit un logiciel malveillant dans l'installateur pour X Trader**, un logiciel fourni par Trading Technologies.
- Résultat? **Exfiltration de données du navigateur** (historique de navigation, incluant titres et URLs).



Services du Centre pour la cybersécurité



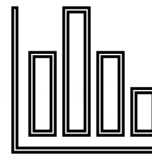
Alertes



CyberFlash



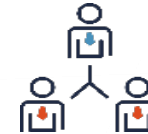
Notifications du
système NCTNS



Bulletin
CyberPosture



AVENTAIL



Comptes-rendus
sur les menaces



Howler



Note d'information



Rapport technique
hebdomadaire



Malware



BeAVER



Passons à l'action



L'Outil canadien de
cybersécurité
(OCC)



GeekWeek



Communiquez avec nous

 montreal@cyber.gc.ca

Pour signaler une fraude :

Centre antifraude du Canada

1 888 495-8501

www.antifraudcentre-centreantifraude.ca

Pour signaler un cybercrime :

Service de police local ou

Gendarmerie royale du Canada

www.rcmp-grc.gc.ca

Pour signaler un cyberincident :

Centre canadien pour la cybersécurité

Portail signalement d'un cyber incident



Centre de la sécurité des
télécommunications Canada

Centre canadien
pour la cybersécurité

Communications Security
Establishment Canada

Canadian Centre
for Cyber Security

Canada



Building a Defensible Cyber and Physical Security Program

Senior CIP Compliance Analyst
Jonathan Espinosa

2026 Régie Annual Reliability Seminar | October 6, 2026

Public



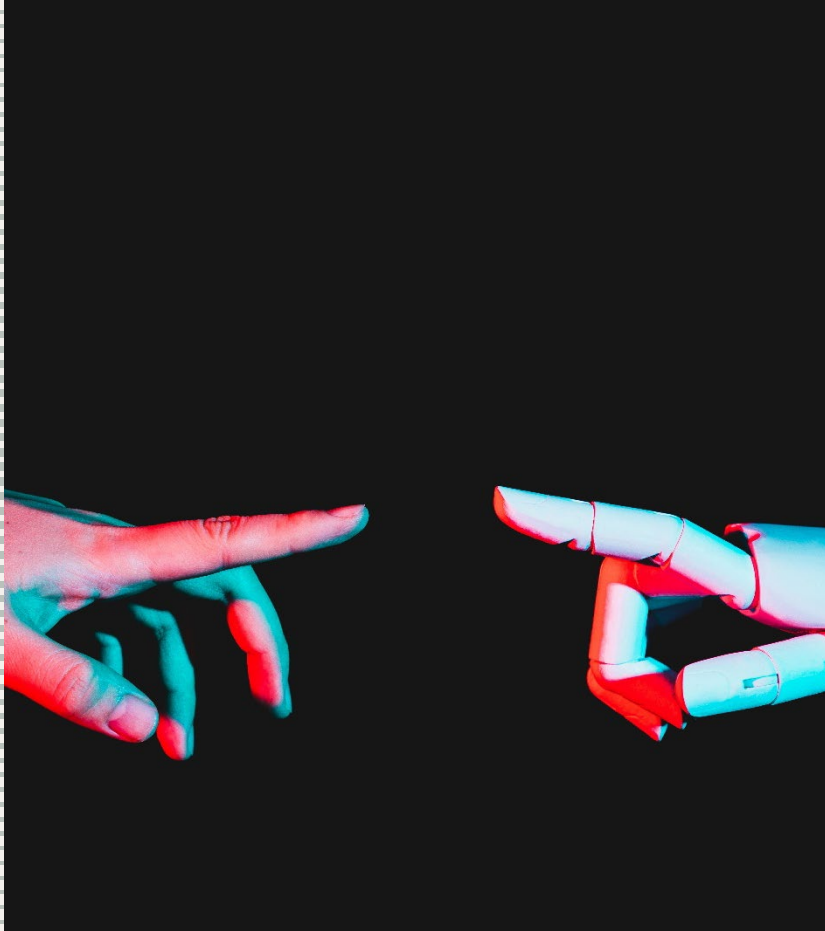
Agenda

- The Dynamic Threat Landscape
- Compliance Requirements
- Defense in Depth
- Key Takeaways & Close





The Dynamic Threat Landscape



AI is Compressing the Attack Timeline

- Agentic AI can be tasked to perform reconnaissance.
- Automated exploit generation lowers the time needed for the weaponization of disclosed Common Vulnerabilities and Exposures (CVEs).
- AI-scaled social engineering – deep fake voice/video, convincing phishing messages.



Physical Security is not a Secondary Concern

In 2025 there were 3500 physical security incidents reported to the E-ISAC of which 3% resulted in operational disruptions.

Historical Examples:

- Moore County, NC – December 3rd, 2022
 - Gunfire on two distribution substations.
 - Estimated 45,000 customers without power.
- Tacoma / Pierce County, WA – December 25th, 2022

Supply Chain Risk: IBR's

Québec's Plan de gestion intégrée des ressources énergétiques (PGIRE) targets up to 25 GW of wind and 5GW of solar to meet future electricity demand. As inverter-based resource (IBR) deployment grows, so does exposure to supply-chain risks associated with foreign made components.

- In May 2025, Reuters reported Chinese-made solar inverters and batteries contained undocumented communication devices, not listed in product specifications.
- Hidden channels could allow remote actors to bypass controls.





Compliance Requirements

Relevant CIP Requirements

CIP Requirement	What the requirement establishes
CIP-003-9 R2, Attachment 1, Section 1, 2, 6*	Reinforce cyber-security practices at least once every 15 calendar months, control physical access based on need, and address vendor electronic remote-access.
CIP-007-6 R3	Deploy method(s) to deter, detect, or prevent malicious code.
CIP-013-2	Address vendor practices, procurement, software integrity, notifications, and remote access.
CIP-014-3	Address potential threats and vulnerabilities and security plans for applicable RTP Assets.
CIP-015-1*	Establish processes to detect and evaluate anomalous network activity.

* Subject to future enforcement



A wide-angle, nighttime photograph of the New York City skyline. The Manhattan skyline is visible in the background, with numerous skyscrapers illuminated with various colors of lights. The Brooklyn Bridge spans the foreground, its structure and lights reflected in the water below. The water is dark, and the reflections of the city lights create a vibrant, colorful pattern on its surface.

Defense in Depth

What is Defense in Depth?

- Defense in depth means no single control is trusted to stop a threat on its own.
- Multiple, overlapping layers used to protect.
 - Deter
 - Detect
 - Delay
 - Respond



Defense in Depth

Physical Security Example – Substation



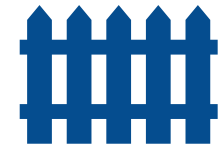
Deter

Perimeter security lighting, signage, visible cameras.



Detect

Intrusion detection, fence sensors, thermal cameras, gunshot detection.



Delay

Anti-climb / anti-cut perimeter fencing, vehicle barriers, hardened enclosures around critical equipment.

Defense in Depth Pt. 2

Cyber Security Controls



Reconnaissance

Detection of Active Scanning



Initial Access

Application Isolation and Sandboxing



Execution/Impact

Antivirus/Antimalware



Persistence

Privileged Account Management



Exfiltration

Network Intrusion Prevention





Bringing it Together

A Defensible Program, End to End

A defensible program connects current threats, applicable requirements, and layers protections.



Key Takeaways

- The threat landscape should inform how CIP requirements are implemented.
- Layered defenses mapped to multiple tactics and techniques alert on what single-point controls might miss.
- A defensible program can clearly explain, the threats being addressed, the applicable CIP requirement, and if any additional controls are necessary to address the threat landscape.



Questions?

Contact Us: npcc.org/contact

Building a Defensible Cyber and Physical Security Program | Public

2026 Régie Annual Reliability Seminar | October 6, 2026

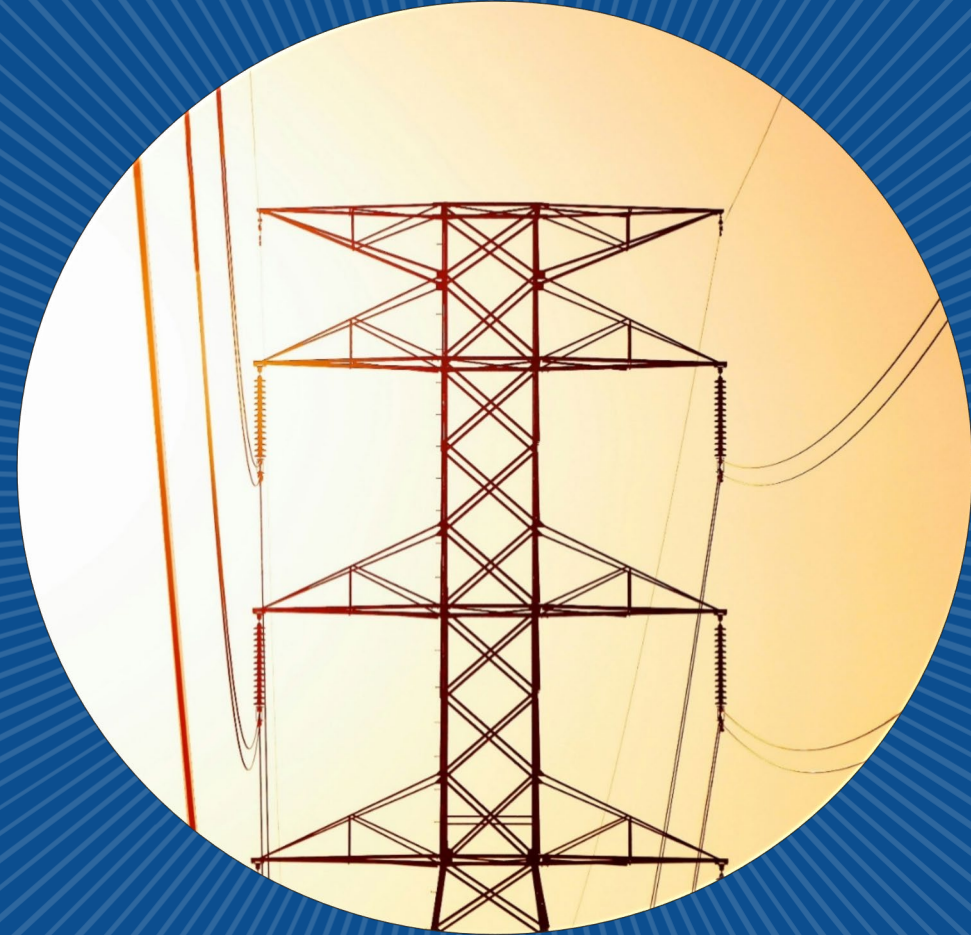


Bridging the Gap: Addressing Reliability Risk Management

Joshua Trichon, Enforcement Attorney

2026 Régie Annual Reliability Seminar | October 6, 2026

Public



Agenda

- Background and the Regulatory Gap
- Cloud Computing Example
- Implications of the Interim Period
- Recommended Risk-Based Approach



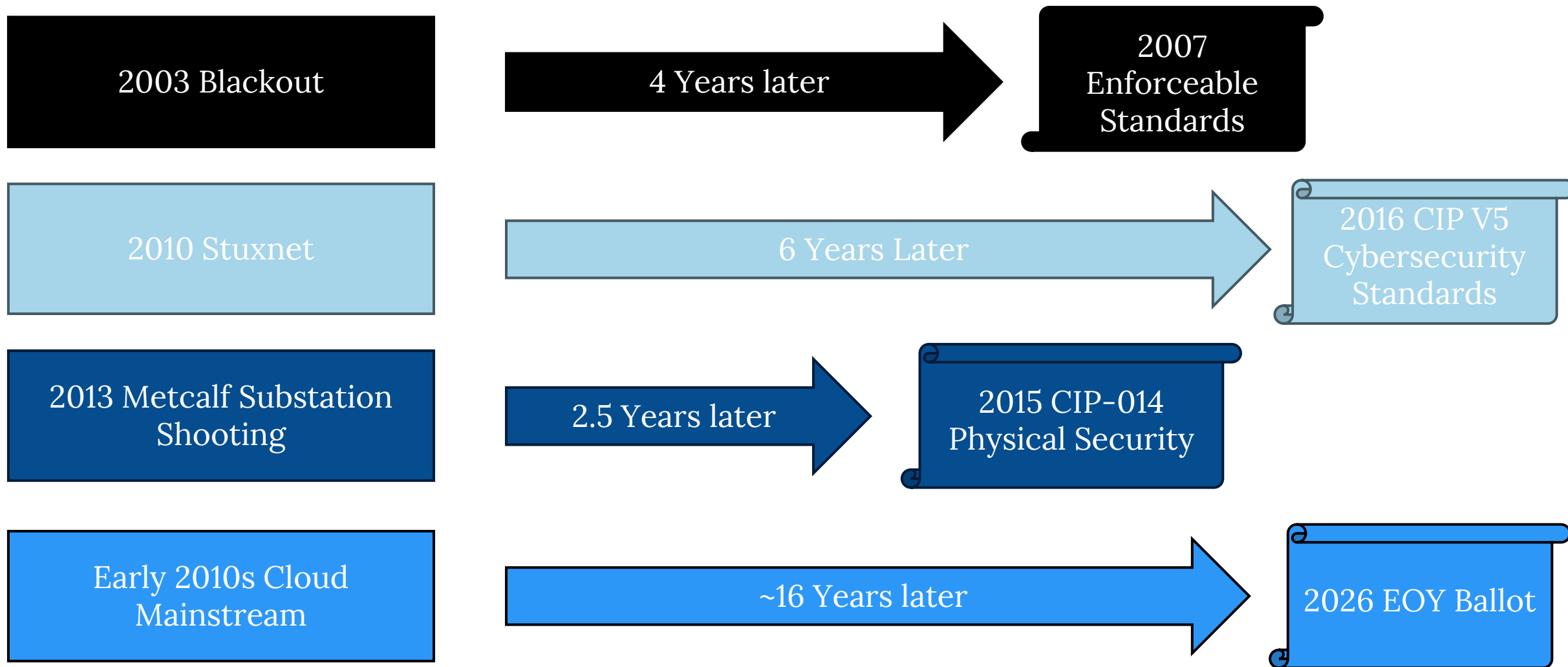
Background



- **Acknowledging the Technology-Regulatory Gap**
 - Technological changes evolve rapidly and tend to outpace development of regulatory standards, resulting in a regulatory gap.
- **Modern Cyber Threat Landscape**
 - Increasingly sophisticated cyber threats exploit vulnerabilities in cloud and third-party infrastructure.
- **Risk-Based Interim Actions**
 - During standards transition periods, NPCC recommends proactive, risk-based measures that emphasize reliability and security beyond compliance.
 - Continuous monitoring and clear communication ensures that issues are actively addressed, despite slow formal standards development.
- **Transparency, Ongoing Monitoring, and Risk Management**
 - Acknowledging the regulatory gap underscores the need for supplemental risk management and modernization efforts.
- **Complexity in Compliance**
 - Systems may be secure but not fully aligned with existing standards, or compliant yet exposed to new risks.



Identified Risk vs Regulation Pace Examples





Reliability Risk Standard Gap Example: Cloud Computing

Expansion of Cloud and Third-Party Infrastructure

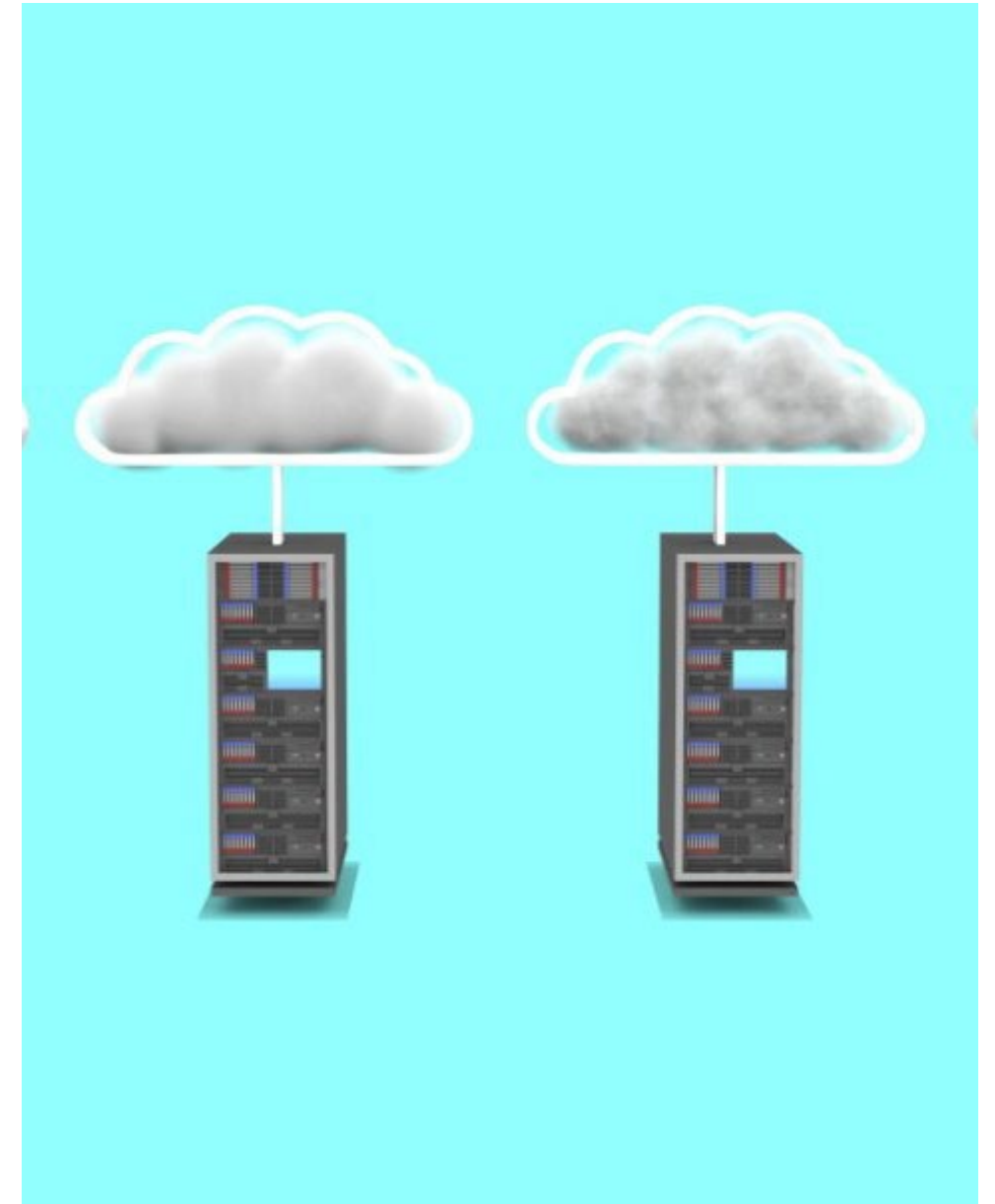


- **Shift to Cloud-Based Solutions**
 - Utilities and vendors increasingly adopt cloud solutions for scalability and resiliency, moving away from on-premises, local products.
- **Challenges with CIP Framework**
 - Existing CIP standards do not fully address cloud-based architectures, complicating compliance and security practices.
- **Shared Responsibility Model**
 - Cloud environments rely on shared responsibility between customers and providers, impacting asset control and access management.
- **Need for Updated Standards**
 - Modern architectures require updated standards to ensure security and reliability without compromising innovation.



Existing Standards and Standard Development

- Physical Security Assumptions
 - CIP-006 assumes direct control over physical facilities, which is limited in cloud environments managed by service providers.
- Static Network Perimeter Challenges
 - CIP-005 depends on static electronic security perimeters, but cloud networks are dynamic and software-defined, complicating perimeter enforcement.
- Compliance and Audit Implications
 - Structural mismatches create compliance and audit challenges in cloud environments without implying reduced security levels.
- Risk Management for Third-Party Cloud Services
 - Project 2023-09. Working on establishing risk-based, outcome-driven, updated standards that allow cloud services for CIP systems while ensuring reliability and security.





Implications of the Interim Period

Technology and Threats Continue to Advance

A rapidly changing threat landscape combined with slower standards development creates an interim period where compliance alone may not fully address risk.



Interim Regulatory Challenges

The gap between emerging technology adoption and new standards creates complex operational challenges for organizations.



Advancing Cloud Technologies

Cloud technologies continue to evolve rapidly, supporting critical operations across various industries and offering improved, scalable protections.



Increasing Cyber Threats

Cyber threat actors grow more capable and faster at exploiting vulnerabilities.



Need for Dynamic Governance

Effective governance is essential to manage risks as threats tend to evolve faster than reliability standard updates.

A nighttime photograph of the New York City skyline, featuring the Manhattan Bridge in the foreground and the illuminated skyscrapers of Lower Manhattan in the background, with their lights reflecting on the water.

Recommended Risk-Based Approach

Going Beyond Minimum Compliance

NPCC recommends a proactive, risk-based approach that goes beyond minimum compliance by accelerating patching, strengthening monitoring, and prioritizing security outcomes.

Proactive Risk-Based Approach

- Encourage a proactive approach prioritizing security outcomes and resilience beyond minimum compliance.

Accelerated Patch Management

- Speed up patch review and installation especially for high-risk vulnerabilities that may be exploited.

Enhanced Monitoring and Detection

- Strengthen internal monitoring to detect anomalous behavior indicating potential exploitation of vulnerabilities.

Focus on Risk Reduction

- Shift focus from checklist compliance to reducing risk and adapting to evolving cyber threats effectively.



Enhanced Monitoring, Governance, and Framework Alignment

Additional risk mitigation for cloud-based infrastructure includes early adoption of enhanced monitoring practices, strong cloud governance, use of cybersecurity industry frameworks, and active industry engagement to stay aligned with evolving standards.



Early Adoption of Security Standards

Adopting upcoming standards enhances detection where rapid patching is challenging.



Governance and Risk Controls

Strict governance and risk controls ensure accountability in cloud-based infrastructure use.



Use of Industry Frameworks

Cybersecurity industry frameworks supplement CIP requirements with modern best practices.



Industry Group Engagement

Active participation in organizations like NPCC keeps entities updated and influential in standards development.

Conclusion and Ongoing Engagement

NPCC acknowledges the timing gap between technology and standards is an industry-wide concern and is addressing it by promoting proactive risk management while actively monitoring and supporting ongoing standards development.

Industry-Wide Timing Gap

- There is a critical gap between adopting new technology and updating relevant regulatory standards industry-wide.

Modernizing CIP Framework

- NERC is working on modernizing the CIP framework, but implementation will take several years.

Risk Management Focus

- NPCC encourages proactive risk management through operational controls, informed judgment, and cybersecurity best practices.

Ongoing Monitoring and Engagement

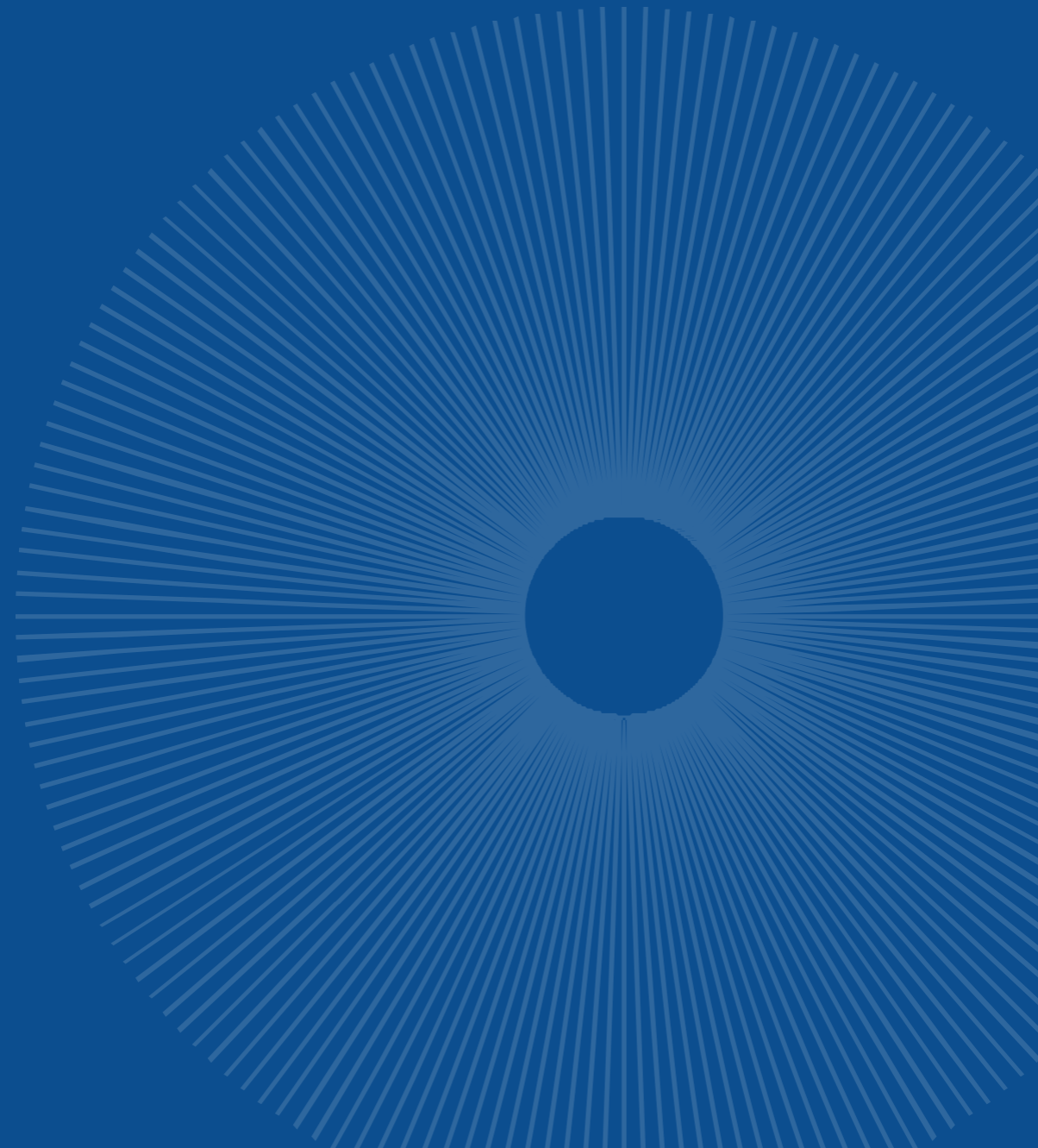
- NPCC will continue monitoring standards, engaging stakeholders, and providing expert briefings as needed.



Questions?

Bridging the Gap: Addressing Reliability Risk Management | Public

2026 Régie Annual Reliability Seminar | October 6, 2026





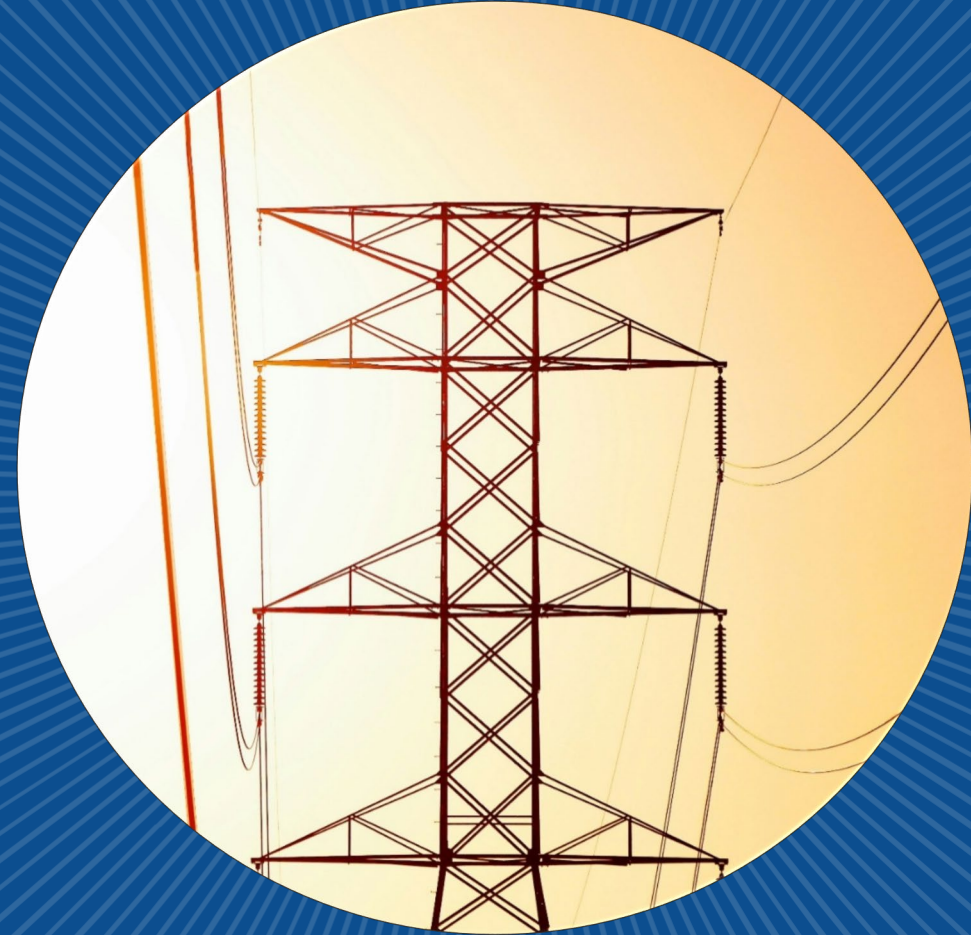
Inherent Risk Assessment and Compliance Oversight Plans

How Risk Informs Monitoring

NPCC – Registration, Certification and Risk
Tracy MacNicoll

2026 Régie Annual Reliability Seminar | October 6, 2026

Public



Agenda

- Overview of Risk-Based Compliance Monitoring
- Inherent Risk Assessments and Compliance Oversight Plans
 - Risk Questionnaires
 - Inherent Risk Assessment Process
 - Compliance Oversight Plan Process
 - Compliance Monitoring





Overview of Risk-Based Compliance Monitoring

- “The ERO Enterprise Risk-based Compliance Monitoring Framework (Framework) focuses on identifying, prioritizing, and addressing risks to the bulk power system (BPS), which enables each Compliance Enforcement Authority (CEA) to focus resources where they are most needed and likely to be the most effective.”
- Inherent Risk Assessments (IRA) and Compliance Oversight plans (COP) are tools we use to perform Risk-based Compliance Monitoring

Source: [ERO Enterprise Guide for Compliance Monitoring](#)





Inherent Risk Assessments and Compliance Oversight Plans

2026 Régie Annual Reliability Seminar | October
6, 2026

IRA and COP Process



- Risk Questionnaire
- Inherent Risk Assessment
- Compliance Oversight Plan
- Compliance Monitoring

IRA and COP Process



IRA and COP Process



Risk Questionnaire

- Issued by NPCC
- Completed by Registered Entity
- Questions based on functional registration



IRA and COP Process



Inherent Risk Assessment

- Responses from Risk Questionnaire used to complete IRA
- Completed by NPCC
- 20 Risk Factors
 - CIP
 - Transmission
 - Generation
 - Load
 - Automatic Load Shedding
 - System Restoration
 - Remedial Action Scheme
 - Etc...

Source: [ERO Enterprise Risk Factors and Risk Categories](#)



Risk Factors

- Balancing Authority (BA) Coordination
- CIP – External Electronic Communication
- CIP – Impact Rating
- CIP – Monitor and Control Capability
- Critical Transmission
- Largest Generator Facility
- Load
- Generator Planned Facilities
- Transmission Planned Facilities
- RAS
- System Restoration
- Total Generation Capacity
- Transmission Portfolio
- UFLS Development and Coordination
- UFLS Equipment
- UVLS
- Variable Generation
- Generator Voltage Control
- Transmission Voltage Control
- Workforce Capability

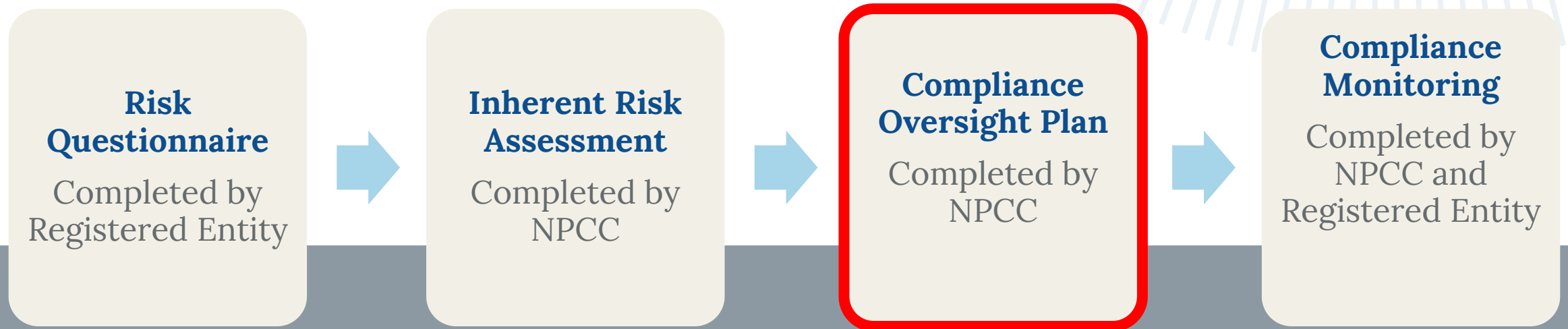


Inherent Risk Assessment

- Output:
 - Risk level assessment for each Risk Factor (N/A, Low, Medium, High)
 - Overall Inherent Risk Rating: (Lower, Moderate, Higher)



IRA and COP Process



Compliance Oversight Plan

- Inherent and Operational risks identified used to produce Compliance Oversight Plan
- Completed by NPCC
- [Report](#) Provided to Registered Entity
- Identifies Risk Categories

Source: [COP Report Template](#)



Risk Categories

- Asset/System Identification
- Asset/System Physical Protection
- Emergency Operations Planning
- Entity Coordination
- Identity Management and Access Control
- Long-term Studies/Assessments
- Modeling Data
- Normal System Operations
- Operating During Emergencies/Backup & Recovery
- Operational Studies/Assessments
- System Protection
- Training
- Inverter-Based Resources – BES
- Inverter-Based Resources – Non-BES



Risk Category Example

Risk Category	Description/Risk Failure	Related Standards
Asset/System Physical Protection	Failure to ensure the physical protection of BES assets could lead to access by unauthorized personnel. Such access might lead to actions that result in instability, uncontrolled separation or cascading within an Interconnection.	CIP-003 CIP-006 CIP-014



Compliance Oversight Plan Contents



Risk Categories

- [15 Risk Categories](#)
- 3-5 will be identified in Compliance Oversight Plan

Standards and Requirements

- Standards/Requirements associated with the identified Risk Categories
- Takes into account compliance history

Demonstrated Positive Performance

- Performance Considerations

Source: [ERO Enterprise Risk Factors and Risk Categories](#)



Compliance Oversight Plan Report

- Oversight Strategy:
 - Overall Inherent Risk
 - With or Without Demonstrated Positive Performance

Table 1.1 Oversight Strategy			
Category ³	Category Description	Target Monitoring Interval	Primary CMEP Tools
1	Represents an entity that has higher inherent risk without demonstrated positive performance considerations.	Every 1-3 years	Compliance Audit (on/off-site) Spot Check Self-Certification
2	Represents an entity that has higher inherent risk with demonstrated positive performance considerations.	Every 2-4 years	Compliance Audit (on/off-site) Spot Check Self-Certification
3	Represents an entity that has moderate inherent risk without demonstrated positive performance considerations.	Every 3-5 years	Compliance Audit (on/off-site) Spot Check Self-Certification
4	Represents an entity that has moderate inherent risk with demonstrated positive performance considerations.	Every 4–6 years	Compliance Audit (off-site) Spot Check Self-Certification
5	Represents an entity that has lower inherent risk without demonstrated positive performance considerations.	Every 5-7 years	Compliance Audit (off-site) Spot Check Self-Certification
6	Represents an entity that has lower inherent risk with demonstrated positive performance considerations.	Every 6+ years	Compliance Audit (off-site) Spot Check Self-Certification

Source: [COP Report Template](#)



Compliance Oversight Plan Report

- Summary of Risk Categories
- Appendix A: IRA Results Summary
- Appendix B: Standards and Requirements

Appendix A: IRA Results Summary

Appendix A identifies inherent risk by risk factors and assessment criteria of high, medium, or low based on predetermined criteria in the *ERO Enterprise Guide for Compliance Monitoring*. Included are RE justifications or explanations to support risk determinations.

Risk Factor Assessment		
Risk Factor	(High, Medium, Low, NA)	Explanation

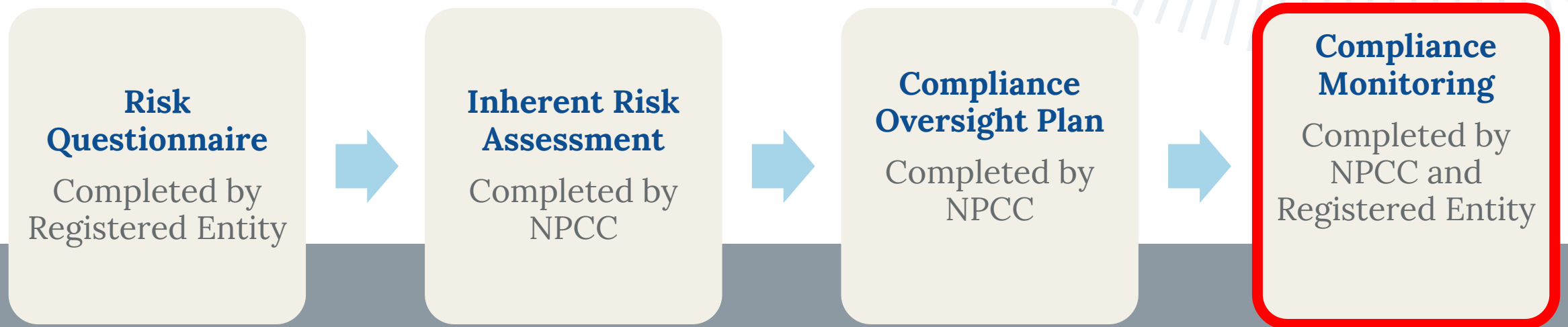
Appendix B: Standards and Requirements for Monitoring

Appendix B identifies the NERC Reliability Standards that may be associated with the risk outlined in Section 2 and considered as part of the oversight strategy. Note that a COP is dynamic and subject to change. CMEP Tools are used, as needed, by REs to evaluate compliance. They are implemented considering numerous factors including, but not limited to, the required notification periods within the NERC Rules of Procedure. Registered entities are required to be compliant with all applicable Standards and Requirements at all times.

Associated NERC Reliability Standards and Requirements for Monitoring	
Standard	Requirement

Source: [COP Report Template](#)

IRA and COP Process



Compliance Monitoring

- Results of COP help determine
 - Monitoring type
 - Monitoring interval
 - Scope of engagement





Questions?

Contact Us: npcc.org/contact

NPCC – Registration, Certification and Risk
Tracy MacNicoll



NERC & NPCC Compliance Resources

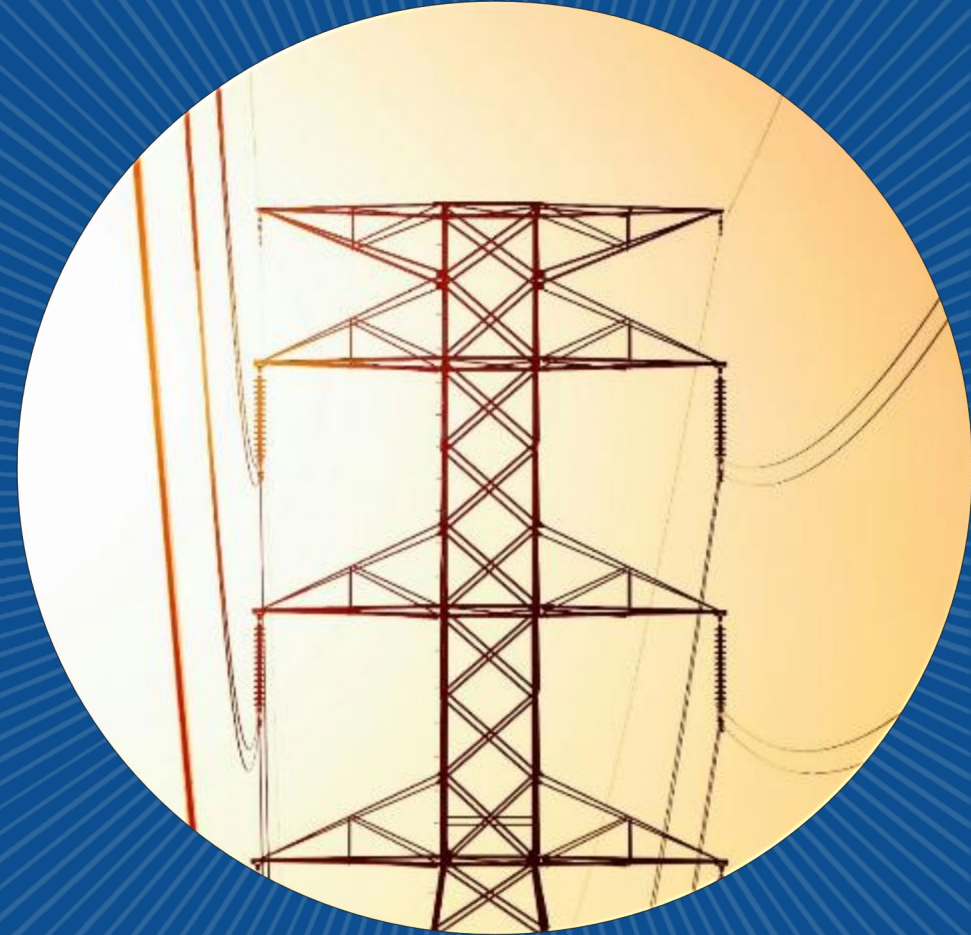
Supporting Effective and Sustainable Compliance Programs

NPCC-Compliance Program

Seema Thakur
Senior Compliance Engineer

2026 Régie Annual Reliability Seminar | October 6, 2026

Public



Outline

- Overview
- CMEP Practice Guides
- Implementation Guides
- QRSAs
- Self-Certification Worksheets
- Key Takeaways
- Questions



Overview

Compliance Resources to Support Effective Compliance Programs

CMEP Practice Guides

- Clarify CMEP Expectations

Implementation Guide (IG)

- Explain Compliance Approaches

NPCC Self-Certification Worksheets

- Demonstrate Auditors Approach to Evaluating Compliance

Quebec Reliability Standard Audit Worksheets (QRSAs)

- Demonstrate Compliance



CMEP Practice Guides

2026 Régie Annual Reliability Seminar | October 6, 2026

CMEP Practice Guides



Purpose

- Provide transparency into ERO Enterprise CMEP approaches
- Offer insight into how compliance staff evaluate risks, evidence, and program effectiveness
- Help entities understand audit focus areas, risk assessments, and evidence expectations
- Support stronger internal controls and risk-based compliance
- Complement Implementation Guidance



Content

- Reliability Standard Reference
- Purpose of guide creation
- Scope and Applicability
- Compliance Evaluation Considerations
- Examples of evidence
- Internal Controls Considerations
- Auditor Guidance on Observations and Evaluation Approaches



Key Benefits

- Consistency
- Transparency
- Audit Readiness
- Risk Reduction
- Operational Efficiency

List of CMEP Practice Guides

CMEP Practice Guides

Partial List

PRC-029-1 Enforcement Discretion

PRC 029 Enforcement Discretion Template

Inverter-Based Resources

Using the Work of Others

Modeling and Studies Involving DER

CIP-014-3 R1

CIP-002-5.1a R1 - Generation Segmentation

TOP-002-4, R6, R7 Determination of Provisions of Operating Plans

Evaluation of Facility Ratings and System Operating Limits

BES Cyber System Information

CMEP Practice Guide Calendar Month Annual

TOP-001-4 and IRO-002-5 Redundant and Diversely Routed

Phased Implementation Completion Percentages



Implementation Guidance (IG)

2026 Régie Annual Reliability Seminar | October 6, 2026

Implementation Guidance (IG)



Purpose

- Clarify Reliability Standards
- Understand regulatory intent
- Strengthen internal controls
- Offers examples, not mandatory methods



Content

- Reliability Standard Reference
- Compliance challenge, interpretation question, or implementation topic
- Methods to satisfy the requirement
- Factors in applying the guidance
- Risk-based considerations & operational differences
- Compliance documentation examples
- Technical Rationale for Reliability Standard objective



Key Benefits

- Consistency
- Audit Readiness
- Risk Reduction
- Operational Efficiency

List of Current Implementation Guides

ERO Enterprise
Implementation Guidance

Partial List

CIP-013 Using Independent Assessments of Vendors (NATF)

CIP-013 Supply Chain Risk Management Plans (NATF)

CIP-013-1 Supply Chain Risk Management Plans (NATF)

CIP-014-2, R5 Developing and Implementing Physical Security Plans (NATF)

CIP-002-5.1a R1 Shared Ownership of BES Facilities (CIPC)

CIP-014-2 R4 Evaluating Potential Physical Security Attack (NATF)

CIP-010-3 R1.6 Software Integrity and Authenticity (NATF)

CIP-004-6 R3 - NGOP Employee Access to TO Sites (CIPC)

CIP-013-1 Supply Chain Risk Management Plans (2016-03 SDT)

CIP-002-5.1 R1 Identify and Categorize BES Cyber Systems and Cyber Assets (MRO SC)

EOP-012-3 Requirement R1 – Determining Extreme Cold Weather Temperatures

TPL-001-5.1 Implementation Guidance

TPL-001-4 System Planning Performance Requirements (MRO SC)





Québec Reliability Standard Audit Worksheets (QRSAWs)

QRSAWs



Purpose

- Identify compliance narratives, responsibilities, processes and evidence
- Used for audits, spot checks, & internal assessments
- Maintain ongoing compliance



Content

- Requirement-by-requirement compliance narrative
- Evidence references
- Auditor guidance on what may demonstrate compliance
- Questions that help auditors evaluate compliance



Key Benefits

- Consistency
- Transparency
- Gap identification
- Knowledge retention
- Strong Compliance Culture
- Evidence Management
- Risk Reduction
- Operational Efficiency

Example: QRSAW PRC-005-6

Requirement R3



[Quebec Reliability Standard Audit Forms](#)



NPCC Self-Certification Worksheets

2026 Régie Annual Reliability Seminar | October 6, 2026

Self Certification Worksheets



Purpose

- Identify compliance narratives, responsibilities, processes, and evidence
- Use during **self-certifications** but can be used as a resource for entity's in evaluating their programs
- Provide reasonable assurance of compliance, targets specific system risks
- Allow regional entities to monitor bulk power system reliability without a full audit



Content

- Entity Information
- Standard and Requirement
- Processes, controls, and procedures used to meet the requirement
- Evidence Documentation
- Compliance Determination



Key Benefits

- Consistency
- Risk Reduction
- Early Gap Identification
- Supports internal controls

List of Available Self-Certification Worksheets

PRC-024-3

PRC-006-NPCC-2

PRC-005-6

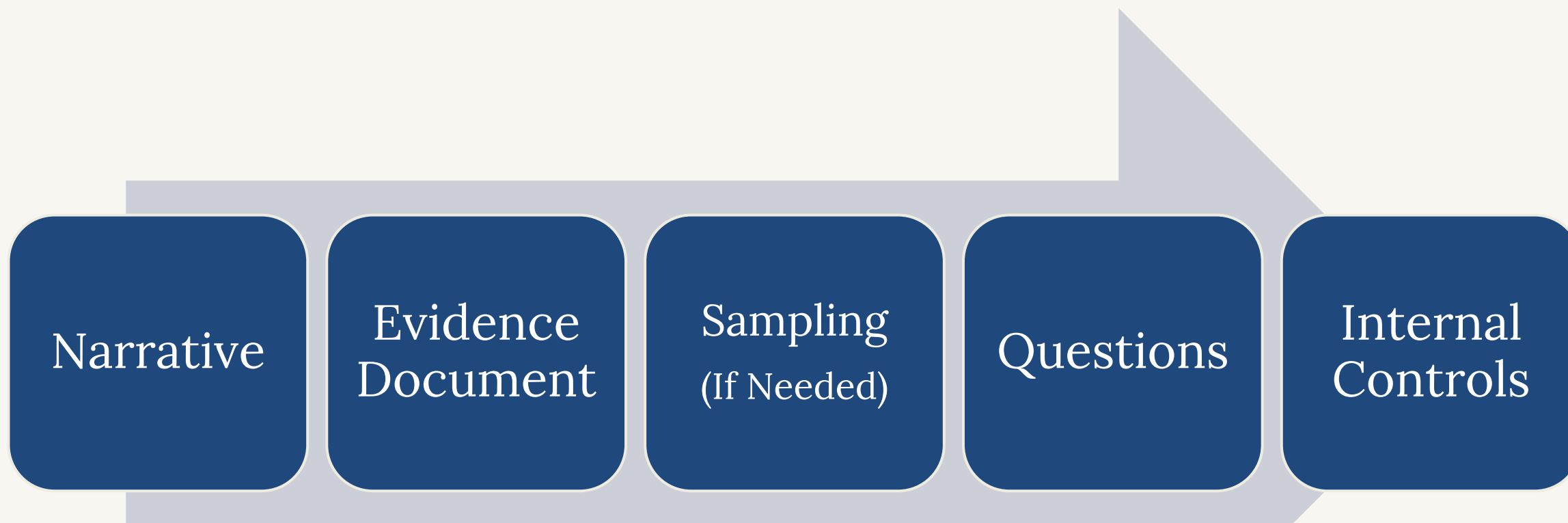
CIP-003-9 *Effective July 1, 2027

CIP-003-9

EOP-012-3



Example: Steps for PRC-005-6 R3 Self-Certification

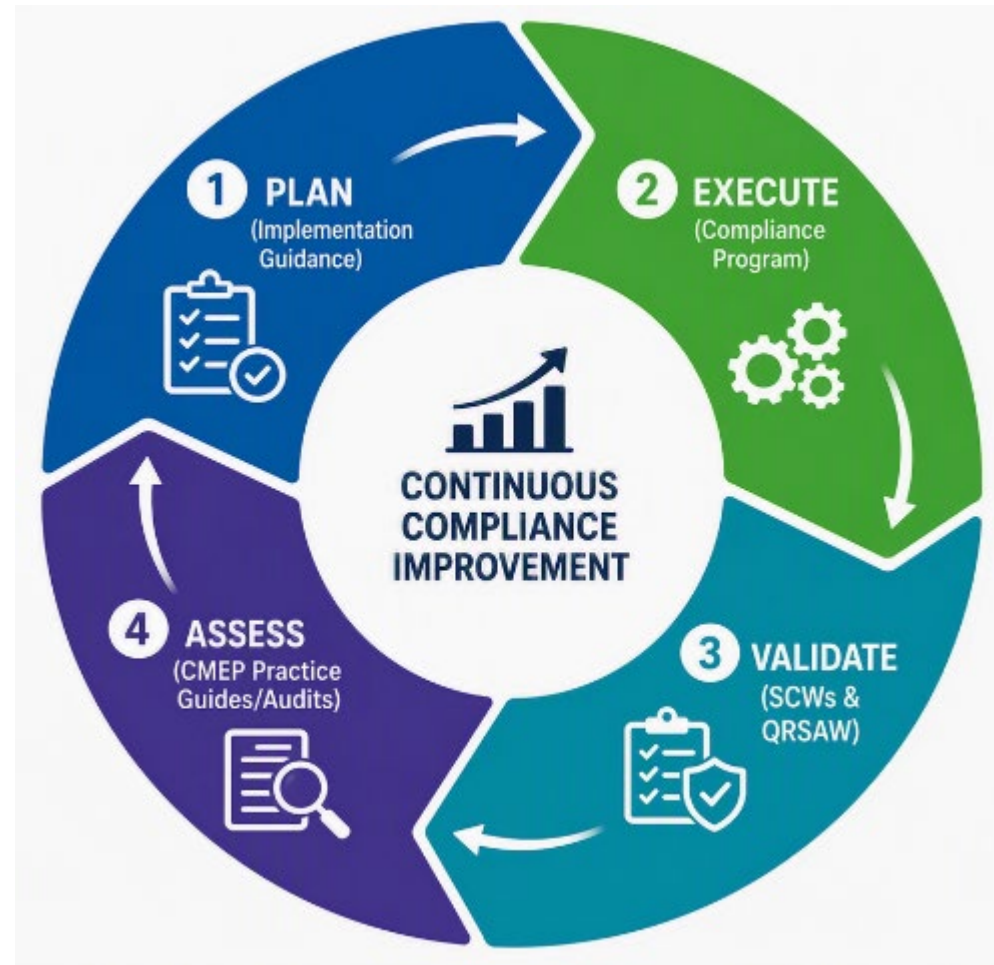


Comparison of Compliance Resources

Document	Key Question Answered	Typical Use	Key Output	Key Benefit
Implementation Guidance (IG)	"What does this requirement mean?"	Developing procedures and controls	Recommended implementation approaches	Consistency
Self-Certification	"Are we compliant?"	Self-assessment activities	Compliance determination	Compliance Verification
QRS AW	"How do we prove compliance?"	Audit preparation and evidence management	Evidence-to-requirement mapping	Audit Readiness
CMEP Practice Guides	"How will compliance be evaluated?"	Strengthening compliance programs	Improvement opportunities and best practices	Transparency



Key Takeaways





Questions?

Contact Us: npcc.org/contact

NPCC-Compliance Program
Seema Thakur



Quebec Reliability Standards Update

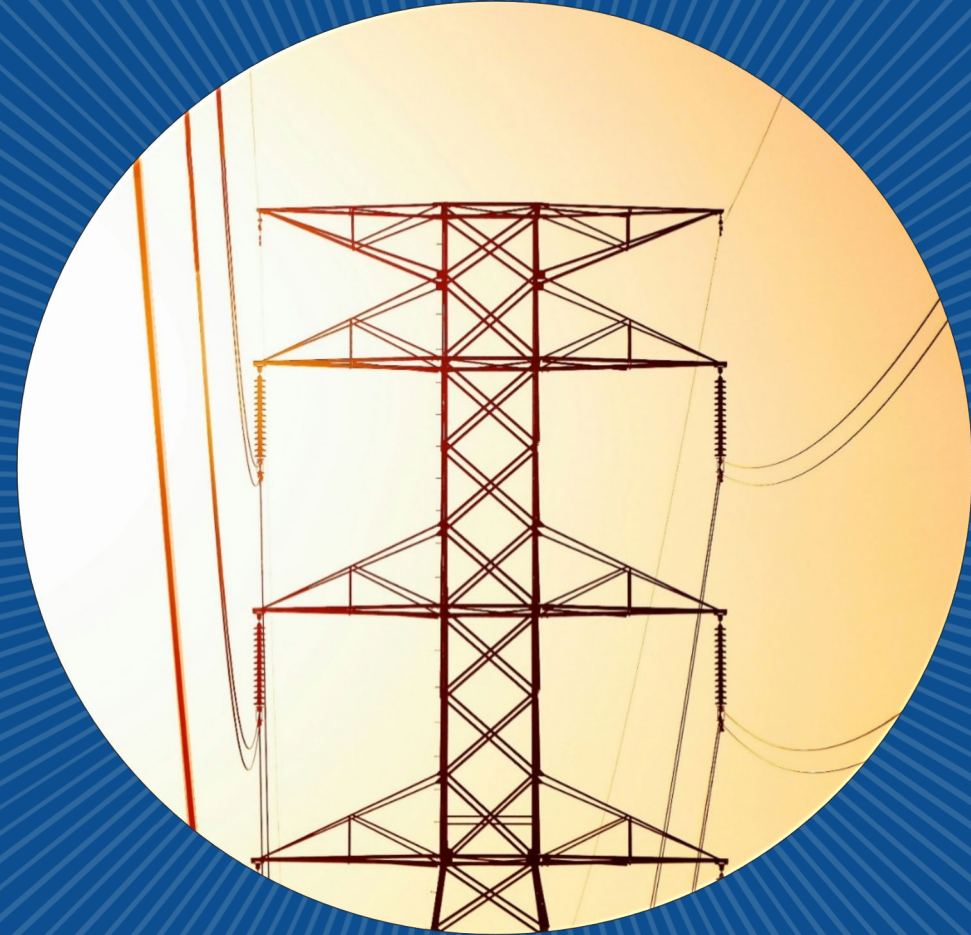
Key Changes for 2026 - 2027

NPCC Standards & Criteria

Patrick Davis
Senior Standards & Criteria Engineer

2026 Régie Annual Reliability Seminar | October 6, 2026

Public



Agenda

- Grid Operations and Operating Limits
- Protection and Control Systems
- Cybersecurity and Communications
- Reliability in the Evolving Resource Mix
- Effective Dates Summary
- Resources
- Discussion





Grid Operations and Operating Limits

FAC-003-5 | FAC-011-4 | FAC-014-3 | IRO-008-3 | TOP-001-6

FAC-003-5 Transmission Vegetation Management

Effective Date: October 1, 2026

Key Changes	Québec-Specific Modifications	Compliance Considerations	Implementation Impacts
<ul style="list-style-type: none">• Requirements consolidated into R1• Planner-based risk assessments• Vegetation management and transmission planning alignment	<ul style="list-style-type: none">• Extended inspections: up to 30 months• Six years of supporting data required• Revised R6 evaluation criteria	<ul style="list-style-type: none">• Robust qualification documentation• Inspections + risk analyses reviewed• PDS quarterly outage reporting	<ul style="list-style-type: none">• Fewer inspections for eligible facilities• More analysis and documentation needed• Assess program eligibility for extensions



FAC-011-4

System Operating Limits for the Operations Horizon

Effective Date: October 1, 2026

Key Changes	Québec-Specific Modifications	Compliance Considerations	Implementation Impacts
<ul style="list-style-type: none">• Requirements for SOL methodology development• Introduces System Voltage Limits• Expands stability limit and contingency analysis requirements• Implements a risk-based SOL exceedance communication framework	<ul style="list-style-type: none">• Temporary exemptions from certain three-phase fault evaluations• Applies to qualifying RTP facilities below 230 kV• Applies to certain industrial generation facilities not substantially modified after 2019	<ul style="list-style-type: none">• Identify facilities eligible for exemptions• Update SOL methodologies to reflect revised requirements• Retain supporting documentation for exemption eligibility	<ul style="list-style-type: none">• Reduced modeling burden for qualifying facilities• Additional methodology development and coordination effort• Track exemption sunset dates and facility modifications.



FAC-014-3 Establish and Communicate System Operating Limits

Effective Date: R1 – R5 October 1, 2026 | R6 – R8 Phased Implementation

Key Changes	Québec-Specific Modifications	Compliance Considerations	Implementation Impacts
<ul style="list-style-type: none">• Sets SOL & IROL responsibility• Stronger planning and operations coordination• Expands information sharing• Communication of instability risks	<ul style="list-style-type: none">• Direct adoption• Phased implementation:<ul style="list-style-type: none">• R1 – R5 on effective date• R6 next Planning Assessment• R7 & R8 one year later	<ul style="list-style-type: none">• Implementation timelines• Review communication and information sharing procedures• Align planning and operational criteria	<ul style="list-style-type: none">• Additional coordination• Expanded information sharing• Phased implementation reduces implementation burden

IRO-008-3 Reliability Coordinator Operational Analyses and Real-time Assessments

Effective Date: October 1, 2026

Direct Adoption



Key Changes

- Use of SOL methodology to identify exceedances
- Operational assessments aligned to FAC-011
- Updated SOL exceedance communication req's
- Notifications focused on impacted entities

Compliance Considerations

- Verify assessment processes align with RC methodology
- Update supporting documentation as needed
- Review notification procedures

Implementation Impacts

- Limited process changes for most entities
- Greater alignment to revised SOL framework
- Minor administrative and procedural updates

TOP-001-6 Transmission Operations

Effective Date: October 1, 2026

Key Changes	Québec-Specific Modifications	Compliance Considerations	Implementation Impacts
<ul style="list-style-type: none">• Requires TOPs to apply RC SOL methodologies• Aligns SOL exceedance communications with FAC-011• Clarifies expectations for mitigating SOL exceedances• Improves consistency between RC and TOP processes	<ul style="list-style-type: none">• Provides a unique interpretation of load-shed instructions• Compliance may be achieved through reduction of net transfers• Transfer reductions may include reducing transfers to zero	<ul style="list-style-type: none">• Review operating procedures for Québec-specific requirements• Ensure operators understand transfer-reduction expectations• Confirm SOL exceedance processes align with RC methodologies	<ul style="list-style-type: none">• Possible updates to operating procedures• Additional operator training requirements• Improved coordination with Reliability Coordinators





Protection and Control Systems

PRC-023-6 | PRC-026-2

PRC-023-6 Transmission Relay Loadability

Effective Date: October 1, 2026, with Requirement specific guidance

Key Changes	Québec-Specific Modifications	Compliance Considerations	Implementation Impacts
<ul style="list-style-type: none">• Consolidates R1 and R2• Stable power swing exclusion removed• Relay loadability and security objectives aligned• Eliminates redundant requirements	<ul style="list-style-type: none">• Transformer loadability – R1 Criteria 10 and 11• Relay settings based on Québec emergency transformer ratings• Overload protection	<ul style="list-style-type: none">• Review relay setting studies• Validate transformer loadability• Confirm implementation schedules for new facilities	<ul style="list-style-type: none">• Potential protection study and settings updates• Reassess transformer overload protection• PC's incorporate transition requirements



PRC-026-2 Relay Performance During Stable Power Swings

Effective Date: October 1, 2026, with specific implementation criteria

Key Changes	Québec-Specific Modifications	Compliance Considerations	Implementation Impacts
<ul style="list-style-type: none">• SOL framework alignment• Replaces legacy angular stability terminology with SOL-based concepts• Facility identification criteria updates• Maintains existing relay evaluation and corrective-action requirements.	<ul style="list-style-type: none">• No substantive technical changes from NERC requirements• Includes Québec-specific implementation and transition provisions• Establishes initial assessment timing requirements for Planning Coordinators	<ul style="list-style-type: none">• Confirm timing of initial assessments• Continue using existing relay evaluation methodologies• Verify applicability under revised SOL terminology	<ul style="list-style-type: none">• Minimal technical changes for most entities• Limited effort beyond transition planning• Existing programs can generally be retained



Cybersecurity and Communications

CIP-003-9 | CIP-012-2

CIP-003-9 Security Management Controls

Effective Date: July 1, 2027

Key Changes	Québec-Specific Modifications	Compliance Considerations	Implementation Impacts
<ul style="list-style-type: none">• Adds vendor remote-access controls for low-impact BES Cyber Systems• Requires processes to determine and disable vendor access when needed• Requires detection of known or suspected malicious vendor communications• Expands protection against supply-chain cybersecurity risks	<ul style="list-style-type: none">• Exempts:<ul style="list-style-type: none">• Certain generating facilities rated 300 MVA or less• Associated generator step-up substations• Applies where facilities cannot synchronize with neighboring systems	<ul style="list-style-type: none">• Determine qualification for Québec exemptions• Update cybersecurity policies and governance documents• Review vendor remote-access controls and monitoring capabilities	<ul style="list-style-type: none">• Additional oversight of vendor access activities• Potential technology or monitoring upgrades• Exempt facilities may avoid certain compliance obligations• Most entities can leverage existing NERC CIP programs



CIP-012-2 Communications Between Control Centers

Effective Date: April 1, 2027

Key Changes	Québec-Specific Modifications	Compliance Considerations	Implementation Impacts
<ul style="list-style-type: none">• Expands:<ul style="list-style-type: none">• Focus from confidentiality and integrity to include availability• Responsibility-sharing between entities• Requires:<ul style="list-style-type: none">• Mitigation methods for communication loss• Recovery plans for failed communication links	<ul style="list-style-type: none">• Uses a Québec-specific definition of Control Center• Applies to RC, BA, TOP, and certain GOP control center functions• Technical cybersecurity controls remain largely unchanged from NERC standard	<ul style="list-style-type: none">• Review applicability using the Québec Control Center definition• Validate communication inventories and dependencies• Document recovery and availability responsibilities	<ul style="list-style-type: none">• Limited operational changes for mature CIP programs• Possible updates to recovery and resilience procedures• Enhanced documentation of communication responsibilities





Reliability in the Evolving Resource Mix

BAL-007-1 | TOP-003-7

BAL-007-1

Near-Term Energy Reliability Assessments

Effective Date: October 1, 2027

Direct Adoption



Key Provisions

- Mandatory Near-Term Energy Reliability Assessments
- Evaluates energy adequacy over a 5-day to 6-week horizon
- Stress testing for demand, fuel, and energy supply risks
- Operating Plans for forecasted Energy Emergencies

Compliance Considerations

- Review existing energy assessment processes
- Develop evidence retention and documentation practices
- Establish Operating Plans tied to assessment results

Implementation Impacts

- Significant new assessment and forecasting requirements
- Increased focus on fuel and energy limitations
- Additional coordination between planning and operations functions.

TOP-003-7

Data and Information Specification and Collection

Effective Date: October 1, 2027

Key Changes	Québec-Specific Modifications	Compliance Considerations	Implementation Impacts
<ul style="list-style-type: none">• Data to support Near-Term ERAs• Identification and collection of energy-related reliability data• Data specification distribution requirements• Supports implementation of Near-Term ERAs	<ul style="list-style-type: none">• Direct adoption with limited administrative adaptations• Applies using Québec RTP applicability definitions	<ul style="list-style-type: none">• Review applicability of facilities and data obligations• Update data-sharing agreements where necessary• Validate availability of ERA-related information	<ul style="list-style-type: none">• Enhanced data governance requirements• Additional data collection and sharing obligations• Closer coordination with Balancing Authority assessment processes



Effective Date Summary

FAC-003-5

- Enforcement tied to PC/TP identification
- 12 months after identification or applicable planning year

FAC-011-4

- Industrial generation exemption to 2029
- RTP $\leq$ 230 kV exemption to 2036

FAC-014-3

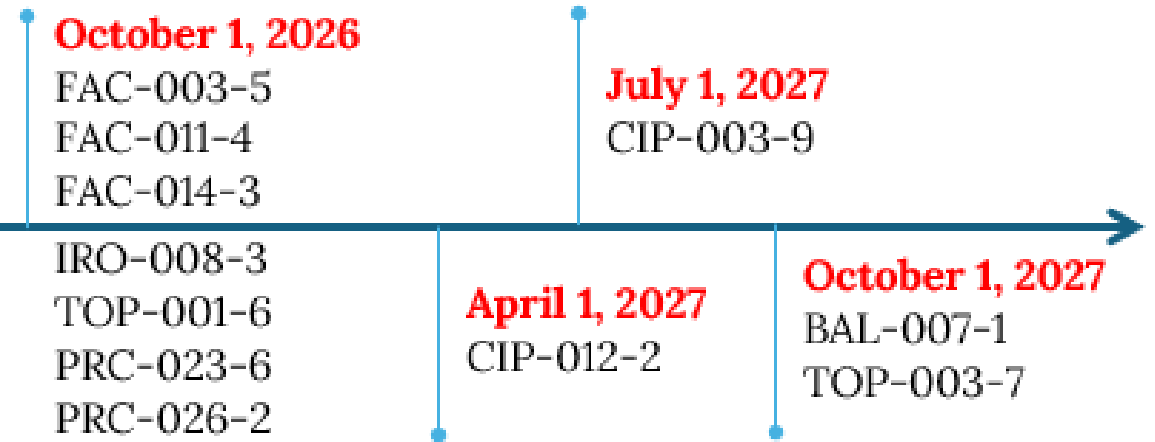
- R1-R5 effective October 1, 2026
- R6 next Planning Assessment cycle
- R7, R8 effective by October 1, 2027

PRC-023-6

- First PC assessment: next calendar year or 15 months after last assessment
- Newly selected facilities: 39 months after notification or first applicable year

PRC-026-2

- R1 transition assessment in 2026
- R2-R4 effective October 1, 2026



Additional Resources

<u>Project 2015-09 Establish and Communicate System Operating Limits</u>				<u>Project 2020-03 Supply Chain Low Impact Revisions</u>	
<u>FAC-003-5</u>	Supplement in Standard	<u>IRO-008-3</u>	<u>Technical Rationale</u>	<u>CIP-003-9</u>	<u>Technical Rationale</u>
<u>FAC-011-4</u>	<u>Technical Rationale</u>	<u>PRC-026-2</u>		<u>Project 2020-04 Modifications to CIP-012</u>	
<u>FAC-014-3</u>	<u>Technical Rationale</u>	<u>TOP-001-6</u>	<u>Technical Rationale</u>	<u>CIP-012-2</u>	<u>Technical Rationale</u>
<u>Project 2022-03 Energy Assurance with Energy-Constrained Resources</u>				<u>Project 2021-05 Modifications to PRC-023</u>	
<u>BAL-007-1</u>	<u>TOP-003-7</u>	<u>Technical Rationale</u>		<u>PRC-023-6</u>	<u>Technical Rationale</u>





Questions?

Contact Us: npcc.org/contact

NPCC Standards & Criteria

Patrick Davis
Senior Standards & Criteria Engineer

Quebec Reliability Standards Update | Public

2026 Régie Annual Reliability Seminar | October 6, 2026

Participation des entités visées au processus de consultations publiques



Présenté par Junji Yamaguchi, ing.
Chef – Affaires réglementaires du Coordonnateur, analyse et encadrements,
Hydro-Québec

6 octobre 2026



Junji Yamaguchi

Chef – Affaires réglementaires du Coordonnateur, analyse et encadrements, Hydro-Québec

Fort de plus de vingt ans d'expérience, il veille à ce que le réseau électrique du Québec soit fiable et conforme aux normes de fiabilité NERC, tout en travaillant avec différents partenaires pour améliorer la sécurité et la performance du réseau.

Diplômé en génie électrique de l'Université de Sherbrooke et titulaire d'une maîtrise en administration des affaires de HEC Montréal, il est reconnu pour son leadership, sa capacité à innover et à expliquer clairement des sujets complexes à tous les publics.

Passionné par la collaboration et le partage des connaissances, il aime rendre accessibles les enjeux techniques et réglementaires, et croit que la fiabilité du réseau repose autant sur l'expertise que sur l'engagement des équipes.

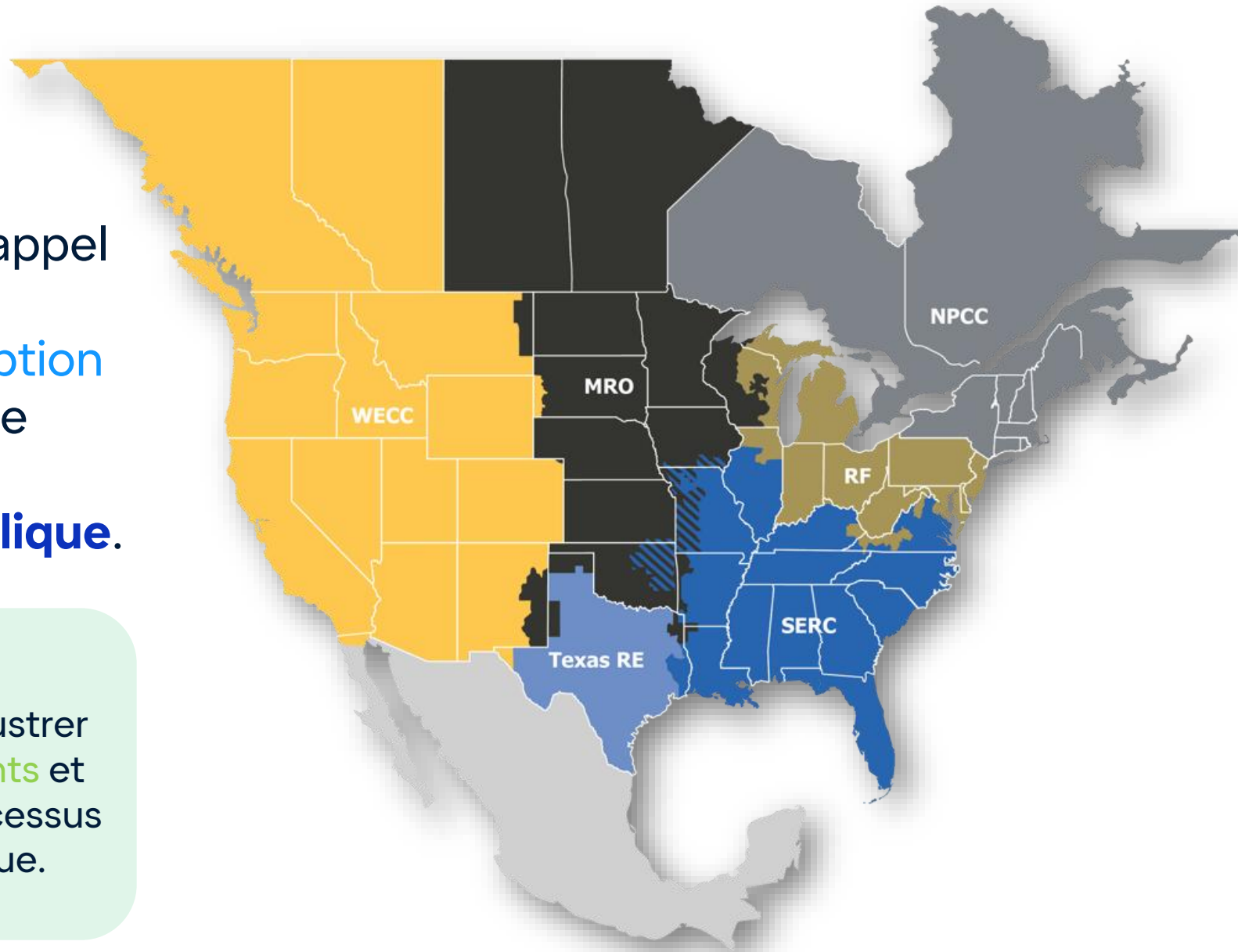
Introduction

Cette présentation inclura un rappel du **contexte Nord-américain** entourant l'élaboration et l'adoption des **normes** et mettra en lumière **l'importance de participer au processus de consultation publique.**



Un exemple pratique

sera présenté afin d'illustrer les différents **documents** et les **étapes clés** du processus de consultation publique.



Évolution du régime de normes obligatoires au Québec

2006

Adoption au Québec de la stratégie énergétique (projet de loi 52 devenu loi 46) qui confère de nouveaux pouvoirs à la Régie sur l'application des normes obligatoires

2009

Première entente entre la Régie, la NERC et le NPCC : développement des normes de fiabilité, procédures et programme de surveillance

2015

Entrée en vigueur du régime **obligatoire** des normes de fiabilité au Québec

2022

Troisième entente entre la Régie, la NERC et le NPCC : Révision des rôles et responsabilités du PSCAQ

2007

Désignation du Coordonnateur de la fiabilité au Québec par la Régie

2014

Deuxième entente entre la Régie, la NERC et le NPCC : mise en œuvre du programme de surveillance de la conformité et d'application des normes de fiabilité du Québec (PSCAQ)

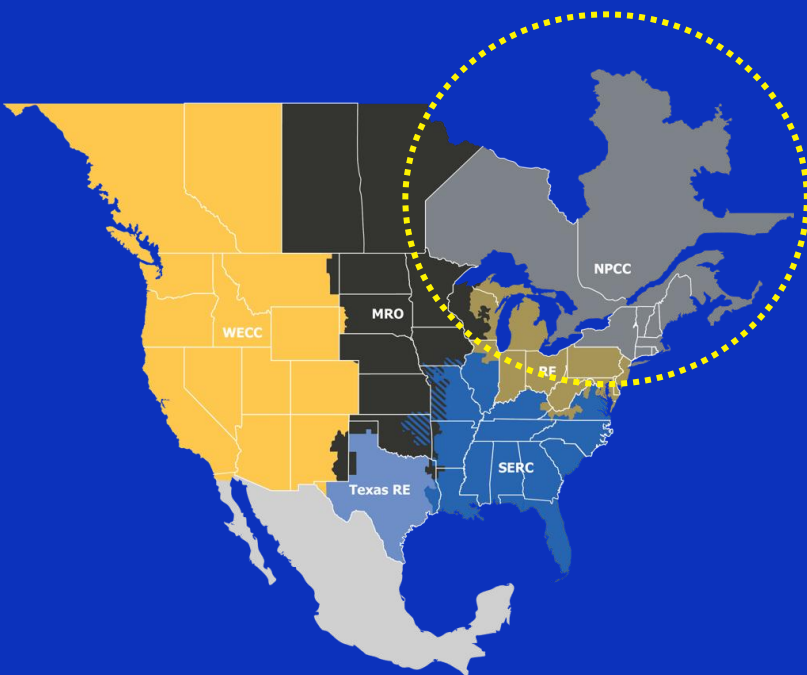
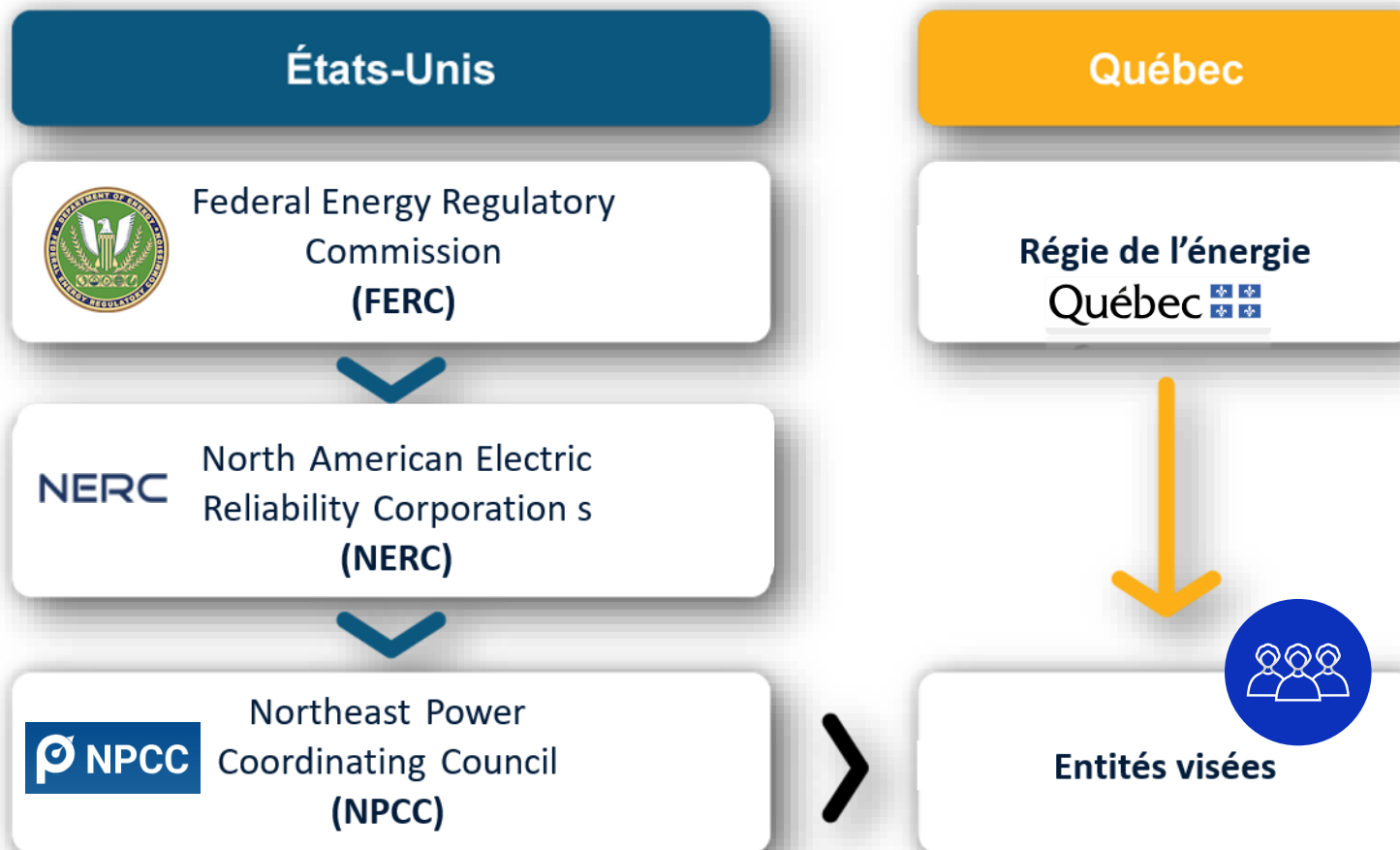
2016

Guide des sanctions en cas de contravention

2023

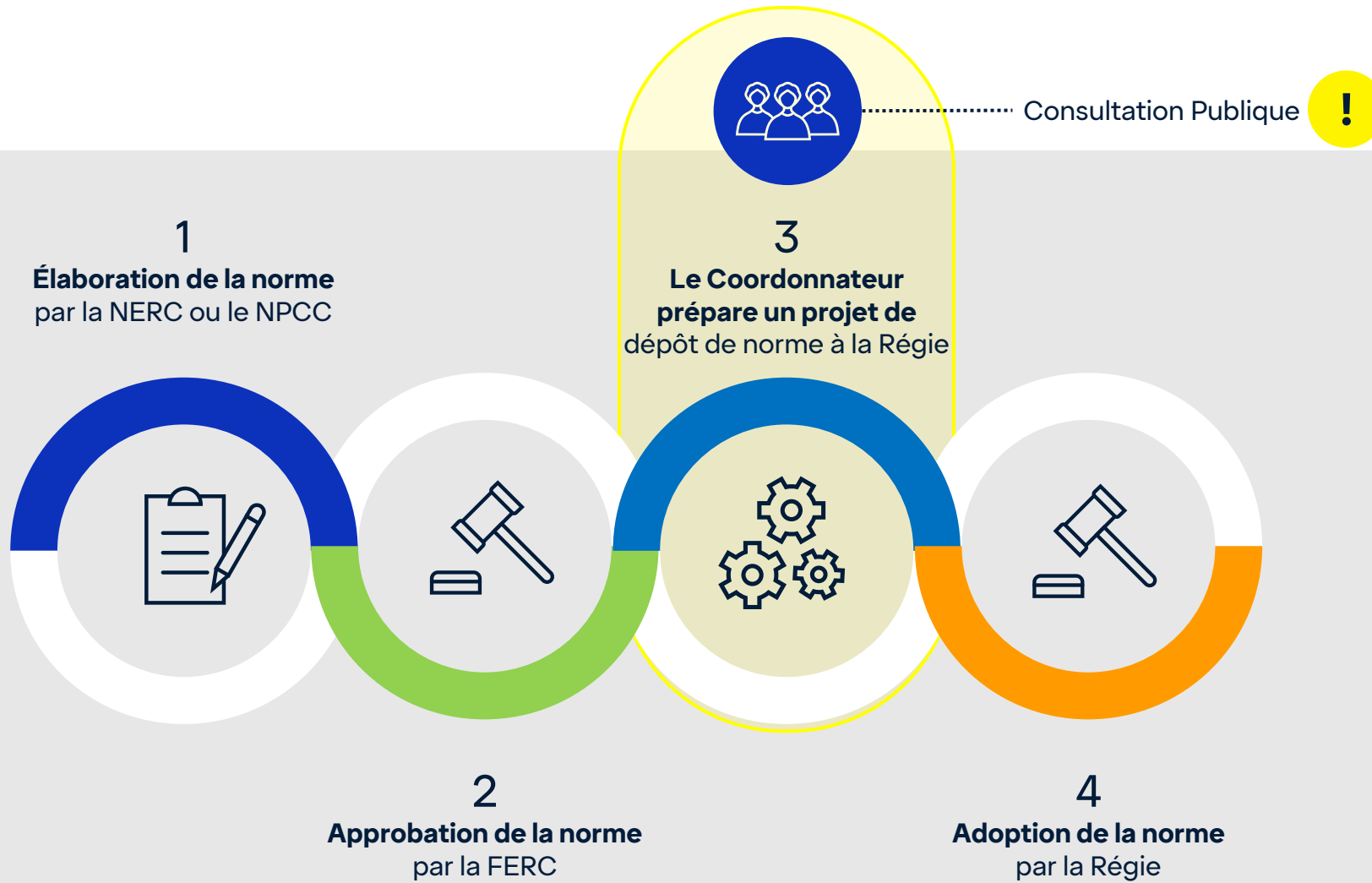
La Régie prend acte d'une définition du réseau de transport principal (RTP) comportant un critère net pour l'inclusion des éléments exploités à 300 kV ou plus

Les acteurs du régime obligatoire des normes



Cadre réglementaire des normes au Québec

Survol : l'élaboration et l'adoption des normes



1

Élaboration de la norme
par la NERC ou le NPCC

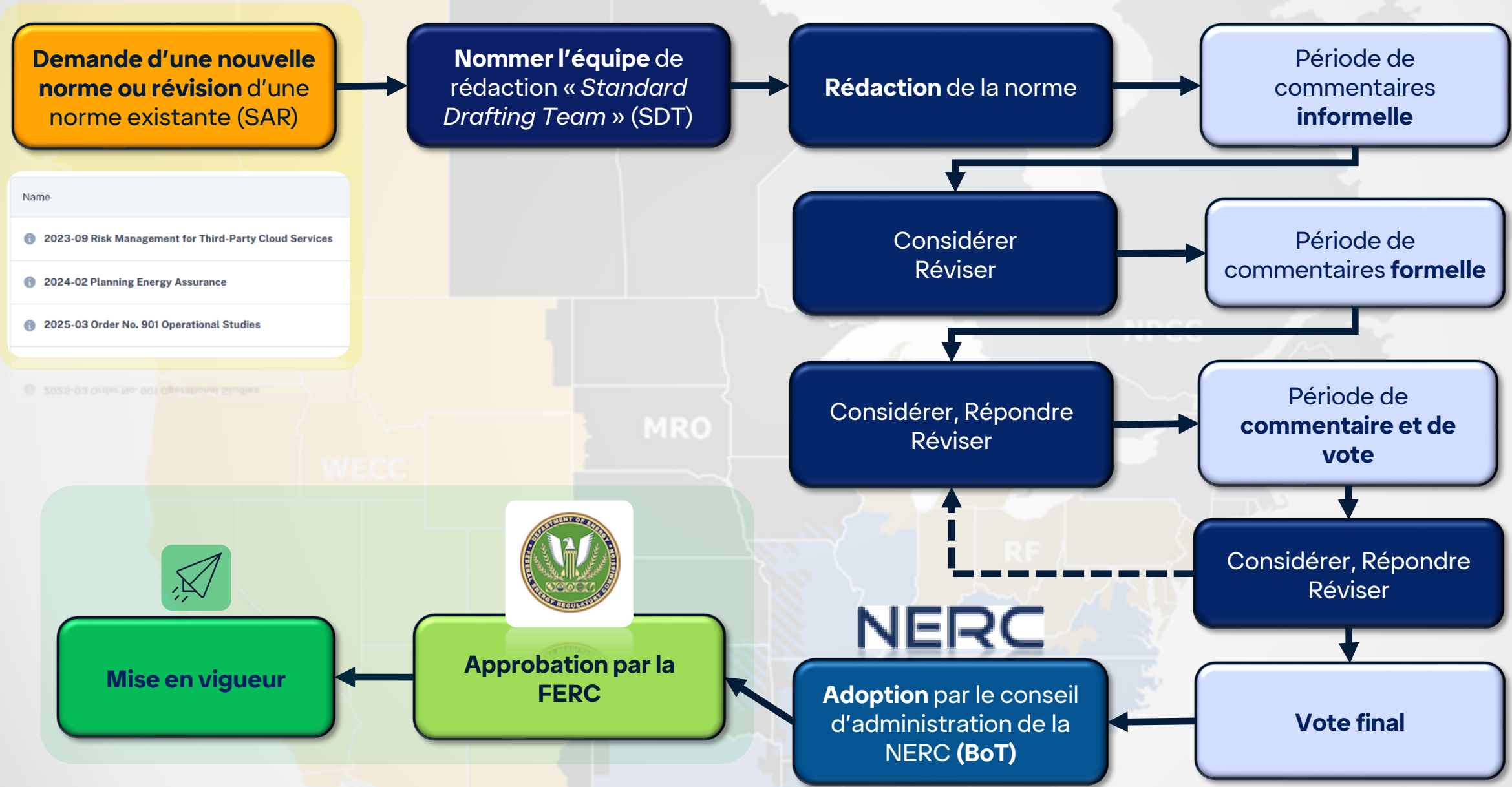


2

Approbation de la norme
par la FERC

L'élaboration et l'adoption d'une norme NERC

Le processus d'élaboration des normes NERC



3

**Le Coordonnateur
prépare un projet de
dépôt de norme à la Régie**



4

**Adoption de la norme
par la Régie**

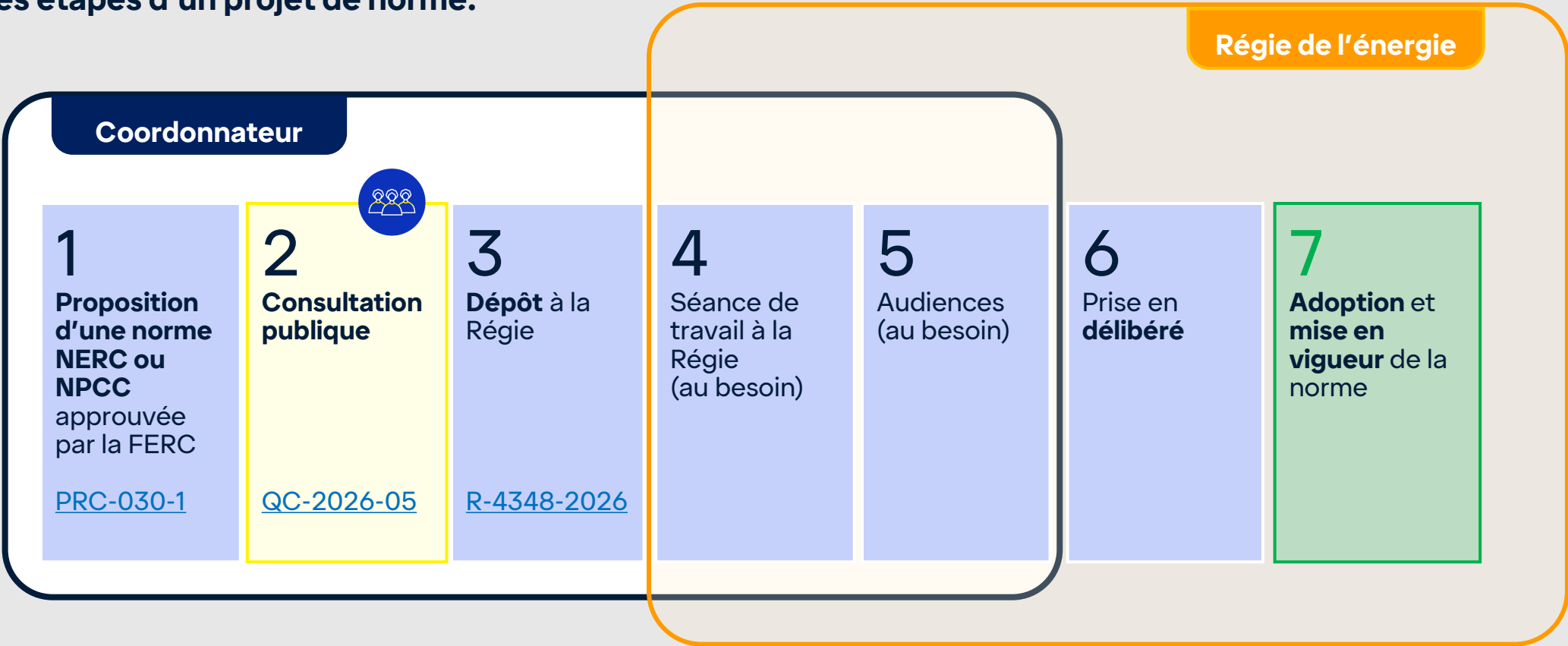
La préparation du projet de dépôt de norme à la Régie

Le processus de dépôt des normes à la Régie



Exemple pratique:
Demande d'adoption de la norme PRC-030-1:
«Correction des comportements imprévus des sources d'énergie raccordées au moyen d'onduleurs»

Les grandes étapes d'un projet de norme:



La préparation du dossier

Proposition d'une norme NERC approuvée par la FERC: PRC-030-1 (QC-2026-05)

PRC-030-1 – Correction des comportements imprévus des sources d'énergie raccordées au moyen d'onduleurs

A. Introduction

- Titre :** Correction des comportements imprévus des sources d'énergie raccordées au moyen d'onduleurs
- Numéro :** PRC-030-1
- Objet :** Détecter, analyser et corriger les variations imprévues de la puissance de sortie des sources d'énergie raccordées au moyen d'onduleurs (SERMO).
- Applicabilité :**
 - Entités fonctionnelles :**
 - 4.1.1.** Propriétaire d'installation de production
 - Installations :**
 - 4.2.1.** SERMO faisant partie du système de production-transport d'électricité (BES).
 - 4.2.2.** SERMO hors BES qui ont une puissance nominale combinée égale ou supérieure à 20 MVA, ou qui contribuent à fournir une telle puissance, et qui sont raccordées par un dispositif conçu principalement pour injecter cette production à un point de raccordement commun à une tension égale ou supérieure à 60 kV.

Annexe PRC-030-1-QC-1

Dispositions particulières applicables au Québec visant la norme

PRC-030-1 – Correction des comportements imprévus des sources d'énergie raccordées au moyen d'onduleurs

La présente annexe établit les dispositions particulières d'application au Québec de la norme qu'elle vise. Les dispositions de la norme visée et de l'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 a préséance.

A. Introduction

- Titre :** Aucune disposition particulière.
- Numéro :** Aucune disposition particulière.
- Objet :** Aucune disposition particulière.
- Applicabilité :** Dans l'application de cette norme, toute référence au terme « système de production-transport d'électricité » ou « BES » doit être remplacée par les termes « réseau de transport principal » ou « RTP » respectivement.

Les installations visées par cette norme sont les installations du réseau de transport principal (RTP).

 Coordonnateur de la fiabilité au Québec

Projet QC-2026-05

Correction des comportements imprévus des sources d'énergie raccordées au moyen d'onduleurs

1. PRÉSENTATION DES NORMES

1.1. Applicabilité

Le Coordonnateur de la fiabilité (ci-après le « Coordonnateur ») demande l'approbation de la nouvelle norme de fiabilité PRC-030-1.

La fonction visée par la norme proposée pour adoption, soit la *norme de fiabilité* PRC-030-1, est indiquée dans le tableau ci-dessous.

Norme	Fonctions visées
PRC-030-1	Propriétaire d'installation de production (GO)

Traduction de la norme

- Envoi de la norme à l'équipe de traduction
- Réception de la norme traduite: Vérification et réponse aux commentaires
- Validation avec les SMÉ (si requis)
- Renvoi de la version corrigée au traducteur. Émission de la version attestée

Annexe Québec

- Analyse de l'annexe Québec actuelle
- Détermination des dispositions particulières
- Consultation des SMÉ (si requis)

Sommaire de la norme

- Analyse de la documentation du projet de la NERC et de l'historique au Québec
- Consultation des experts sur l'évaluation de l'impact préliminaire
- Décision sur le délai d'implantation au Québec
- Lecture de la décision de la FERC et analyse

La préparation du dossier

Proposition d'une norme NERC
approuvée par la FERC



Avis de consultation publique

- **Document normalisé** lors de l'émission d'une consultation publique (date, contenu, objectif, formulaire de commentaire)
- Décisions sur la date de consultation publique

1

Avis de consultation Projet QC-2026-05

Mai 2026

Avis est donné

- Aux entités inscrites au Registre des entités visées;
- À la North American Electric Reliability Corporation, inc. (NERC);
- Au Northeast Power Coordinating Council, inc. (NPCC);
- Aux coordonnateurs de la fiabilité du NPCC;
- À la Régie de l'énergie du Québec (la « Régie »).

2

Période de consultation : du 4 mai 2026 au 25 mai 2026.

Objectif de la consultation

Conformément à la décision [D-2011-139](#) et [D-2023-049](#) de la Régie, le Coordonnateur de la fiabilité au Québec (le « Coordonnateur ») sollicite les commentaires des entités visées sur la norme de fiabilité suivante en vue de son éventuelle adoption par la Régie.

3

Nouvelle version de la norme :

- PRC-030-1 – Correction des comportements imprévus des ressources raccordées par onduleur

Le Coordonnateur demande aux entités visées de se prononcer sur la pertinence et les impacts de la norme de fiabilité à adopter et retirer. À cet effet, veuillez utiliser le formulaire disponible en ligne sur le site Web du Coordonnateur, à la page Consultation publique des entités (<https://www.hydroquebec.com/coordonnateur-fiabilite/documentation/consultation.html>). Veuillez prendre soin d'indiquer clairement sur quel document (et sur quelle section de celui-ci) portent vos commentaires.

Vous pouvez également transmettre vos questions et commentaires par courriel à fiabilite@hydro.qc.ca.

4

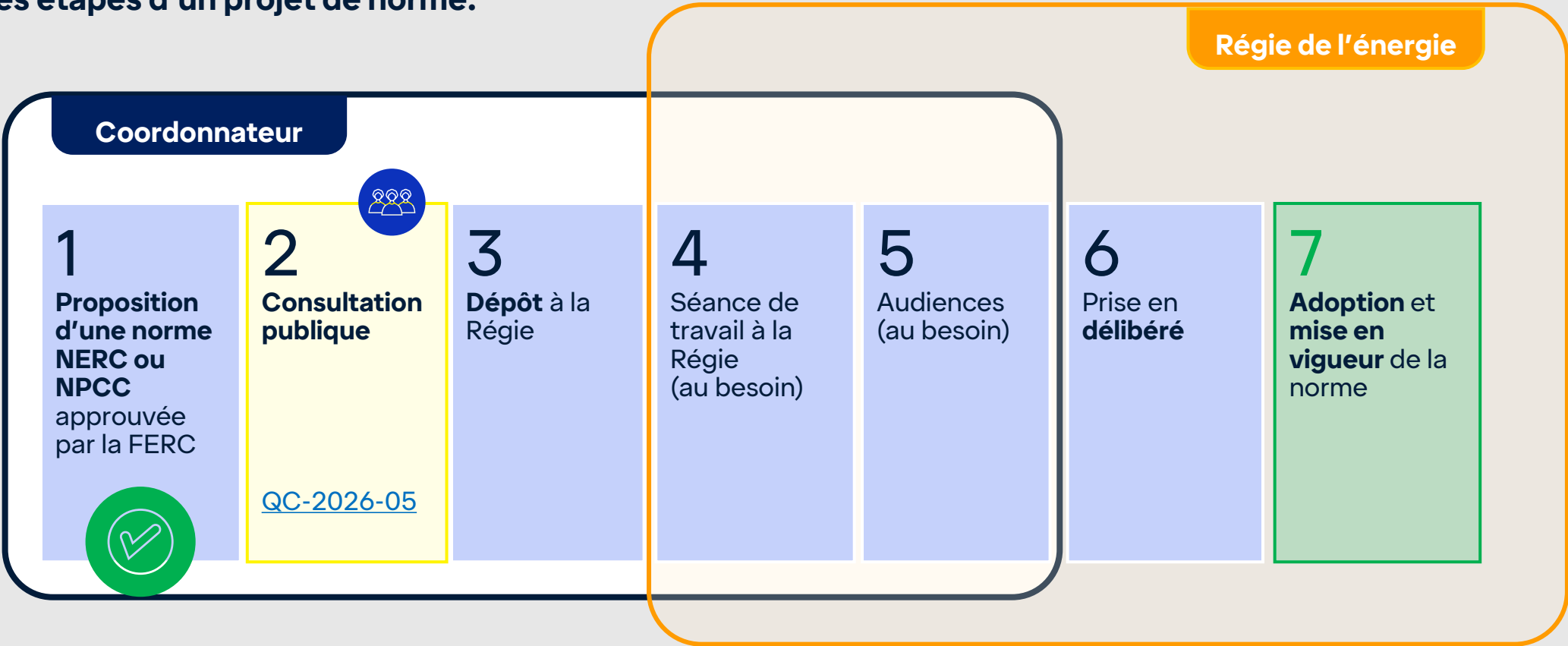
Documents

- Norme et annexe QC proposée;
- Sommaire de la norme à adopter, y compris une évaluation préliminaire de la pertinence et de l'impact;
- Justification technique de la norme proposée.

Le processus de dépôt des normes à la Régie

La consultation publique

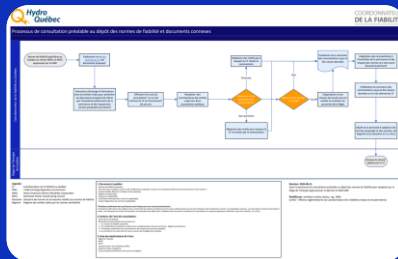
Les grandes étapes d'un projet de norme:





La consultation publique

Processus de C.P.
approuvé par la Régie



Tous les intervenants du secteur de l'électricité en Amérique du Nord qui sont susceptibles d'être touchées par les normes de fiabilité de la [North American Electric Reliability Corporation \(NERC\)](#) **peuvent participer** à l'élaboration de nouvelles normes et à la révision des normes existantes.

Au Québec, le coordonnateur de la fiabilité est chargé de consulter les entités avant de déposer les normes de la NERC à la Régie de l'énergie pour adoption.

- [Processus de consultation approuvé par la Régie de l'énergie du Québec \[PDF 73 ko\]](#)
- [Décision de la Régie de l'énergie approuvant le processus de consultation du coordonnateur de la fiabilité \(D-2011-139\) \[PDF 424 ko\]](#)
- [Décision de la Régie de l'énergie modifiant le processus de consultation du coordonnateur de la fiabilité \(D-2023-049\) \[PDF 584 ko\]](#)

<https://www.hydroquebec.com/coordonnateur-fiabilite/documentation/consultation.html>



La consultation publique

Les documents de la consultation publique:

- ✓ **l'avis** de consultation transmis aux parties prenantes **par courriel** ;
- ✓ **les normes** sur lesquelles porte la consultation ainsi que l'évaluation de leur pertinence et de leur impact faite par le Coordonnateur de la fiabilité ;
- ✓ **les formulaires** à remplir pour fournir des commentaires ;
- ✓ **les réponses aux commentaires des parties prenantes** formulées par le Coordonnateur de la fiabilité après la consultation et suivant une analyse rigoureuse.

La consultation publique



Avis de consultation : QC-2026-05

Documents visés

Premier avis [PDF 1.15 ko]

Documents [ZIP 1.49 Mo]

Formulaires de consultation

Normes et documents complémentaires [ZIP 1.31 Mo]

Évaluation des impacts des normes proposées [ZIP 1.79 Mo]

Réponses du Coordonnateur aux commentaires à la suite de la période de consultation

Réponses du Coordonnateur aux commentaires

Publication sur le site internet du Coordonnateur

Émission de l'avis aux entités visées

Réception des commentaires
Généralement deux semaines de délai pour commenter la documentation

Hydro Québec

Projet QC-2026-05

Réponses aux commentaires reçus pendant la période de consultation

Mai 2026

Ce document est une synthèse des commentaires présentés par les entités, tels qu'ils ont été reçus et dans la langue et selon la rédaction utilisée par celles-ci pendant la période de consultation portant sur le projet QC-2026-05.

Document visé	Section visée	Commentaires	Entité	Réponse du coordonnateur de la fiabilité
PRG-030-1	Annexe GC-1	Section A3: tableau de mise en application. Pour la mise en application des SERMO Hous-RTP et avant d'être adoptés par le conseil d'administration, les documents doivent être en français et en anglais de la norme PRG-030-1.1. La date d'entrée en vigueur de la norme PRG-030-1.1 ne sera pas inférieure que 2 ans après sa mise en vigueur.	RTA	Le Coordonnateur remercie l'entité pour sa participation à la consultation publique. Le Coordonnateur a apporté les modifications suivantes à l'annexe GC-1 de la PRG-030-1: <ul style="list-style-type: none">• Dans (2) entités visées au sein (3) de la norme PRG-030-1.1, la phrase « Pour le Québec, ce document est équivalent à celui accordé aux États-Unis, tel que précisé dans le plan d'implantation de la NERC ».
PRG-030-1	Annexe GC-1	Article 4.2.2: On devrait spécifier que la disposition particulière remplace l'article 4.2.2 de la norme.	RTA	Les dispositions de la norme visée et de l'annexe doivent obligatoirement être comprises. De manière générale, lorsqu'une disposition particulière est prévue à l'annexe GC, elle remplace la disposition correspondante de la norme visée. Pour cette raison, le Coordonnateur estime que l'article 4.2.2 de l'annexe GC est suffisamment clair tel quel.
PRG-030-1	Annexe GC-1	Article 4: Applicable. On devrait ajouter la description des installations de l'article 4.2.2.1 à la suite du texte suivant de l'annexe GC: Les installations visées par cette norme sont les installations du réseau de transport principal (RTP).	RTA	Le Coordonnateur remercie le commentateur de RTA. Les corrections nécessaires seront apportées à l'article 4 de l'annexe GC de la PRG-030-1, de la même manière que pour l'annexe GC de la PRG-030-1, qui traite de la partie relative à la NERC.
PRG-030-1	Annexe GC-1 (version anglaise)	We have no concerns with the proposed implementation dates for non-RTP investor-based resources. <ul style="list-style-type: none">• At the latest of the following dates:<ul style="list-style-type: none">○ The effective date of PRG-030-1, or○ Within two (2) calendar years of the effective date of PRG-030-1.	RTA	Le Coordonnateur remercie l'entité pour sa participation à la consultation publique. Le Coordonnateur a apporté les modifications suivantes à l'annexe GC de la PRG-030-1: <ul style="list-style-type: none">• Dans (2) entités visées au sein (3) de la norme PRG-030-1, la phrase « Pour le Québec, ce document est équivalent à celui accordé aux États-Unis, tel que précisé dans le plan d'implantation de la NERC ». The Coordinator thanks the entity for its participation in the public consultation. The Coordinator incorporated the following modifications to the Appendix GC of PRG-030-1: <ul style="list-style-type: none">• Within two (2) calendar years of PRG-030-1 approval date, by the RTA. OR The effective date of PRG-030-1.• For Québec, this timeframe is equivalent to that granted in the United States, as specified in NERC's implementation plan.

Traitement et publication des réponses aux commentaires

Préparation des réponses aux commentaires.

16 Hydro-Québec

La consultation publique

Exemple d'avis par courriel : QC-2026-05 (PRC-030-1)



Consultation publique QC-2026-05 | Norme de fiabilité PRC-030-1



> Coordonnateur de la fiabilité

À < Coordonnateur de la fiabilité

Cci < Secretariat-Régie



Diffusion restreinte

Aux entités inscrites au registre des entités visées proposé;
À la North American Electric Reliability Corporation, inc. (NERC);
Au Northeast Power Coordinating Council, inc. (NPCC);
Aux coordonnateurs de la fiabilité du NPCC;
À la Régie de l'énergie du Québec.

Le Coordonnateur de la fiabilité au Québec sollicite vos commentaires sur sa demande d'adoption de la norme PRC-030-1.

L'Avis de consultation **QC-2026-05** se trouve sur le [site de consultation](#) du Coordonnateur de la fiabilité où vous trouverez également les formulaires appropriés pour transmettre vos commentaires.

La consultation publique se termine le 25 mai 2026.

Pour toute question à ce sujet, vous pouvez communiquer avec nous par courriel à : fiabilite@hydro.qc.ca

Cordialement,



Coordonnateur de la fiabilité

Direction Principale, Contrôle des mouvements d'énergie et Exploitation des réseaux

Courriel : fiabilite@hydro.qc.ca

Site internet : <http://www.hydroquebec.com/coordonnateur-fiabilite/>

← Répondre

← Répondre

1



COORDONNATEUR
DE LA FIABILITÉ

Avis de consultation Projet QC-2026-05

Mai 2026

Avis est donné

- Aux entités inscrites au Registre des entités visées;
- À la North American Electric Reliability Corporation, inc. (NERC);
- Au Northeast Power Coordinating Council, inc. (NPCC);
- Aux coordonnateurs de la fiabilité du NPCC;
- À la Régie de l'énergie du Québec (la « Régie »).

Période de consultation : du 4 mai 2026 au 25 mai 2026.

Objectif de la consultation

Conformément à la décision D-2011-139 et D-2023-049 de la Régie, le Coordonnateur de la fiabilité au Québec (le « Coordonnateur ») sollicite les commentaires des entités visées sur la norme de fiabilité suivante en vue de son éventuelle adoption par la Régie.

Nouvelle version de la norme :

- PRC-030-1 – Correction des comportements imprévus des ressources raccordées par onduleur

Le Coordonnateur demande aux entités visées de se prononcer sur la pertinence et les impacts de la norme de fiabilité à adopter et retirer. À cet effet, veuillez utiliser le formulaire disponible en ligne sur le site Web du Coordonnateur, à la page Consultation publique des entités (<https://www.hydroquebec.com/coordonnateur-fiabilite/documentation/consultation.html>). Veuillez prendre soin d'indiquer clairement sur quel document (et sur quelle section de celui-ci) portent vos commentaires.

Vous pouvez également transmettre vos questions et commentaires par courriel à fiabilite@hydro.qc.ca.

Documents

- Norme et annexe QC proposée;
- Sommaire de la norme à adopter, y compris une évaluation préliminaire de la pertinence et de l'impact;
- Justification technique de la norme proposée.

Direction principale – Contrôle des mouvements d'énergie et exploitation du réseau

1 / 1

2

[Avis de consultation : QC-2026-05](#)

Documents visés

> [Premier avis](#) [PDF 115 ko]

> [Documents](#) [ZIP 1,49 Mo]

Formulaires de consultation

> [Normes et documents complémentaires](#) [ZIP 1,31 Mo]

> [Évaluation des impacts des normes proposées](#) [ZIP 1,79 Mo]

Réponses du Coordonnateur aux commentaires à la suite de la période de consultation

> [Réponses du Coordonnateur aux commentaires](#) [PDF 164 Ko]

La consultation publique

Site internet du coordonnateur



Coordonnateur de la fiabilité au Québec > Documentation >

Consultation publique des entités

Tous les intervenants du secteur de l'électricité en Amérique du Nord qui sont susceptibles d'être touchées par les normes de fiabilité de la [North American Electric Reliability Corporation \(NERC\)](#) peuvent participer à l'élaboration de nouvelles normes et à la révision des normes existantes.

Au Québec, le coordonnateur de la fiabilité est chargé de consulter les entités avant de déposer les normes de la NERC à la Régie de l'énergie pour adoption.

- [Processus de consultation approuvé par la Régie de l'énergie du Québec \[PDF 73 ko\]](#)
- [Décision de la Régie de l'énergie approuvant le processus de consultation du coordonnateur de la fiabilité \[PDF 424 ko\]](#)

Liste des consultations

Voici la liste des consultations que le Coordonnateur de la fiabilité a menées depuis 2012. Cliquez sur le titre d'une consultation pour prendre connaissance des éléments suivants :

- l'avis de consultation transmis aux parties prenantes ;
- les normes sur lesquelles porte la consultation ainsi que l'évaluation de leur pertinence et de leur impact faite par le Coordonnateur de la fiabilité ;
- les formulaires à remplir pour fournir des commentaires ;
- les réponses aux commentaires des parties prenantes formulées par le Coordonnateur de la fiabilité après la consultation et suivant une analyse rigoureuse.

[Avis de consultation : QC-2024-02](#)



[Avis de consultation : QC-2024-01](#)



La consultation publique

Formulaires à compléter



COORDONNATEUR
DE LA FIABILITÉ

1

Normes et documents complémentaires

Formulaire de commentaires

Nom		Courriel		N° de l'avis
Téléphone		Entité (nom de la compagnie)		
	Document visé	Section du document visée	Commentaires	
✕ 1				
✕ 2				
✕ 3				
✕ 4				
✕ 5				
✕ 6				
✕ 7				
✕ 8				
✕ 9				
✕ 10				

Ajouter une ligne Envoyer par courriel



COORDONNATEUR
DE LA FIABILITÉ

2

Évaluation des impacts des normes proposées

Activités et coûts liés à l'implantation des changements proposés

Nom		Courriel		N° de l'avis	
Téléphone		Entité (nom de la compagnie)			
	Normes proposées	Coûts de mise en œuvre	Coûts récurrents annuels	Justifications (coûts de mise en œuvre et coûts récurrents)	Autres impacts
✕ 1					
✕ 2					
✕ 3					
✕ 4					
✕ 5					
✕ 6					
✕ 7					
✕ 8					
✕ 9					
✕ 10					
		0,00 \$	0,00 \$		

Ajouter une ligne Envoyer par courriel

Direction – Contrôle de mouvements d'énergie
063-1586 (14-12) E FRM

Page 1 de 1

3



fiabilite@hydro.qc.ca.

La consultation publique

Exemple de réponses aux commentaires: QC-2026-05 (PRC-030-1)



Coordonnateur de la fiabilité

Projet QC-2026-05

Réponses aux commentaires reçus pendant la période de consultation

Mai 2026

Ce document est une synthèse des commentaires présentés par les entités, tels qu'ils ont été reçus et dans la langue et selon la rédaction utilisée par celles-ci pendant la période de consultation portant sur le projet QC-2026-05.

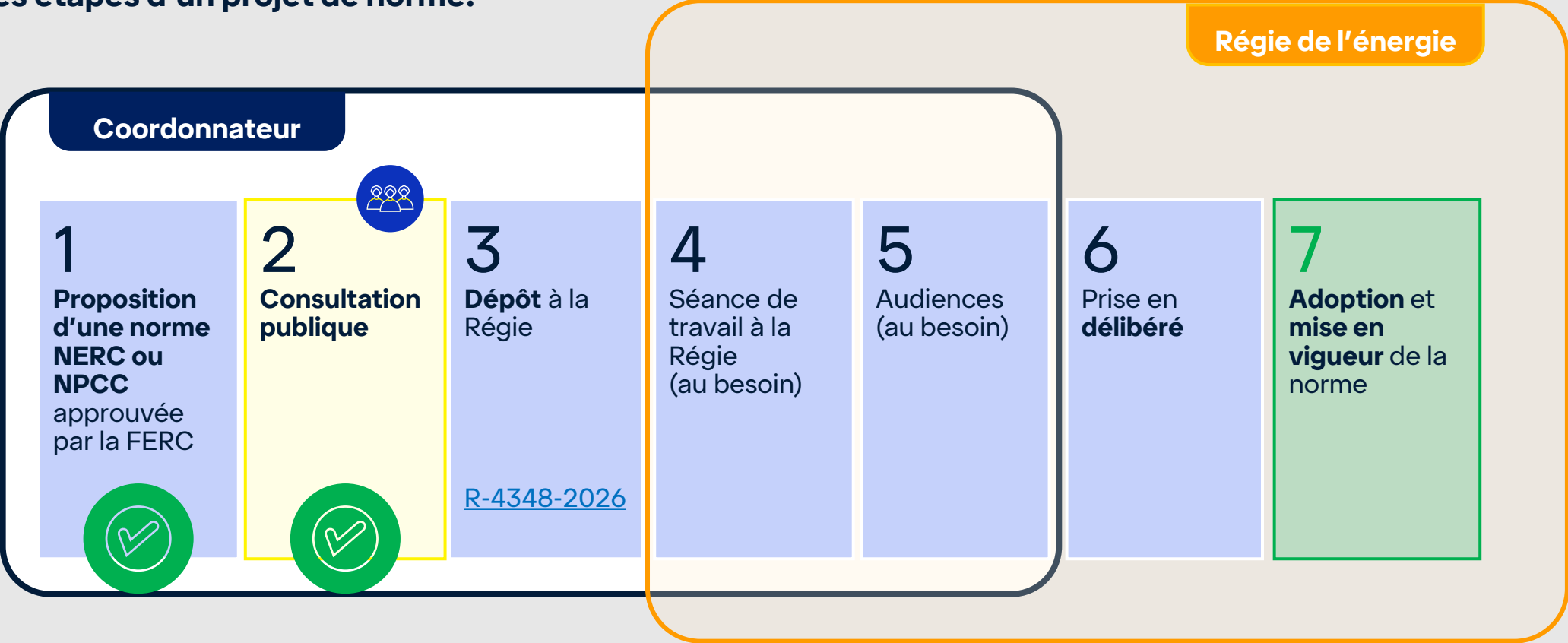
Document visé	Section visée	Commentaire	Entité	Réponse du coordonnateur de la fiabilité
PRC-030-1	Annexe QC-1	Section A5: tableau de mise en application. Pour la mise en application des SERMO Hors-RTP il serait plus simple de seulement indiquer "Deux (2) années civiles suivant la date d'entrée en vigueur de la norme PRC-030-1", car la date d'entrée en vigueur de la norme PRC-030-1 ne sera jamais plus tardive que 2 ans après sa mise en vigueur.	RTA	<p>Le Coordonnateur remercie l'entité pour sa participation à la consultation publique. Le Coordonnateur a apporté les modifications suivantes à l'annexe QC de la PRC-030-1:</p> <ul style="list-style-type: none">« Deux (2) années civiles suivant l'adoption de la norme PRC-030-1 par la Régie »;Pour le Québec, ce délai est équivalent à celui accordé aux États-Unis, tel que précisé dans le plan d'implantation de la NERC.
PRC-030-1	Annexe QC-1	Article 4.2.2: On devrait spécifier que la disposition particulière remplace l'article 4.2.2 de la norme.	RTA	<p>Les dispositions de la norme visée et de l'annexe doivent obligatoirement être lues conjointement. De manière générale, lorsqu'une disposition particulière est prévue à l'Annexe QC, elle remplace la disposition correspondante de la norme visée. Pour cette raison, le Coordonnateur estime que l'article 4.2.2 de l'Annexe QC est suffisamment clair tel quel.</p>
PRC-030-1	Annexe QC-1	Article 4. Applicabilité: On devrait ajouter "à l'exception des installations de l'article 4.2.2." à la suite du texte suivant de l'annexe QC "Les installations visées par cette norme sont les installations du réseau de transport principal (RTP)"	RTA	<p>Le Coordonnateur retient le commentaire de RTA. Les corrections nécessaires seront apportées à l'article 4 de l'Annexe QC de la PRC-030-1, de la même manière que pour l'Annexe QC de la PRC-028-1, qui traite de ce point (référence : DDR1, réponse R4.1 au dossier R-4314-2025).</p>
PRC-030-1	Annexe QC-1 (version anglaise)	<p>We have no concerns with the proposed adoption of the standard.</p> <p>We have no concerns with the proposed implementation dates for non-RTP inverter-based resources:</p> <ul style="list-style-type: none">At the latest of the following dates:<ul style="list-style-type: none">The effective date of PRC-029-1, orWithin two (2) calendar years of the effective date of PRC-030-1	TRA	<p>Le Coordonnateur remercie l'entité pour sa participation à la consultation publique. Le Coordonnateur a apporté les modifications suivantes à l'annexe QC de la PRC-030-1:</p> <ul style="list-style-type: none">« Deux (2) années civiles suivant l'adoption de la norme PRC-030-1 par la Régie OU La date d'entrée en vigueur de la PRC-030-1 »;Pour le Québec, ce délai est équivalent à celui accordé aux États-Unis, tel que précisé dans le plan d'implantation de la NERC. <p><i>The Coordinator thanks the entity for its participation in the public consultation. The Coordinator incorporated the following modifications to the Appendix QC of PRC-030-1:</i></p> <ul style="list-style-type: none"><i>"Within two (2) calendar years of <u>PRC-030-1 approval date by the Régie</u> OR The effective date of <u>PRC-030-1</u>;"</i><i>For Québec, this timeframe is equivalent to that granted in the United States, as specified in NERC's implementation plan.</i>

Le processus de dépôt des normes à la Régie

Dépôt à la Régie



Les grandes étapes d'un projet de norme:



Dépôt à la Régie

Finalisation de la documentation



Préparation finale de la documentation

- Norme , Annexe Québec
- Attestation de traduction
- Information relative à la norme
- Présentation de la demande
- Requête et affidavit
- Justification technique et/ou guide d'implantation (s'il y a lieu)



Demande de numéro à la Régie et dépôt

- Numéro R-4XXX-202X
- Dépôt dans le système de dépôt électronique

Régie
de l'énergie
Québec

Accueil SDÉ

Système de dépôt électronique

Dépôt à la Régie

Exemple : R-4348-2026 (PRC-030-1)



Québec

Régie de l'énergie

Calendrier des audiences

Diffusion des audiences

Foire aux questions

Nouvelles

Plaintes des consommateurs

Prix des produits pétroliers

Recrutement

LA RÉGIE

CONSOMMATEURS

PARTICIPANTS - TRAVAUX RÉGLEMENTAIRES

ENTITÉS VISÉES - NORMES DE FIABILITÉ

PRODUITS PÉTROLIERS

Accueil

Participants - Travaux réglementaires

Audiences en cours

Électricité - Fiabilité du réseau de transport

Audiences en cours

Toutes les audiences en cours

Électricité - Distribution

Électricité - Transport

Électricité - Transport et distribution

Électricité - Fiabilité du réseau de transport

Électricité - Application des normes de fiabilité du réseau de transport

Électricité - Autres

Gaz naturel - Énergir

Gaz naturel - Enbridge Gaz Québec

Gaz naturel - Gazifère

Gaz naturel - Autres

Produits pétroliers

Transition énergétique Québec

Autres

Audiences en cours - Électricité - Fiabilité du réseau de transport

R-4349-2026

DPCMÉER - Demande d'adoption des annexes IRO-010-5-QC-2, MOD-032-1-QC-1, PRC-012-2-QC-2, TOP-003-6.1-QC-2 ET VAR-002-4.1-QC-2 – Alignement des définitions GO et GOP

R-4348-2026

DPCMÉER - Demande d'adoption de la norme de fiabilité PRC-030-1

R-4347-2026

DPCMÉER - Demande d'adoption des normes de fiabilité PRC-024-4 et PRC-029-1

Le processus de dépôt des normes à la Régie

Le déroulement à la Régie

Les grandes étapes d'un projet de norme:



Le déroulement à la Régie

Le traitement des dossiers

Mécanismes de traitement

Demandes de renseignements (DDR)

- Très fréquente
- Série de questions à répondre sur le dossier

Séance de travail

- Moins fréquent
- Clarifications à l’oral d’éléments du dossier avec les analystes du dossier

Audiences

- Rare
- Complexe et formel
- Devant le régisseur
- Questions posées par l’avocat de la Régie

Adoption de normes			
Nombre de normes soumises	OU	Complexité d'examen	Délai de traitement visé
1		<div></div> Faible	3 à 4 mois
2-5		<div></div> Moyenne	6 à 12 mois
Plus de 5		<div></div> Élevée	12 mois à 24 mois
Autres demandes			
Complexité d'examen		Besoin d'audience	Délai de traitement visé
<div></div> Faible	Oui ou non		3 à 4 mois
<div></div> Moyenne	Non		4 à 6 mois
	Oui		6 à 12 mois
<div></div> Élevée	Non		6 à 12 mois
	Oui		12 mois à 24 mois

Le processus de dépôt des normes à la Régie

Adoption de la norme

Les grandes étapes d'un projet de norme:



Dépôt à la Régie

Exemple : R-4314-2025 (PRC-002-5, PRC-028-1)

Émission d'une décision de la Régie:

Tout est public sur le site de la Régie:

<https://www.regie-energie.qc.ca/fr/participants/audiences-en-cours>

[67] Pour ces motifs,

La Régie de l'énergie :

ACCUEILLE la Demande du Coordonnateur;

ADOpte les normes de fiabilité PRC-002-5 et PRC-028-1 et leurs annexes Québec, dans leurs versions française et anglaise;

FIXE la date d'entrée en vigueur des normes de fiabilité PRC-002-5 et PRC-028-1 ainsi que leurs annexes Québec, dans leurs versions française et anglaise, au **1^{er} juillet 2026**;

RETIRE la norme de fiabilité PRC-002-4 et son annexe Québec, dans leurs versions française et anglaise, dès l'entrée en vigueur de la norme PRC-002-5;

FIXE au **17 février 2026** la date de dépôt des normes de fiabilité PRC-002-5 et PRC-028-1 et de leurs annexes Québec, dans leurs versions française et anglaise, adoptées et mises en vigueur dans la présente décision et modifiées afin d'y indiquer leurs dates d'adoption et d'entrée en vigueur, selon les ordonnances contenues à la présente décision, et en y ajoutant la référence à la présente décision à la section « Historique des versions »;

ADOpte le glossaire des termes et acronymes relatifs aux normes de fiabilité, dans ses versions française et anglaise;

FIXE la date d'entrée en vigueur du Glossaire adopté dans la présente décision, dans ses versions française et anglaise, au **1^{er} juillet 2026**;

ORDONNE au Coordonnateur de déposer, **au plus tard le 17 février 2026**, une version complète du Glossaire modifié selon les termes de la présente décision dans ses versions française et anglaise, en y ajoutant, à la section « Historique des versions », la référence à la présente décision, de même que sa date et les modifications adoptées;



Merci !

Présentation portant sur les changements finaux du *Programme de surveillance de la conformité et d'application des normes de fiabilité du Québec* (PSCAQ) et documentation des processus de surveillance et d'application

Laurentia Dumitrescu, ing.

Direction générale adjointe, surveillance et projets spéciaux
6 octobre 2026

Les commentaires et positions présentés dans ce texte
appartiennent à l'auteur et ne peuvent d'aucune façon
être imputés à la Régie de l'énergie

1. État de la situation
2. Changements au PSCAQ
3. Documentation et activités de sensibilisation
4. Prochaines étapes
5. Questions

- **Contrainte passée (entente en vigueur de 2022) :** Lors des modifications au PSCAQ, il fallait conclure une entente.
- **Flexibilité offerte par la Loi sur la Régie de l'énergie :**
 - « 85.4. La Régie peut, ~~avec l'autorisation du gouvernement~~ conformément à la loi, conclure une entente avec un organisme qui lui démontre son expertise dans les domaines de l'établissement ou de la surveillance de l'application des normes de fiabilité du transport d'électricité [...] »
- **À venir :** Signature d'une nouvelle entente qui prévoit les modalités de mise à jour du PSCAQ.

2. Changements au PSCAQ

4

Articles dont le contenu a été modifié (présentation antérieure) :

- Article 1.1 – Mise à jour du PSCAQ
- Article 1.2 – Définitions
- Article 2 – Registre
- Article 3 – Plan d'action (anciennement article 4 - pour arrimer avec le CMEP de l'Entreprise ERO)
- Article 4 – Processus de surveillance de la conformité
- Article 4.1 – Audits de conformité
- Article 4.4.1 – Enquête de conformité
- Article 4.6 – Journalisation d'une non-conformité à risque faible
- Article 4.9 – Évaluation préliminaire

2. Changements au PSCAQ

5

Articles modifiés depuis la dernière présentation :

- Article 5 – Application des normes
 - Nouveau processus pour la résolution des non-conformités à risque faible : exception à la conformité (« Compliance exception ») ;
 - ~~Abolition de la signification~~ Reprise de la transmission d'un avis de non-conformité possible à une entité visée.
- Article 5.4 – Projet de règlement
 - ~~Sanction proposée de moins de 1 million de dollars : le NPCC est en charge du processus de négociation. Délai de finalisation : 9 mois. Le NPCC doit fournir à la Régie des mises à jour trimestrielles ;~~
 - ~~Sanction proposée de plus de 1 million de dollars : la Régie est en charge du processus de négociation (mise à jour de la « Politique surveillance »).~~
 - Le NPCC négocie avec l'entité visée et une entente de règlement doit être conclue dans un délai de neuf (9) mois.

2. Changements au PSCAQ

6

- Article 6. Plans de redressement à des contraventions ou à des non-conformités
 - Obligation de l'entité visée de remédier la ou les non-conformités et de mettre en place des **mesures de redressement**.

Transition vers un processus moins formel : mesures de redressement plutôt que plan de redressement le formulaire pour mesures de redressement remplace celui du plan de redressement.

Le dépôt formel d'un plan de redressement est un processus laborieux :

- Approbation du plan de redressement par la Régie à la suite de la recommandation du NPCC.
- Obligation de l'entité visée de :
 - fournir des mises à jour sur l'avancement de la réalisation du plan de redressement ;
 - mettre en place les activités prévues dans le plan et respecter les dates butoirs.

2. Changements au PSCAQ

7

- Article 6.4 – Soumission du plan de redressement

- ~~Délai proposé :~~

- ~~90 jours pour la soumission d'un plan de redressement par une entité visée, lorsque demandé par la Régie ou le NPCC (aucun délai mentionné);~~
 - ~~6 mois après la réception d'un avis de non-conformité par une entité visée, si cette dernière ne conteste pas l'avis (au lieu de 30 jours);~~
 - ~~6 mois après la réception d'un avis de non-conformité par une entité visée, si cette dernière conteste l'avis (au lieu de 10 jours).~~

Une entité visée doit soumettre un plan de redressement dans les situations suivantes :

- a) à la demande de la Régie ou du NPCC ;
- b) dans les trente (30) jours suivant la signification de l'avis de non-conformité et en l'absence de mesures de redressement à la suite de la découverte de la non-conformité ;
- c) dans les dix (10) jours ouvrables après que la Régie détermine qu'il y a eu contravention et si l'entité visée n'a pas préalablement soumis de mesures de redressement ou de plan de redressement.

- Article 6.6 – Confirmation de réalisation du plan de redressement
 - ~~Aucune obligation d'un dirigeant de l'entité visée de remettre une déclaration attestant que toutes les mesures exigées par le plan de redressement ont été réalisées.~~
 - Un dirigeant de l'entité visée responsable de la réalisation du plan, ou son mandataire, doit remettre à la Régie ainsi qu'au NPCC une déclaration attestant que toutes les mesures exigées par le plan de redressement ont été réalisées.
- Article 7. Mesures correctives
 - Ajout d'une phrase pour indiquer que l'étape de consultation du coordonnateur de la fiabilité ne s'applique plus lorsque les mesures correctives sont imposées au coordonnateur lui-même.

■ Documentation

- Processus de journalisation d'une non-conformité à risque faible :
 - Type de document ciblé - *Guide de l'utilisateur du programme de journalisation d'une non-conformité à risque faible.*
 - Mise à jour du guide pour l'adapter au régime obligatoire de normes de fiabilité au Québec.
- Exception à la conformité :
 - Méthode de disposition d'une non-conformité à la discrétion de la Régie après recommandation du NPCC – absence de document élaboré par l'entreprise ERO.



• Sensibilisation auprès des entités visées

- Séances de formation
- Capsules informatives

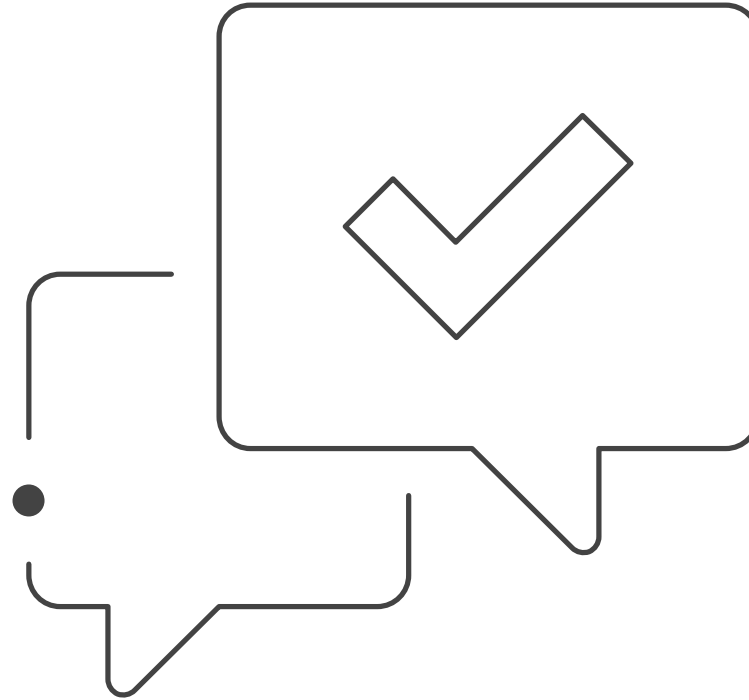
4. Prochaines étapes

10

- 4^e trimestre du 2026 - Publication du PSCAQ révisé
 - Réponses aux commentaires déjà reçus des entités visées
- 1^e trimestre du 2027 – Réponses aux commentaires des entités visées, le cas échéant
- Fin du 1^e trimestre du 2027
 - Signature de l'entente
 - PSCAQ mis en vigueur

Ressources :

Section ENTITÉS VISÉES - NORMES DE FIABILITÉ du site web de la Régie



Questions :

secretariat-PSCAQ@regie-energie.qc.ca

L'audit réglementaire – un levier d'amélioration continue



Michel Belhumeur, conseiller – Normes de fiabilité
Jonathan Trépanier, conseiller – Normes de fiabilité



Michel Belhumeur

Conseiller – Normes de fiabilité

Michel Belhumeur est conseiller en conformité aux normes de fiabilité chez Hydro-Québec. Diplômé en génie électrique de l'École Polytechnique de Montréal, il a travaillé depuis plus de trente ans dans diverses entreprises au maintien de systèmes qualité, à des enquêtes de conformité, et à l'amélioration de processus TI ou de la fiabilité. Il a notamment agi comme auditeur interne de la norme ISO 9001, du modèle CMMI et, à Hydro-Québec, réalisé des audits de sites.

Jonathan Trépanier

Conseiller – Normes de fiabilité



Jonathan Trépanier est conseiller en conformité au bureau de conformité aux normes de fiabilité à Hydro-Québec, spécialisé dans le volet de la sécurité physique (notamment les normes CIP-006 et CIP-014). Titulaire d'un baccalauréat en sécurité et études policières de l'Université de Montréal et certifié dans plusieurs domaines, dont l'audit de système de gestion, la gestion des mesures d'urgence et la sécurité physique, il œuvre depuis plus de 15 ans au sein d'Hydro-Québec dans diverses fonctions, dont la conformité aux normes de fiabilité. Ayant coordonné et accompagné l'organisation lors des récents audits réglementaires, il partage un retour d'expérience pratique visant à faire de l'audit un véritable levier d'amélioration continue.

1

**Retour sur le
déroulement d'un
audit
réglementaire**

Introduction aux différents types de surveillance

Type	Cadre	Préavis	Période	Contrôles	Questionnaires	Preuves
Audit de conformité	Régie (PSCAQ)	105 jours	Passée		QRSAW	
Déclaration sur la conformité	Régie (PSCAQ)	30 jours	Passée		Sur mesure	
Contrôles ponctuels	Régie (PSCAQ)	20 jours	Passée	Probable	Demandes d'informations (RFI)	Probable
Auto-certification	NPCC (CCEP)	S/O	Passée	S/O	Attestation	S/O
Revue de certification	NERC (Rules of procedure)	S/O	Future		Grille	

Légende :

PSCAQ – Programme de surveillance de la conformité et d'application de normes de fiabilité du Québec

NPCC – Northeast Power Coordinating Council

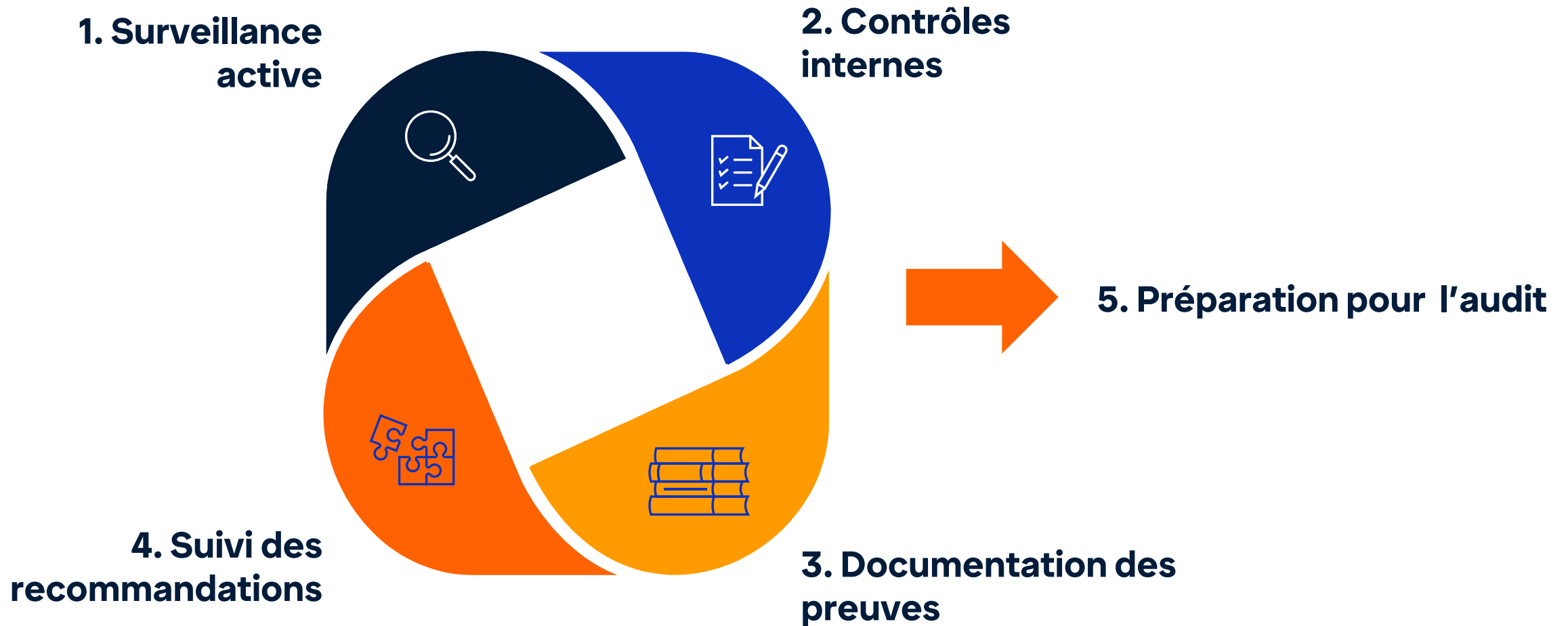
CCEP – Criteria Compliance and Enforcement Program

RFI – Request for Information

Exemple de déroulement – Audit HQ (NIR045) 2026



La préparation continue est le principal facteur de succès



2

**Conseils pour bien
se préparer**

Conseils pour bien se préparer: l'expérience d'Hydro-Québec

Liste d'experts matière ("SME")

- Par norme, par fonction NERC et par exigence
- SME principaux, SME spécialisés, de relève
- S'assurer que la liste est complète et mise à jour
- Rôles et responsabilités clairs

Exemples de formations pour les SME

- Stratégies de conformité et gestion du risque
- Contrôles internes
- Comment bien lire une norme de fiabilité
- Rédaction et maintien d'un QRS AW

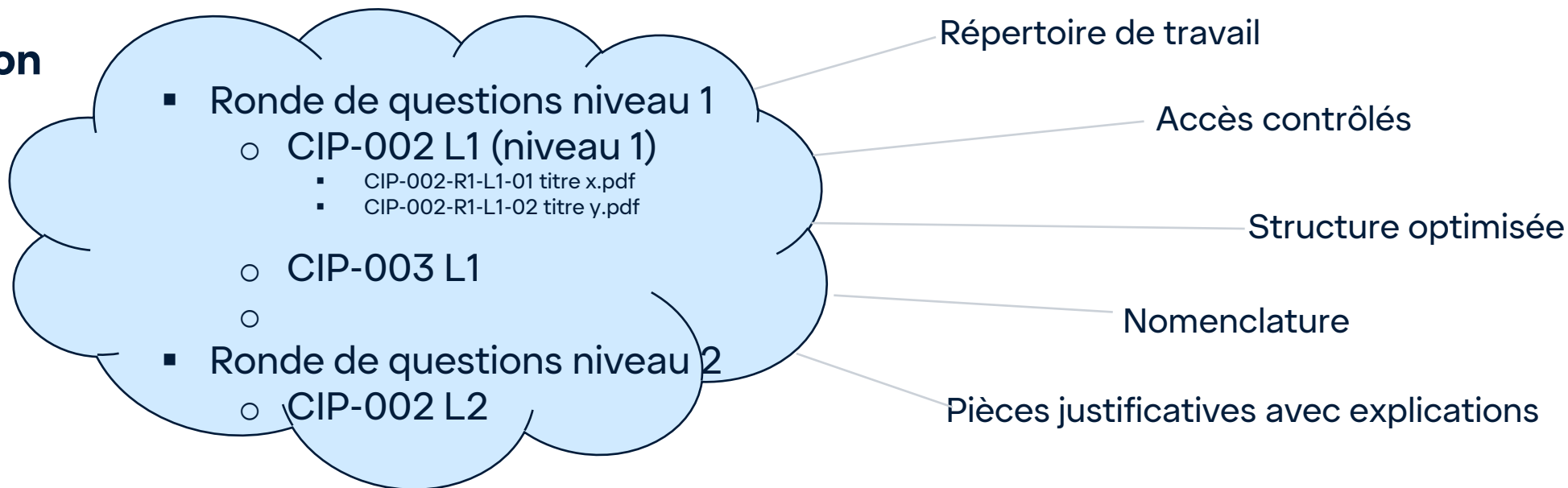
Guides à la disposition des SME

- Exemple, le Guide pour pièces justificatives



Conseils pour bien se préparer : l'expérience d'Hydro-Québec

Documentation



Être prêt



Derrière une simple demande : toute une organisation en action

Une demande paraît parfois simple :

- démontrer l'application d'un processus
- fournir les preuves associées à une exigence
- expliquer un contrôle
- démontrer le respect d'une norme sur une période donnée

Pour répondre adéquatement, il faut souvent :

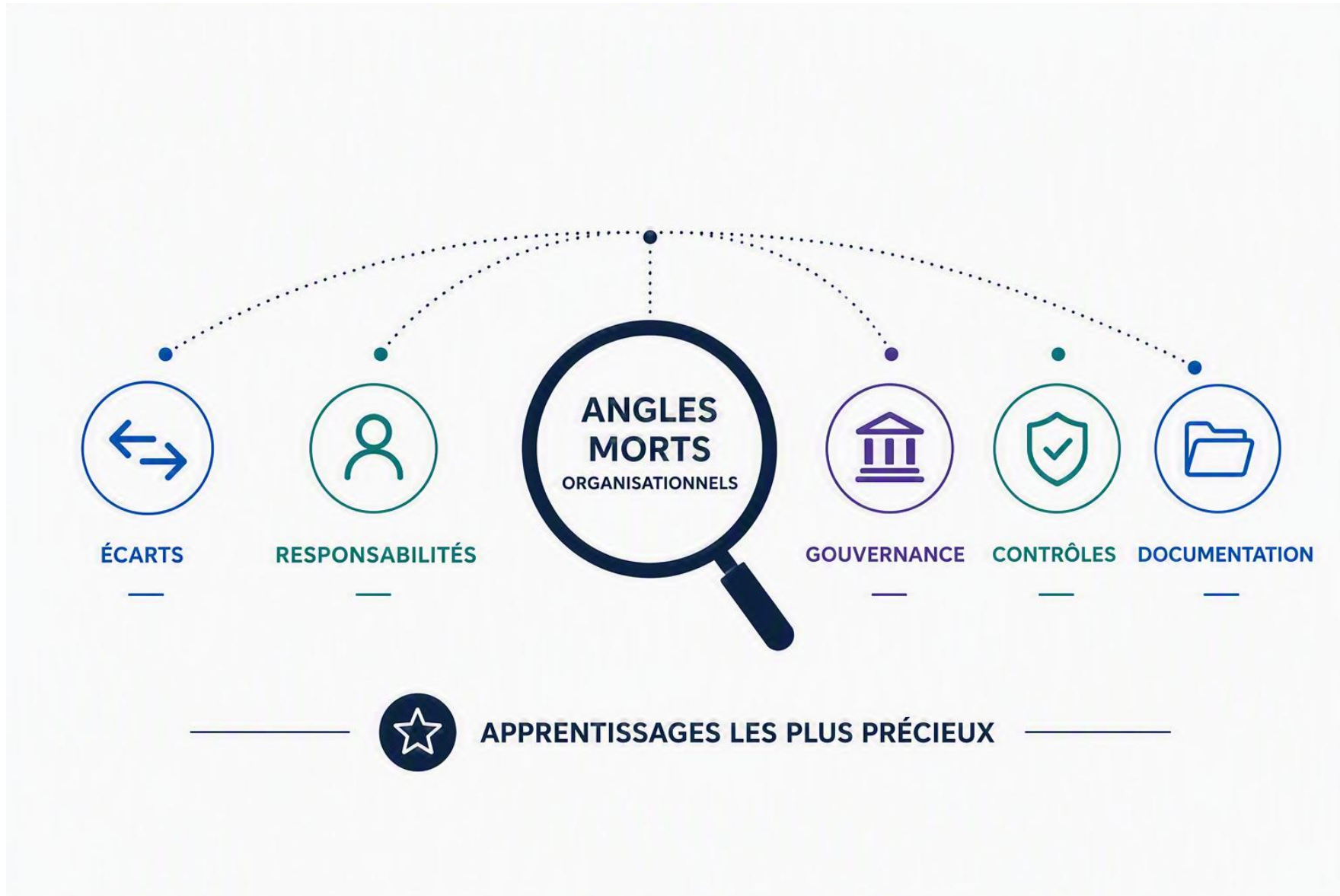
- solliciter plusieurs groupes
- consulter différentes bases documentaires
- reconstituer l'historique de certaines décisions
- valider plusieurs interprétations
- assurer la cohérence des réponses

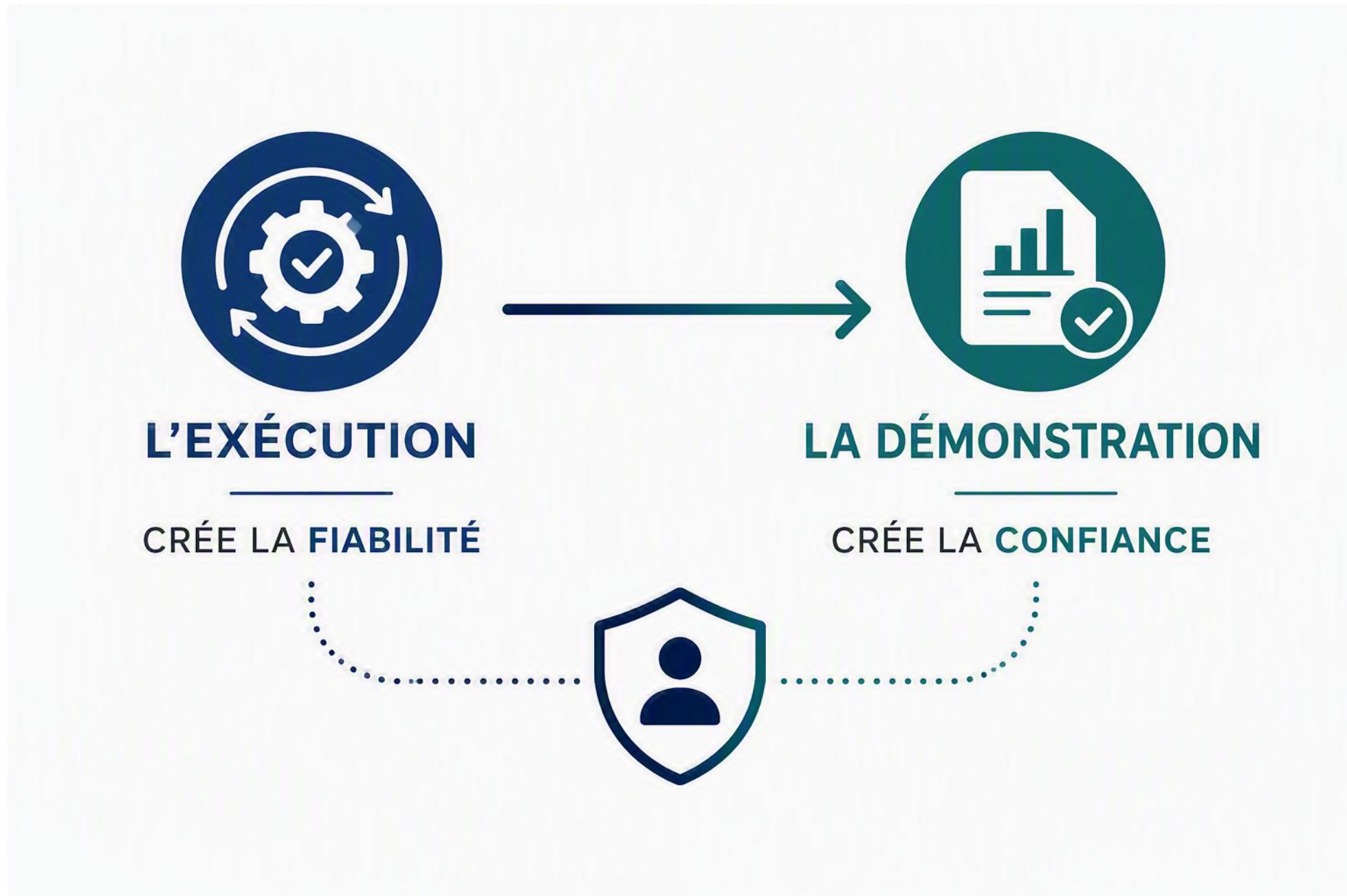


Au-delà de l'exécution : démontrer la conformité



Au-delà de la conformité : les véritables apprentissages de l'audit

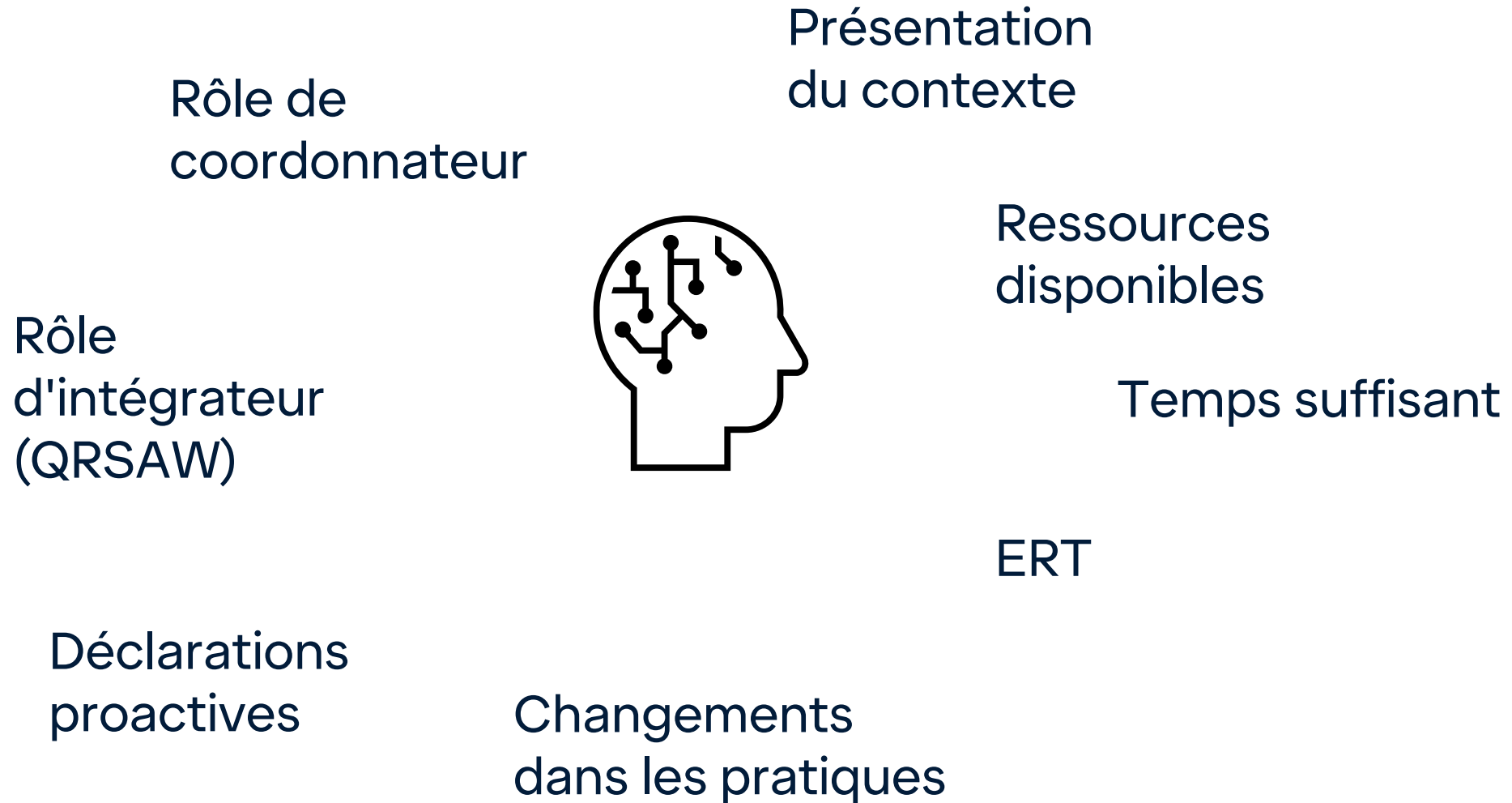




3

Leçons apprises

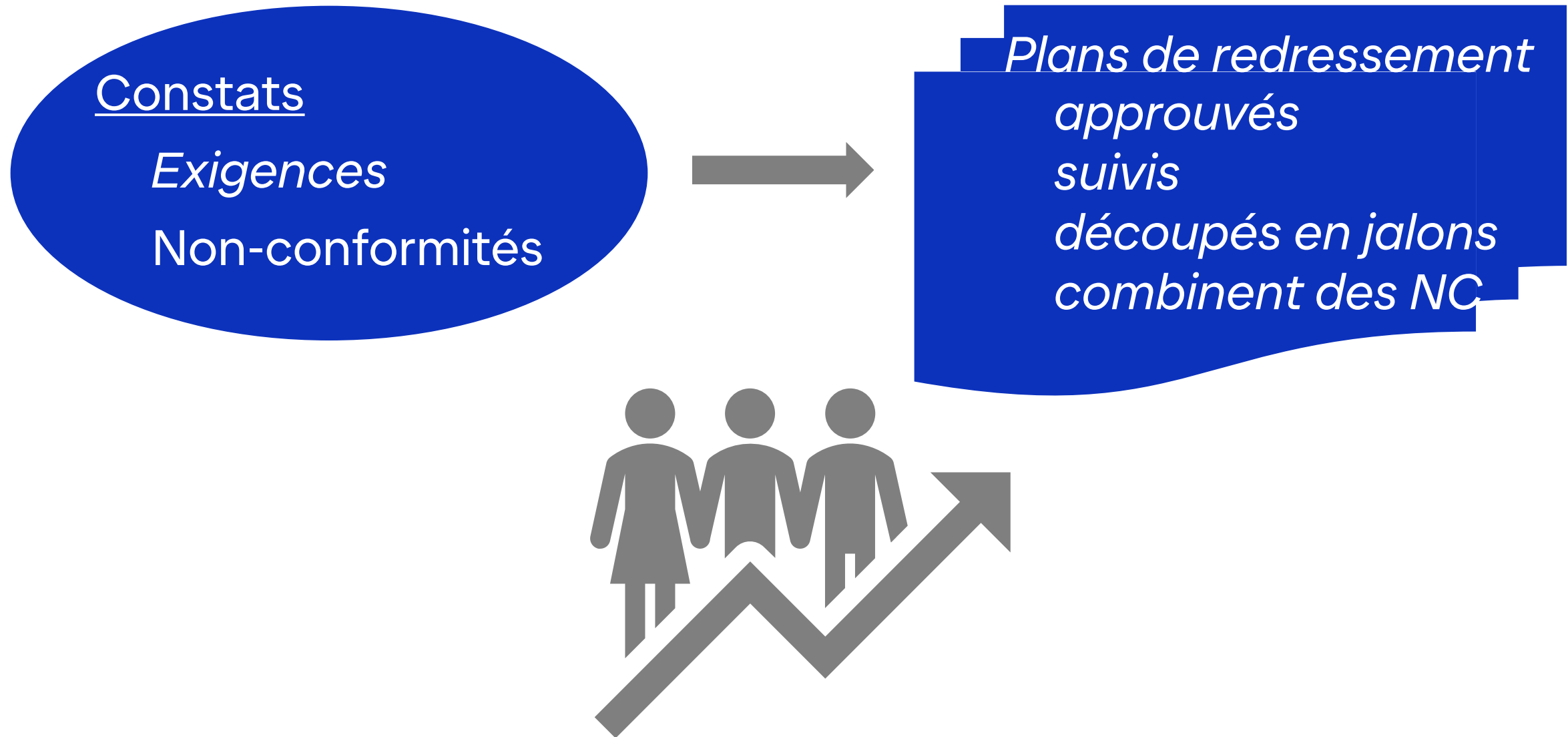
Quelques leçons apprises



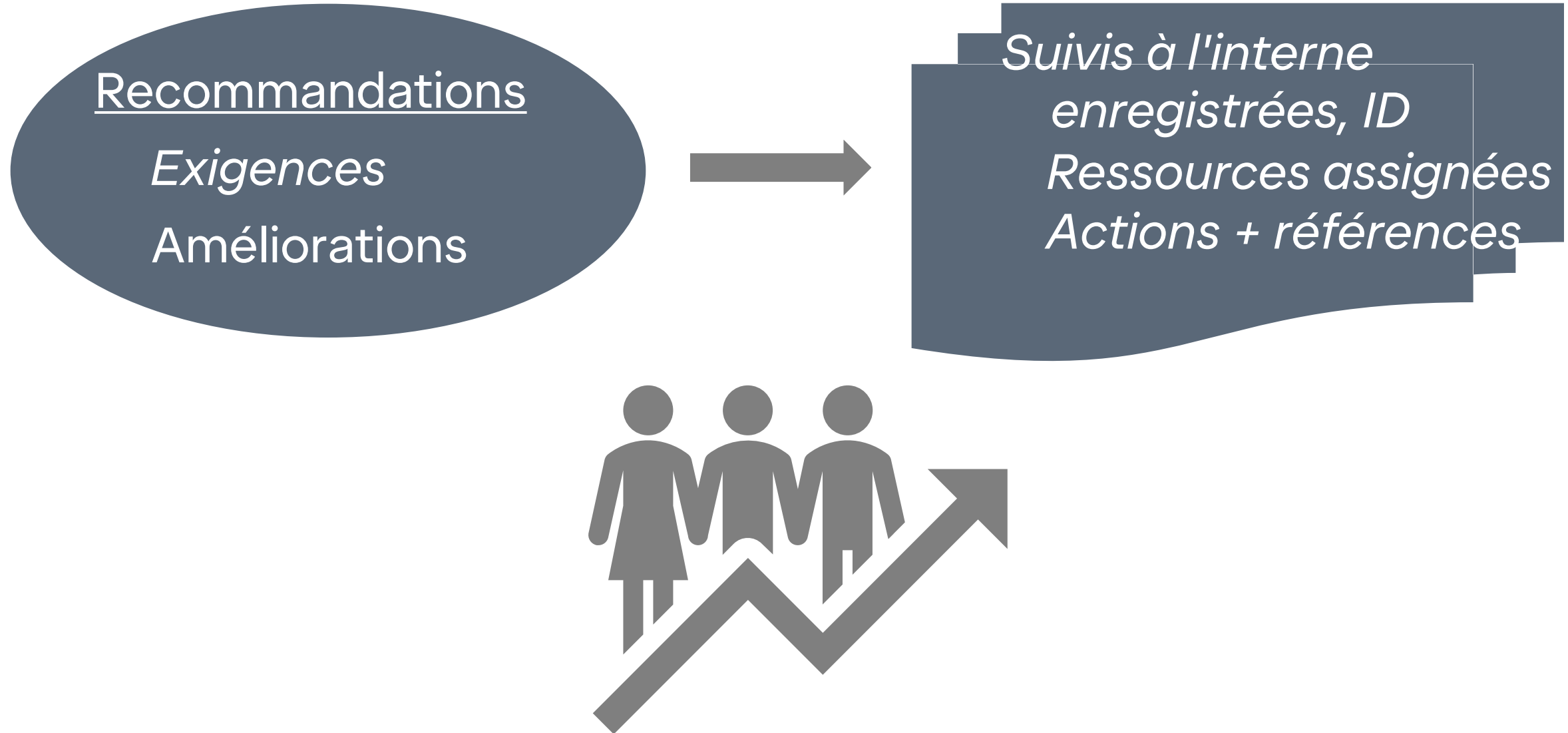
4

**En conclusion:
comment l'audit
réglementaire est
un levier
d'amélioration
continue ?**

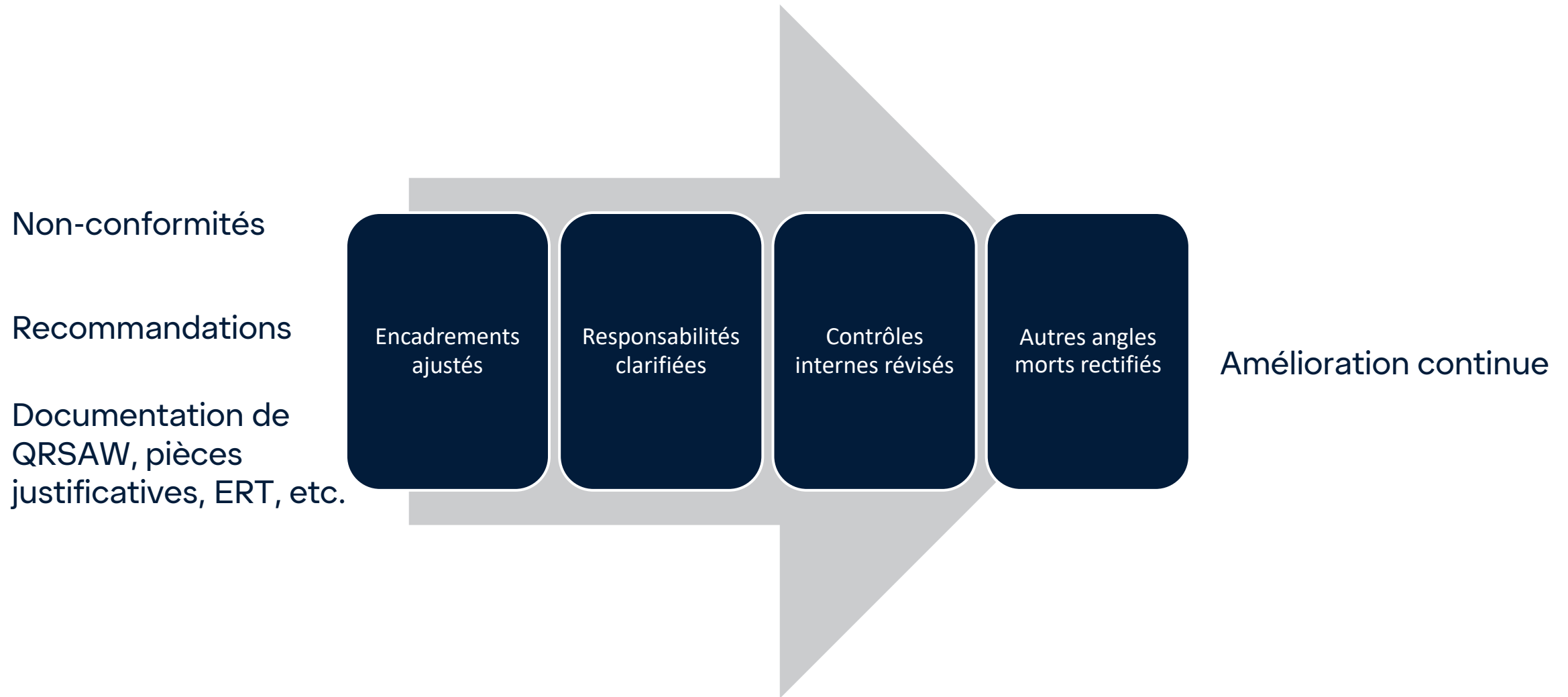
Un levier significatif : les constats



Un levier significatif : les recommandations



En somme, l'audit est un levier





Merci !

NERC Large Loads Action Plan

2026 Régie de l'Énergie Annual Reliability Seminar

Jack Gibfried
Engineer II, NERC

October 6, 2026

Recent Incidents: Voltage Sensitive Customer Initiated Load Reductions

Preliminary reports of a
~3,800 MW customer-
initiated load reduction
event on July 22, 2026



Eastern Interconnection Data Center Customer Initiated Load Reductions

- Jul 2024: 1,500 MW
- Feb 2025: 1,800 MW
- Feb 2025: 428 MW
- Mar 2025: 227 MW
- May 2025: 540 MW
- Jun 2025: 1,300 MW

Crypto Mining Customer Initiated Load Reductions

- Jan 2023 - Apr 2026:
 - 28 Loss Events (100-450 MW Load Loss)

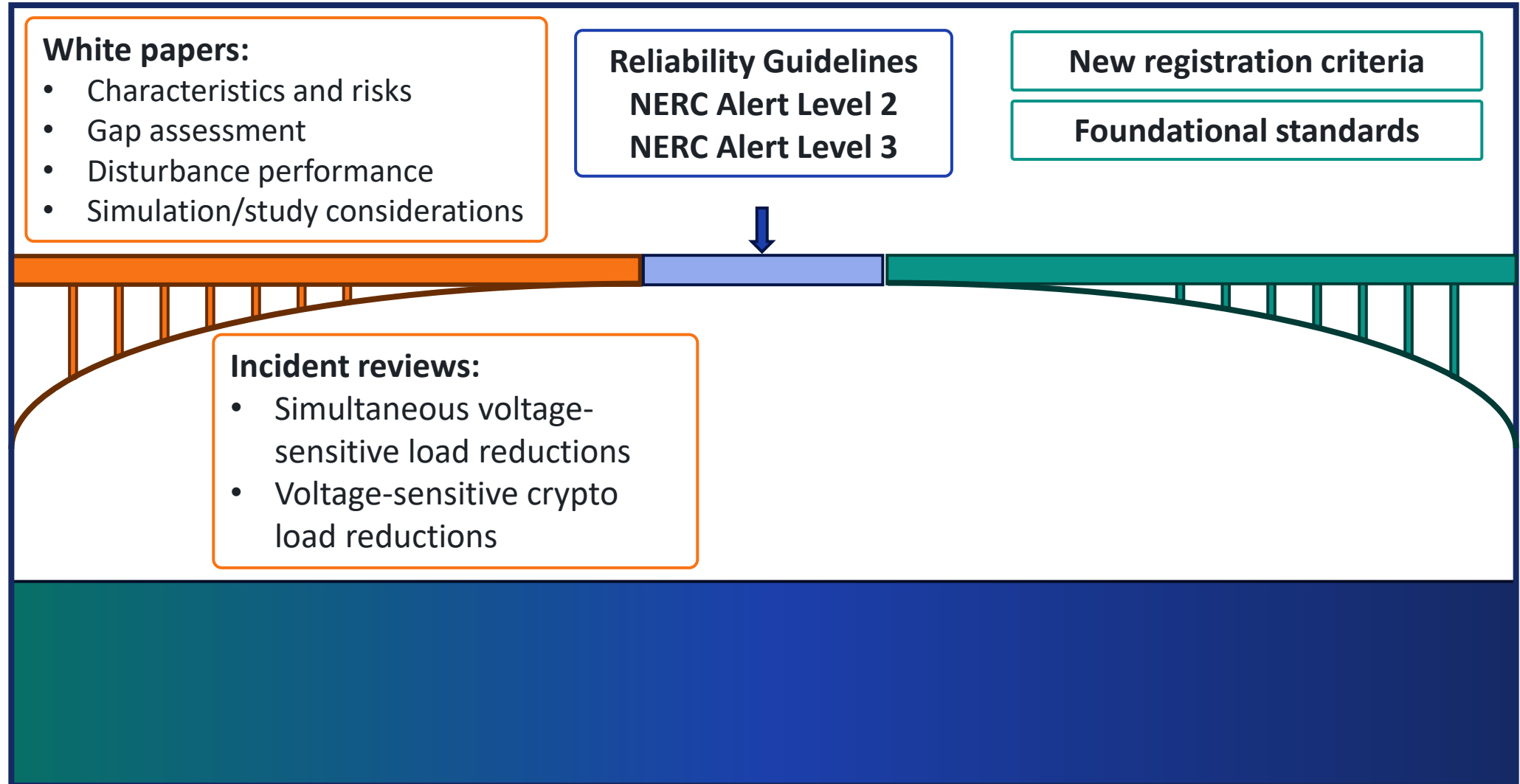
NERC Action Plan to Integrate Computational Loads **NERC**

- Updating registry criteria
- Developing Reliability Standards
- Technical resources, including:
 - White papers
 - Reliability guideline
 - NERC Alerts
 - Incident reviews
 - Collaborative workshops and roundtables



Large Loads Action Plan

Building the Bridge



NERC Large Loads Working Group

NERC

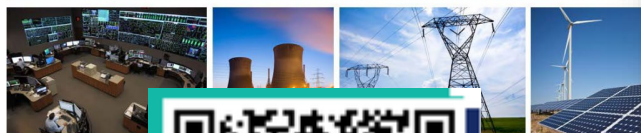
NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Characteristics and Risks of Emerging Large Loads

Large Loads Task Force White Paper

July 2025

RELIABILITY | RESILIENCE | SECURITY



3353 Peachtree
Suite 600, Nor
Atlanta, G
04-446-2560 | www.n



Characteristics and
Risks White Paper

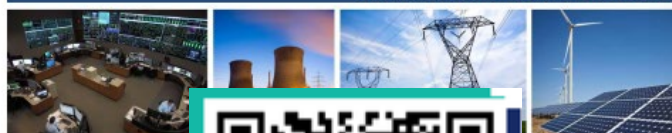
NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Assessment of Gaps in Existing Practices, Requirements, and Reliability Standards for Emerging Large Loads

NERC Large Loads Working Group White Paper

March 2026

RELIABILITY | RESILIENCE | SECURITY



Assessment of
Gaps White Paper

NERC

Final

Risk Mitigation for Emerging Large Loads

Large Loads Working Group Reliability Guideline

May 2026

RELIABILITY | R
POWERING TODAY.



Reliability Guideline

Reliability Guideline Best Practices

Category	Recommendation	LLE	DP	TO	TP	PC	TOP	BA	RC
Data Collection and Modeling	Provide steady-state, dynamic, and other data	P	L	L	SR	SR			
	Install high-speed FR, DDR, and SER	L	C	C					
	Provide high-speed recording data for post-event analysis	P	C	C	C	C	SR	SR	SR
	Provide updates to modeling data (as-built)	P	L						
	Provide real-time electrical measurements	P							
	Provide near-term demand forecasts	P							
	Perform model quality assessment, model verification, model validation	L							
Interconnection	Collect data and share with relevant entities	C	L						
	Study reliability impacts of new large load	C	C						
	Periodic near-term studies for collective impact of new large loads	C	C						
	Comprehensive commissioning process for large loads	C	C						
	Develop EMT screening criteria where needed	M	C						
Long-Term Planning	Study reliability impacts of new large load	C	C						
	Resource adequacy analysis considering unique risks of large loads	C	C						
C = Coordinate L = Lead M = Monitor P = Provide									
Category	Recommendation	LLE	DP	TO	TP	PC	TOP	BA	RC
Operations and Balancing	Verify communications (phone communications, telemetry, etc.)	C						SR	SR
	Integrate into operational systems (forecasting, outages, day-ahead studies)	C						SR	SR
	Conduct commissioning tests of the large load	C		C				SR	SR
	Post-commissioning testing and verification	C						SR	SR
	Provide real-time electrical measurements	P		P				SR	SR
	Provide near-term demand forecasts	P		C				SR	SR
	Specify data requirements for large loads real-time analysis and monitoring	C						SR	SR
	Prepare for largest expected load contingency (CILR, ramping, or other)	C			C	C		SR	SR
	Minimize variability via large load facility software mitigations	L						SR	SR
	Respond to operating instructions	L						SR	SR
Stability	Event analysis	C			L	L	L	L	L
	Define disturbance performance criteria based on studies	C	C	C	C	SR	C	C	SR
	Study and mitigate risks from CILR events	C	C	C	L	L	M	L	L
	Design and operate facilities to follow disturbance performance criteria	L	C	C	SR	SR	C	C	SR
Power Quality	Study, mitigate, and monitor power quality risks from large loads	C	M	L	L	C	C		C
Physical and Cyber Security	Holistic risk assessment	L							
	Implement security-by-design practices	L							
	Study and plan for operational interdependency between utility and large loads	C	C	C	C	C	C	C	L
	Implement physical security considerations	L							
Resilience	Implement cyber security considerations	L							
	Monitor any large loads involved in manual load shed, UFLS, and UVLS	C	C	C				L	L
	Consider integration of large loads into UFLS and UVLS schemes	C	L	L				L	L
C = Coordinate L = Lead M = Monitor P = Provide SR = Specify/Requirements									

Level 2 Alert Findings

NERC

Aggregated Report on NERC Level 2 Industry Recommendation: Large Load Interconnection, Study, Commissioning, and Operations

Summary
The Alert was published on September 9, 2025, and required Transmission Owners (TO), Resource Planners (RP), Transmission Operators (TOP), Transmission Planners (TP), Balancing Authorities (BA), Planning Coordinators (PC), Distribution Providers (DP), and Reliability Coordinators (RC) on the NERC Compliance Registry (NCR) to respond by January 28, 2026.

The purpose of the Alert was to recommend and encourage the following to facilitate the integration of large loads with the bulk power system (BPS) in a manner that supports continued reliability:

- TOs, in collaboration with relevant TPs, PCs, RCs, TOPs, and BAs, should establish clear facility design and performance criteria in their interconnection requirements for large loads.
- TPs and PCs should establish a comprehensive interconnection and system-wide study process to assess the reliability impacts of large loads.
- TOs should enhance their load commissioning activities to establish a comprehensive commissioning process that ensures operational readiness for large loads.
- TOs should establish operating protocols and the necessary communication infrastructure to support reliable ongoing operations after large load facilities enter into commercial operations.
- TPs, RPs, and PCs should, in consultation with their appropriate regulatory bodies, identify and implement a process to include large loads in their long-term transmission planning horizon demand forecasts as well as their near-term transmission planning horizon demand forecasts.

The full text of the Alert has been posted to the NERC website.¹ Responses to this Alert have informed NERC of the extent of the condition of the rapid and unprecedented rise in large electronic loads (sometimes also referred to as computational loads). Additionally, this Alert raised industry awareness of the potential reliability concerns associated with such large loads and provided recommendations to TOs, RPs, TOPs, TPs, BAs, PCs, DPs, and RCs to mitigate these concerns.

Background
The purpose of this Alert is to expeditiously address the risks observed from the analyzed large load behavior and assess the status of industry preparedness in relation to large loads.

As part of its normal course of business, NERC often either discovers, identifies, or is provided with information that is critical to ensuring the reliability of the BPS in North America. In order to effectively disseminate this information, NERC utilizes email-based "alerts" designed to provide concise, actionable information to the

¹ <https://www.nerc.com/globalassets/programs/ops/alerts/2025/nerc-alert-level-2-large-loads.pdf>

RELIABILITY | RESILIENCE | SECURITY

POWERING TODAY. PROTECTING TOMORROW.

- Many entities at the time of this Alert do not have:
 - Specific procedures to handle the unique challenges associated with large loads
 - A process to coordinate with TOs and DPs to establish protection coordination requirements for large loads.
- Many entities report waiting on or coordinating with a separate entity, primarily their ISO or RTO.



Level 2 Alert



Summary Report

Level 3 Alert Essential Actions

- Recommends seven near-term mitigation actions to address critical reliability risks to the bulk power system.
 - Follows on specific process findings from Level 2 Alert.
- Focus on models, studies, fault recording equipment, operations, protection, and control.

NERC

Essential Action to Industry

Computational Load Modeling, Studies, Instrumentation, Commissioning, Operations, Protection, and Control

Initial Distribution: May 4, 2026

The purpose of this Level 3 NERC Alert is to ensure Essential Actions are taken by registered entities to address the risks posed by existing and new computational loads¹ interacting with the bulk power system (BPS), inclusive of computational load interconnecting with collocated generation.²

NERC issued a previous Level 2 Alert Industry Recommendation: *Large Load Interconnection, Study, Commissioning, and Operations*³ that discussed the recommended practices that NERC deemed necessary to address the emerging risks from large loads. In the responses provided to the Alert, NERC found that entities generally did not have sufficient processes, procedures, or methods to address risks associated with computational loads. This contrasts with the robust historical experience with traditional non-power electronic non-computational load. As seen in the public report, NERC found specific deficiencies with the treatment of computational loads. Examples of this load include artificial intelligence training, cryptocurrency mining, and traditional data center uses.

As stated in the public report, NERC determined a set of immediate actions that registered entities should take to reduce the risk to the BPS that warrant issuance of this Level 3 alert. These actions relate to the modeling, study, installed fault recording or instrumentation, commissioning, operation, protection, and control of computational load.

NERC issues this Level 3 Alert for entities to implement specific changes⁴ to handle critical risks. Additional actions are discussed as part of NERC's Large Loads Action Plan and include the draft registry criteria⁵ and Standard Authorization Request (SAR) for computational load⁶ posted on NERC's website on April 1, 2026. Responses will also help

¹ NERC is currently working to register a "Computational Load Entity" for these loads. Currently, this would include loads that are 20 MW and greater, connected at 60kV, and contain more than 1 MW of IT Load. More information is available on NERC's [Rules of Procedure](#) webpage.

² Colocation with generation is one significant way computational load is interacting and using the BPS.

³ See [Aggregated Report on NERC Level 2 Industry Recommendation: Large Load Interconnection, Study, Commissioning, and Operations](#) to see the results of the previous Level 2 Alert.

⁴ As indicated in the public level 2 alert report, entities that do not have and do not expect to integrate computational loads within two years may not find it useful to implement these Essential Actions. These Essential Actions are for those entities that have or could expect to have computational loads or that may include these loads in the next two years. This includes entities that do not have computational load in their territory but could feasibly receive a request for one. Entities should implement these Essential Actions prior to receiving a computational load interconnection request.

⁵ More information is available on NERC's [Rules of Procedure](#) webpage.

⁶ More information is available on the [Project 2026-02](#) webpage.

RELIABILITY | RESILIENCE | SECURITY

POWERING TODAY.



Level 3 Alert

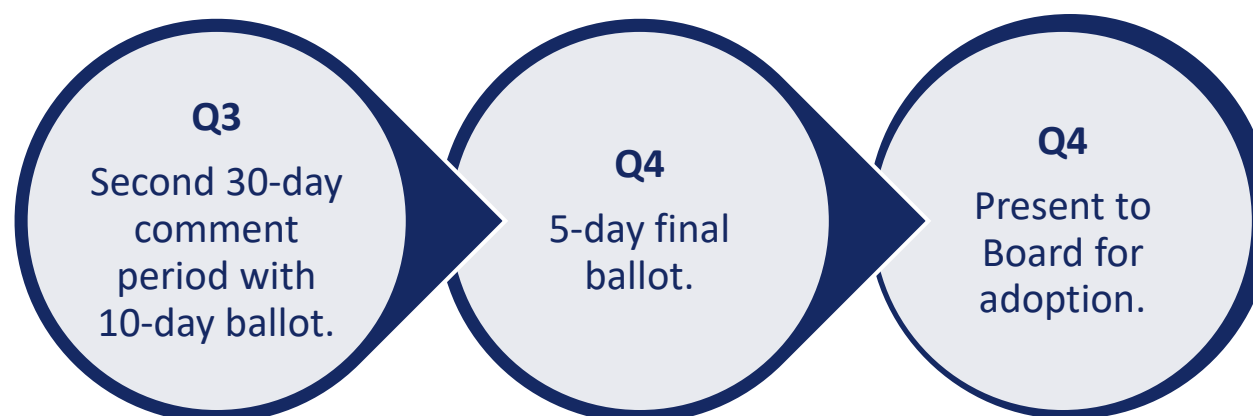
Registration Criteria for Large Loads

- NERC posted draft registry criteria for Computational Load Owners and Computational Load Operators.
- The criteria define the scope of what entities will be required to register with NERC and comply with NERC Reliability Standards.
 - Proposed threshold of 50 MW or more aggregated computational load supplied through electrical equipment connected at a voltage level greater than or equal to 100 kV.
- Rules of Procedure Revisions were posted for additional public comment during August 19 – September 18.



Draft Registry Criteria

- New and updated Reliability Standards will address computational loads in the Bulk Power System.
 - Some for existing registered entities, some for new computational load entities.
 - Proposed CLO-001, CLO-002, and CLO-003 standards based on requirements from previously approved Reliability Standards
- NERC posted draft new and updated standards for public comment for 30 days from August 19 to September 18, 2026.
 - Ten-day ballot occurred September 9 to September 18.
 - Final ballot October 9-14.



Project 2026-02

Large Loads Action Plan: 2026-2027

Q4 2026

- Request Board approval of registry criteria, glossary, and standard(s) (October)
- Seek a final ballot for CLO foundational standards (October)
- File registry criteria , glossary, and standard(s) (Fall, *subject to Board approval*)

Q1–4 2027

- Draft and file additional applicable Reliability Standards (*as needed*)
- File action plan detailing next steps to FERC (March)



A light blue map of the United States serves as the background. A thin vertical line runs through the center of the map, passing between the words "NERC" and "Discussion".

NERC

Discussion

Strategic Value of E-ISAC Information Sharing for Global Industry Resilience

2026 Annual Reliability Seminar by the Régie de l'énergie

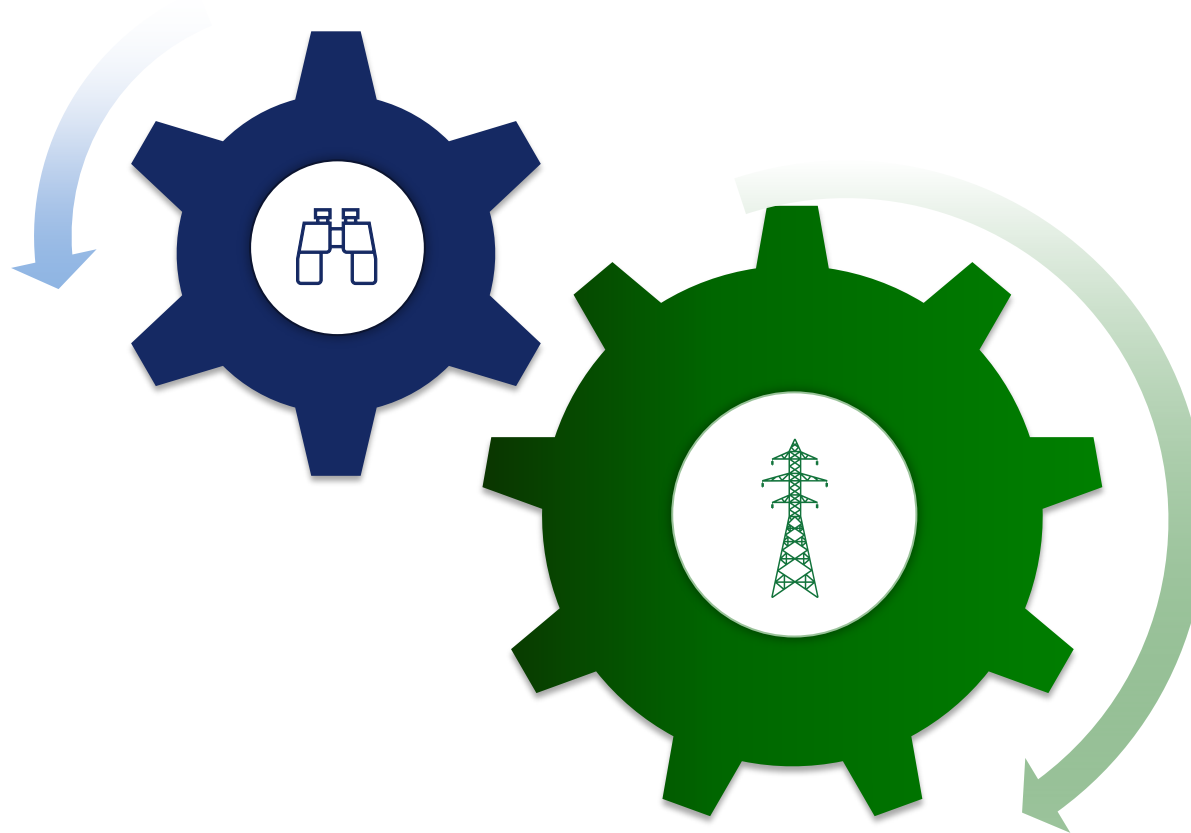
TLP:CLEAR

Lauren Gattone
Director, Security Operations

October 6, 2026

Vision

To be a world-class, **trusted** source for **quality analysis** and **rapid sharing** of security information for the electric industry



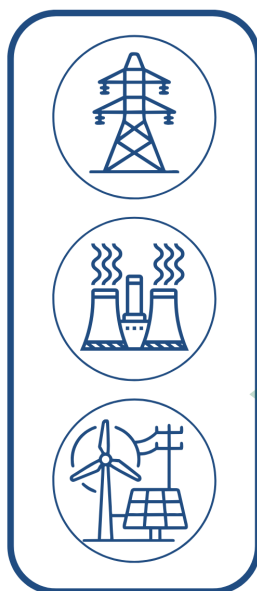
Mission

The E-ISAC reduces cyber and physical security risk to the electric industry across North America by providing unique insights, leadership, and collaboration

110+ Canadian and **28** International utility and partner organizations are part of the E-ISAC community

TRUSTED | SECURE | VOLUNTARY

INDUSTRY



Threat Intelligence
Situational Awareness
Analysis & Insights
Incident Coordination



GOVERNMENT



Threat Intelligence
Situational Awareness
Analysis & Insights
Incident Coordination

Threat Actors Targeting Critical Infrastructure



Nation States

China
Russia
Iran
North Korea



Criminal Groups

Increasingly AI-enabled
Ransomware/extortion
Increased OT interest

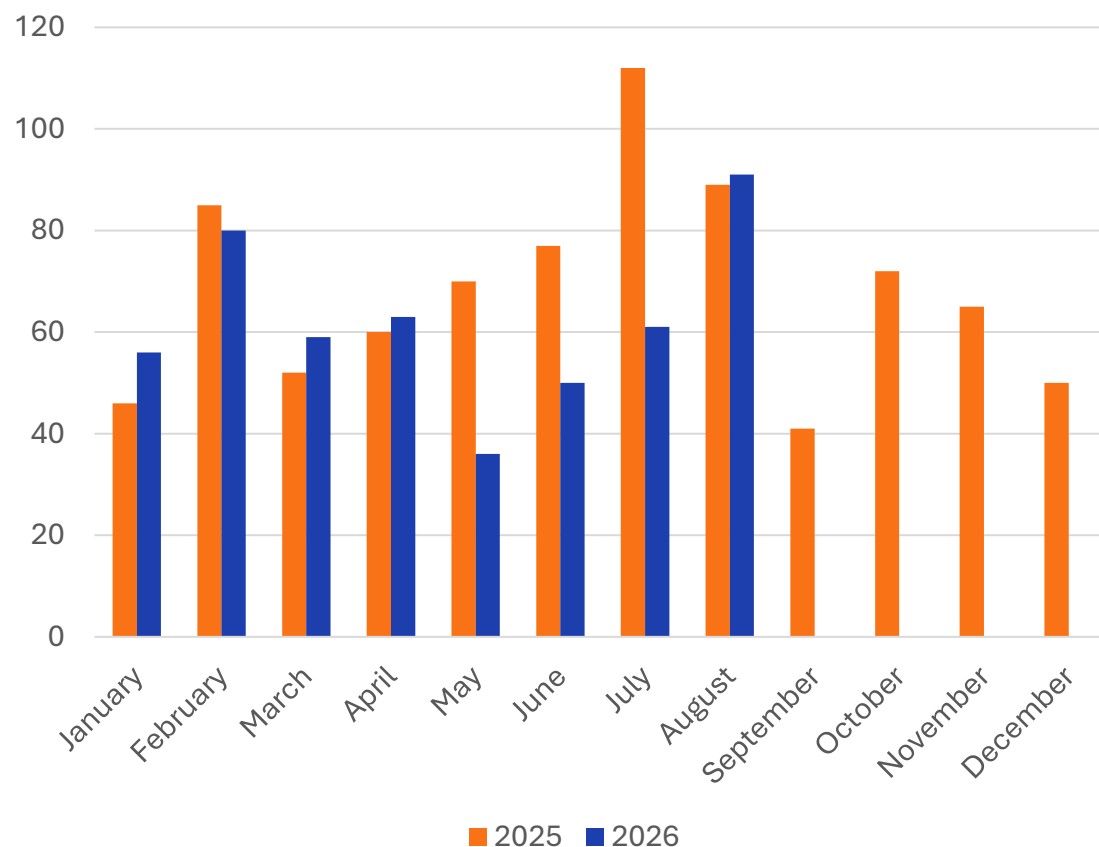


Extremists/ Activists

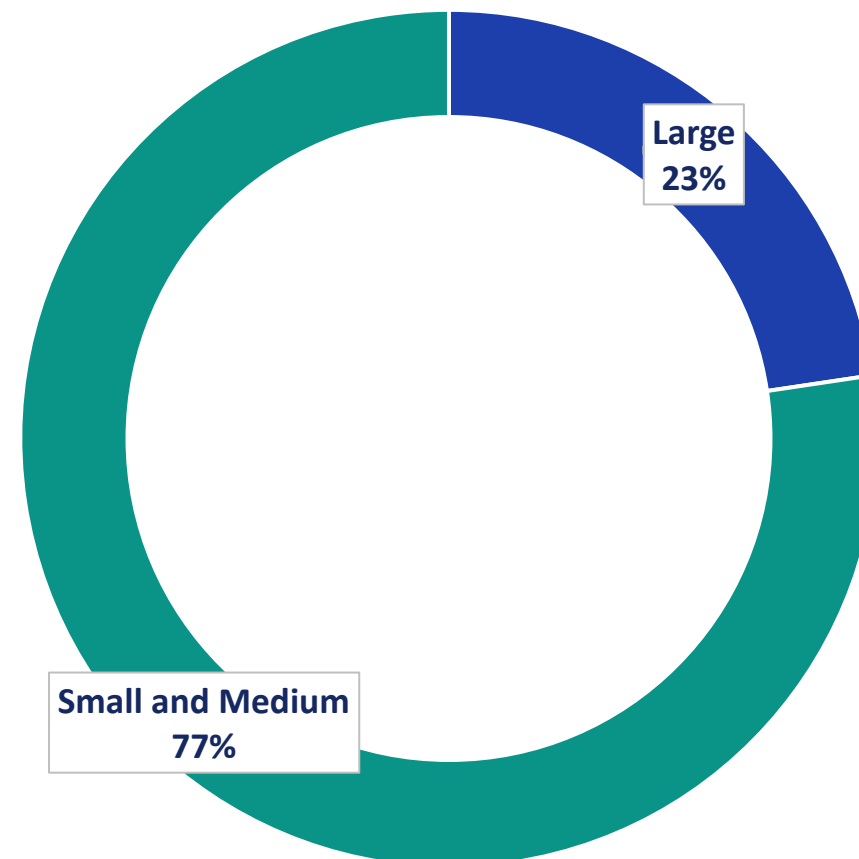
Cyber hacktivism
Threats related to data
centers and AI

Continuous targeting of vulnerable critical infrastructure

Direct Shares to E-ISAC Members



53 Direct Shares to Canadian Members



Theft Analysis & Forecasting

AT&T Offers \$10K Reward for Tips as Cable Theft Soars Alongside Copper Prices

Sarah Holzmam - Barchart - 1 hour ago Columnist



TLP: CLEAR

TLP: GREEN

Limited disclosure, recipients can spread this within their community.

Monthly Security Outlook Analysis

September 2026

This document provides analytical support to the September Monthly Outlook Executive Summary with in-depth analysis of historical physical security trends, a copper theft analysis and forecast, and a general threat landscape outlook for September. [Appendix A](#) provides an assessment of the July 2026 Monthly Physical Security Outlook. The E-ISAC is enhancing its forecasting methodology and is implementing an improved copper theft forecasting model. More details about the methodology and model used are provided in [Appendix B](#).

Cyclical Overview of Incidents Shared

Since 2016, members have shared 22,950 incidents with the E-ISAC. [Figure 1](#) provides an annual cyclical incident analysis to show the monthly breakdown of incidents shared since 2016. Based on the cyclical trend analysis, incidents tend to peak in late spring and summer before declining in the fall. For awareness, the increase in the 2022–2026 dataset (when compared to preceding years) can be mostly attributed to an increase in voluntary sharing with the E-ISAC. Throughout 2025, incident shares were lower than in 2024. This decreasing trend was observed across both mandatory reporting and voluntary sharing methods. Incidents shared thus far in 2026 continue to align with the observed cyclical trends, but the E-ISAC is closely monitoring these fluctuating patterns, including identifying and analyzing any correlation with general economic or seasonal trends.

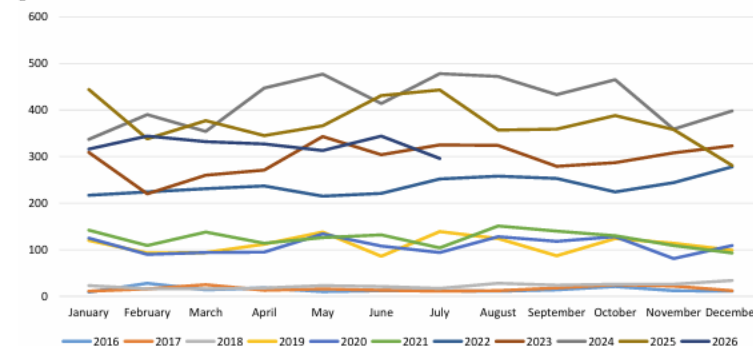


Figure 1: Cyclical Incident Trends (2016–July 2026)

RELIABILITY | RESILIENCE | SECURITY

POWERING TODAY. PROTECTING TOMORROW.

Key Programs Strengthening Grid Security

GridSecCon

Sector Collaboration

Connects industry and government leaders to exchange practical insights on emerging cyber and physical threats.

GridEx

Coordinated Preparedness

Exercises operational response, cross-sector coordination, and executive decision-making.

VISA and OT Mitigation

Physical and Cyber Risk Assessments

Helps utilities assess critical-asset vulnerabilities and prioritize risk-based security improvements.

- VISA leverages a design-basis threat methodology.
- OT Mitigation conducts site walks to help defenders think like attackers.

CRISP

Sector-Wide Cyber Threat Insight

Data is key to spotting trends against the sector.

- CRISP analyzes participant network data to identify threat patterns with government enrichment.

VISOR

Proactive Member Attack Surface Assessments

Leveraging open-source tools, identify and share directly with members any internet-facing vulnerabilities, misconfigurations, and exposures.



Takeaways

CONVENE – Bring utilities, emergency management, regulators, state leadership together before a crisis happens.

UNDERSTAND – Visit facilities, understand security investments, learn operational realities utilities face.

REINFORCE – Champion security investments that strengthen grid reliability and resilience.

EXERCISE – Participate in GridEx, workshops, other preparedness activities so relationships are established before they are needed.



24/7 Operations Center

operations@eisac.com

Membership Questions

memberservices@eisac.com

Speaker Requests

speakerrequests@eisac.com

Vendor Affiliate Program

vendorprogram@eisac.com

CRISP

crisp@eisac.com

Follow Us





E-ISAC | **Discussion**

Aperçu des activités du comité d'utilisation des sanctions

Séminaire annuel sur la
fiabilité
6 octobre 2026

Les commentaires et positions présentés dans ce texte
appartiennent à l'auteur et ne peuvent d'aucune façon
être imputés à la Régie de l'énergie

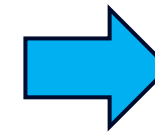
- Formation continue des entités visées
 - Séminaire annuel sur la fiabilité
 - Programme de soutien à la formation
 - Capsules vidéo
 - Traduction de documents de références
- Recherche & innovation
 - Programme de soutien aux projets de recherche collaborative
 - Programme de bourses d'études
- Visitez notre page dédiée
- Nouvelle infolettre

Séminaire annuel sur la fiabilité

- Évènement phare de la Régie en matière de fiabilité du transport d'électricité
- 6^e édition
- Format en constante évolution
- Sujets de présentation d'intérêt général
- Ouverture aux suggestions : répondez à notre sondage pour soumettre vos idées!



Édition 2021



Édition 2026

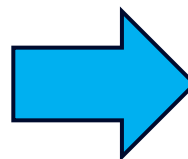
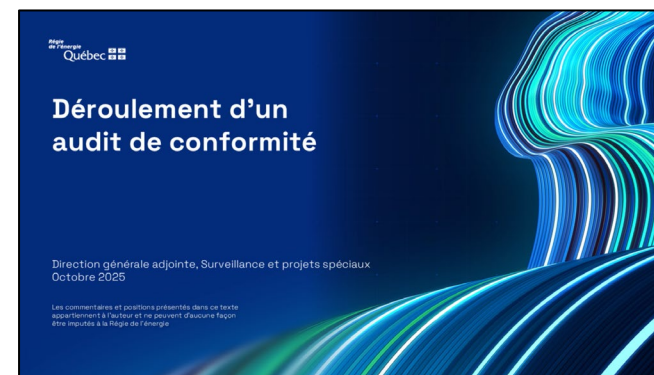


Programme de soutien à la formation

- Offres annuelles depuis 2022 pour l'inscription à des formations spécialisées et conférences
- Restez à l'affut : une nouvelle opportunité de formation en Q1 2027

Capsules vidéo

- Tutoriels vidéo sur les processus opérationnels du régime obligatoire
- Sur un élan : 3 capsules publiées depuis 2025 et 3 nouvelles capsules en cours de production.
- Un endroit pour toutes les consulter : [Formation continue](#)



Traduction de documents de références

- Nouvelle initiative : 11 documents publiés en français et 3 autres documents en cours de traduction
- Sélection de documents pertinents aux entités visées par les normes
- Consultez la nouvelle [page](#) dédiée sur le site web de la Régie
- Ouverture aux suggestions : répondez à notre sondage pour soumettre vos idées!

Vos commentaires nous guident!

Documents traduits

Les documents ci-dessous constituent des **traductions françaises non officielles** de documents publiés par divers organismes. Ces traductions sont fournies **à titre d'information seulement**.

AVIS DE NON-RESPONSABILITÉ

*Les présents documents n'ont aucune portée légale ou réglementaire dans le cadre du régime obligatoire de normes de fiabilité du Québec. Ainsi, la **Régie de l'énergie ne peut garantir l'exactitude, l'exhaustivité ou la mise à jour** de ces documents traduits. En cas de divergence entre un document traduit et sa version originale, **cette dernière prévaut**.*

[GUIDE SUR LA DÉCLARATION DE NON-CONFORMITÉ ET LE PLAN DE REDRESSEMENT POUR LES ENTITÉS VISÉES](#) ↓

Description : Ce guide vise à accompagner les entités visées dans leurs déclarations de non-conformités et l'établissement de plans de redressement. Il précise la nature des renseignements devant être fournis par l'entité.

Source : NERC. (Décembre 2025). *Registered Entity Self-Report and Mitigation Plan User Guide* [Guide sur la déclaration de non-conformité et le plan de redressement pour les entités visées] (Traduction française). Régie de l'énergie. (Travail original publié en 2024).

[Version originale](#) ↓

Extrait de la nouvelle page

Programme de soutien aux projets de recherche collaborative

- Reconduction en 2025 du programme FiabilitÉÉ en collaboration avec InnovÉÉ
- Pour stimuler et accélérer le développement d'innovations en liant expertises et ressources entre partenaires industriels et établissements de recherche
- À venir: Communiqué de presse pour l'annonce des résultats



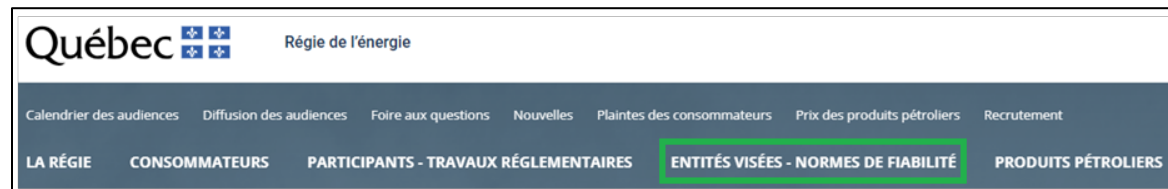
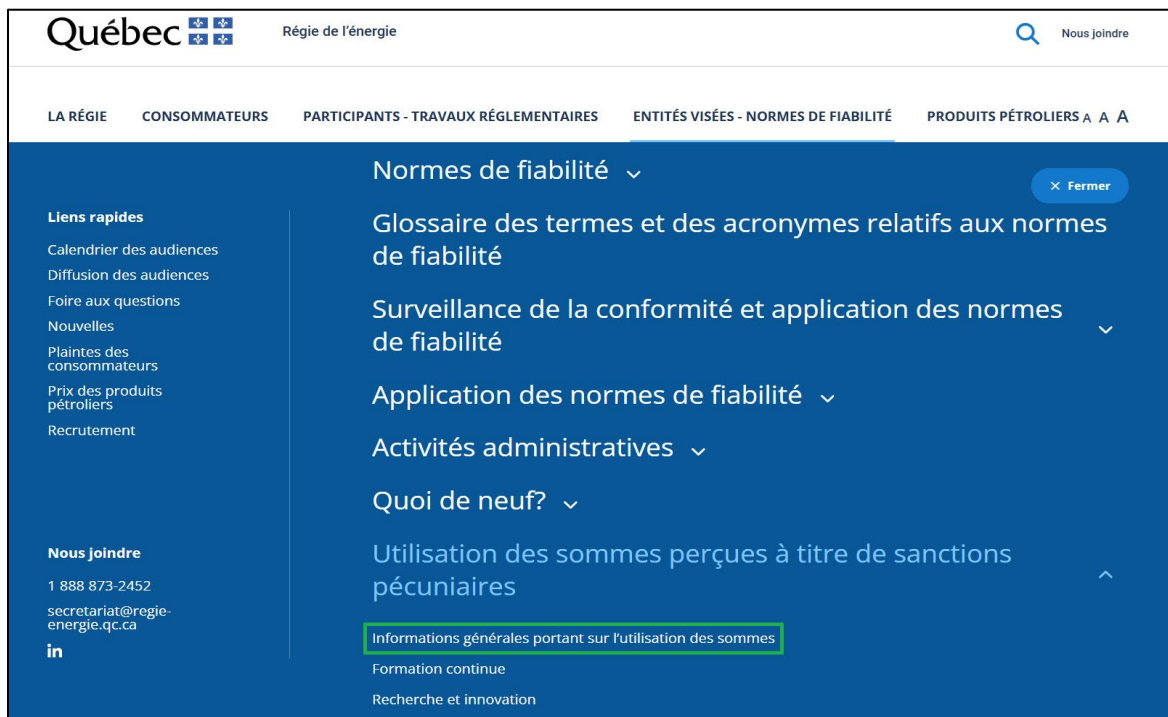
Programme de bourses d'études

- Lancement du 5^e concours en 2026 en collaboration avec le Fonds de recherche du Québec (FRQ)
- Projets de recherche s'inscrivant dans la fiabilité du transport d'électricité (niveau maîtrise)
- Visionnez les capsules *Mon projet de recherche en 1 minute*: [Bourses](#)



Visitez notre page dédiée

7



Informations générales portant sur l'utilisation des sommes

Partager la page

Utilisation des sommes perçues à titre de sanctions pécuniaires

[Informations générales portant sur l'utilisation des sommes](#)

[Formation continue](#)

[Recherche et innovation](#)

English version

En vertu de la *Loi sur la Régie de l'énergie* (la **Loi**), la Régie possède, entre autres fonctions, celle d'adopter et mettre en vigueur les normes de fiabilité applicables au réseau de transport d'électricité au Québec.

Lorsqu'une entité visée contrevient à une ou plusieurs normes de fiabilité, la Régie peut, après avoir déterminé qu'il y a eu contravention par l'entité, imposer à cette dernière une sanction maximale de 500 000 \$ par jour.

Les montants des sanctions imposées par la Régie à la suite d'une ou plusieurs non-conformités aux normes de fiabilité, doivent, conformément à l'article 85.11 de la **Loi**, être versés dans un compte distinct aux fins de s'assurer de la fiabilité du transport d'électricité.

Afin de bien encadrer l'utilisation de ces sommes, la Régie a adopté la [Politique sur la gestion des montants perçus à la suite de l'imposition d'une sanction pécuniaire](#) qui prévoit trois axes d'intervention possibles en cette matière :

1. La [formation continue](#) des entités visées par les normes de fiabilité du réseau de transport d'électricité au sujet de la fiabilité du transport d'électricité.
2. La [recherche et l'innovation](#) dans le domaine de la fiabilité du transport d'électricité, comprenant, notamment, le soutien financier à la recherche fondamentale et appliquée.

Formation continue

Partager la page

Utilisation des sommes perçues à titre de sanctions pécuniaires

[Informations générales portant sur l'utilisation des sommes](#)

[Formation continue](#)

[Recherche et innovation](#)

Les activités financées par la Régie dans le cadre de l'axe relatif à la formation continue des entités visées par les normes de fiabilité du réseau de transport d'électricité au sujet de la fiabilité du transport d'électricité sont les suivantes:

English version

Séminaires sur la fiabilité	+
Soutien à la formation	+
Traduction	+
Capsules informatives	+

Recherche et innovation

Partager la page

Utilisation des sommes perçues à titre de sanctions pécuniaires

[Informations générales portant sur l'utilisation des sommes](#)

[Formation continue](#)

[Recherche et innovation](#)

Les activités financées par la Régie dans le cadre de l'axe relatif à recherche et l'innovation dans le domaine de la fiabilité du transport d'électricité, lequel comporte, notamment, le soutien financier à la recherche fondamentale et appliquée, sont les suivantes :

English version

Soutien financier aux projets de recherche	+
Bourses	+

Nouvelle infolettre

9

Découvrez notre nouvelle infolettre pour recevoir les dernières nouvelles du régime obligatoire des normes.

Pour ne rien manquer, abonnez-vous en consultant la page « [Quoi de neuf?](#) ».

S'abonner



Nouvelles sur les normes de fiabilité du transport de l'électricité



S'abonner

Quoi de neuf : Le régime obligatoire de normes de fiabilité au Québec

1er octobre 2026



Faits Saillants :

◆ Normes de fiabilité en vigueur

Les normes de fiabilité FAC-003-5, FAC-011-4, FAC-014-3, IRO-008-3, PRC-023-6, PRC-026-2, TOP-001-6 entrent en vigueur le 1^{er} octobre 2026. Pour les consulter : [Normes de fiabilité en vigueur](#)

◆ Nouvelle norme de fiabilité : CIP-015-1

Une nouvelle norme de fiabilité relative à la protection des infrastructures critiques ainsi que son annexe Québec font leur entrée dans le régime obligatoire de normes au Québec : CIP-015-1 porte sur la surveillance de sécurité de réseau interne. Pour la consulter : [Normes de fiabilité en vigueur à une date ultérieure](#)

◆ De nouvelles ressources documentaires disponibles en français

Quatre nouvelles ressources externes ont été traduites en français et mises à la disposition des entités visées :

- Entreprise ERO – Guide sur les contrôles internes
- Facteurs de risque et catégories de risque de l'Entreprise ERO
- Guide d'utilisation du codage des causes de l'Entreprise ERO
- Mise à jour de l'outil de demande de preuves pour les normes CIP V9.0

Pour les consulter : [Ressources externes](#)

◆ Consulter tous les détails

Pour plus de détails ou pour prendre connaissance de l'ensemble des modifications, rendez-vous à la page [Quoi de neuf](#)

Extrait de l'infolettre

Merci et à la prochaine!