Journal officiel
de l'Union européenne

FR
Série C

C/2026/5593

6.11.2026

RECOMMANDATION DE LA COMMISSION

du 29 octobre 2026

sur les lignes directrices relatives à la continuité opérationnelle et aux tests de résistance pour les points de contact nationaux dans le cadre du mécanisme de protection civile de l'Union

(C/2026/5593)

LA COMMISSION EUROPÉENNE,

vu la décision nº 1313/2013/UE du Parlement européen et du Conseil du 17 décembre 2013 relative au mécanisme de protection civile de l'Union ([1]), et notamment son article 7,

considérant ce qui suit:

(1) Aux termes de l'article 196, paragraphe 1, point b), du traité sur le fonctionnement de l'Union européenne (TFUE), l'Union vise à promouvoir une coopération opérationnelle rapide et efficace à l'intérieur de l'Union entre les services de protection civile nationaux.

(2) L'Union dispose d'une compétence d'appui dans le domaine de la protection civile, comme indiqué à l'article 6, point f), du TFUE.

(3) Le mécanisme de protection civile de l'Union (ci-après le «MPCU»), institué par la décision nº 1313/2013/UE, vise à renforcer la coopération entre l'Union et les États membres et à faciliter la coordination dans le domaine de la protection civile en vue de rendre plus efficaces les systèmes de prévention, de préparation et de réaction en cas de catastrophes naturelles ou d'origine humaine.

(4) L'Union a connu plusieurs événements extrêmement perturbateurs ces dernières années, notamment les conséquences de la pandémie de COVID-19, la guerre d'agression menée par la Russie contre l'Ukraine, la panne informatique majeure de 2024, la tempête Éowyn en Irlande en janvier 2025 et la panne de courant de 2025 dans la péninsule Ibérique. Les événements perturbateurs peuvent empêcher ou retarder le fonctionnement des systèmes de protection civile, qui devraient rester opérationnels 24 heures sur 24 et 7 jours sur 7.

(5) L'article 7 de la décision nº 1313/2013/UE dispose que le centre de coordination de la réaction d'urgence (ci-après l'«ERCC») est opérationnel 24 heures sur 24, 7 jours sur 7, et est au service des États membres et de la Commission pour la réalisation des objectifs du mécanisme de l'Union. L'article 3 de la décision d'exécution (UE) 2025/704 de la Commission ([2]) précise en outre que chaque État membre désigne un point de contact national (PCN), disponible 24 heures sur 24 et 7 jours sur 7, pour la liaison avec l'ERCC.

(6) La recommandation de la Commission du 8 février 2023 relative aux objectifs de l'Union en matière de résilience face aux catastrophes ([3]) invite l'ERCC et les autorités de protection civile des États membres et des États participant au MPCU à améliorer, dans le cadre de leurs mandats respectifs, leurs capacités de planification de la continuité des activités. Elle précise également que le MPCU «devrait soutenir la réalisation de tests de résistance afin de contrôler la continuité des activités des centres d'opérations d'urgence, et collaborer avec les États membres au suivi à donner aux enseignements tirés et aux recommandations». Les tests de résistance des centres d'opérations d'urgence dans toute l'Europe ont constitué l'initiative phare de l'objectif numéro 5, intitulé «protéger, en se dotant d'un système de protection civile solide», comme souligné dans la communication de la Commission sur les objectifs de l'Union européenne en matière de résilience face aux catastrophes ([4]).

([1]) JO L 347 du 20.12.2013, p. 924, ELI: http://data.europa.eu/eli/dec/2013/1313/oj.
([2]) Décision d'exécution (UE) 2025/704 de la Commission du 10 avril 2025 fixant les modalités de mise en œuvre de la décision nº 1313/2013/UE du Parlement européen et du Conseil relative au mécanisme de protection civile de l'Union et abrogeant les décisions d'exécution 2014/762/UE et (UE) 2019/1310 de la Commission (JO L, 2025/704, 15.4.2025, ELI: http://data.europa.eu/eli/dec_impl/2025/704/oj).
([3]) JO C 56 du 15.2.2023, p. 1.
([4]) Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions «Objectifs de l'Union européenne en matière de résilience face aux catastrophes: agir de concert pour faire face aux futures urgences», COM(2023) 61 final du 8.2.2023.

(7) Ces efforts sont alignés sur d'autres cadres visant à renforcer la résilience, notamment la stratégie européenne pour une union de la préparation ([5]) et les exigences de base de l'OTAN en matière de résilience des pays ([6]). Plus précisément, l'action 51 de la stratégie appelle à adopter «des lignes directrices pour la "simulation de crise" destinée à tester la réaction d'urgence et les centres de crise dans l'ensemble de l'UE».

(8) Dans ce contexte, il est nécessaire de se focaliser sur la continuité opérationnelle des PCN dans le cadre du MPCU et d'accroître leur résilience afin qu'ils puissent rester opérationnels lors d'événements perturbateurs, en renforçant leurs plans et pratiques de continuité opérationnelle au moyen d'évaluations et de tests de résistance systématiques.

(9) En outre, les capacités de réaction qui pourraient être mises à disposition, sur demande, dans le cadre d'une intervention par l'intermédiaire du MPCU peuvent ne pas relever de l'autorité du PCN. Assurer la communication avec les entités qui gèrent ces capacités lors des perturbations est essentiel pour garantir la continuité opérationnelle du MPCU.

(10) Les dispositions visant à garantir cette continuité peuvent facilement passer inaperçues tant qu'aucune perturbation ne survient. Ces perturbations ne découlent pas nécessairement de crises ou d'urgences majeures, mais peuvent résulter d'incidents mineurs ou de conditions négligées ou sous-optimales. Afin d'éclairer la prise de décision concernant les mesures de prévention et d'atténuation, la planification de la continuité opérationnelle pour le PCN doit déterminer les causes potentielles des perturbations qui compromettent les fonctions essentielles du PCN ([7]). Par ailleurs, le personnel travaillant selon un régime de permanence de 24 heures sur 24 et 7 jours sur 7 est confronté à des difficultés uniques sur le plan psychosocial et en matière de bien-être, notamment à des problèmes de santé liés au travail de nuit, au stress professionnel et à l'éloignement familial. S'ils ne sont pas traités, ces problèmes risquent de déboucher sur un épuisement professionnel, une rotation élevée du personnel et d'éventuelles pénuries de personnel.

(11) Les dispositifs de continuité opérationnelle devraient rester efficaces quelle que soit la nature ou la cause de la perturbation, qu'elle résulte de risques naturels, d'accidents, de défaillances techniques, d'erreurs humaines, d'indisponibilités d'infrastructures ou de services d'utilité publique, d'une indisponibilité massive de personnel, d'actes intentionnels ou malveillants, y compris de cyberincidents et d'activités hybrides, ou de toute autre cause.

(12) En se préparant à d'éventuelles perturbations, les PCN renforcent leur capacité à réagir rapidement et efficacement, en réduisant au minimum la durée et l'impact des événements perturbateurs. Cette préparation permet non seulement de garantir la reprise des activités dans un délai acceptable, mais elle limite également les conséquences négatives pour les parties prenantes et les acteurs externes qui dépendent de l'activité du PCN, et préserve la mission et la réputation de l'organisation.

(13) Les perturbations dues à des cyberincidents présentent des caractéristiques distinctes qui méritent une attention particulière: contrairement aux autres menaces pour la continuité opérationnelle, elles peuvent être intentionnelles, se propager par des systèmes interconnectés et compromettre non seulement la disponibilité des données et des communications, mais également leur intégrité ou leur confidentialité.

(14) La réalisation régulière de formations, d'exercices et de mises à jour est indispensable à l'efficacité du programme de continuité opérationnelle. Plus un plan de continuité opérationnelle est mis en pratique, mieux l'organisation est préparée: les exercices permettent de recenser les lacunes et de familiariser le personnel avec les procédures. Un personnel bien formé, ayant une compréhension claire de son rôle et de ses responsabilités, est plus efficace en cas de perturbations. De même, la participation des parties prenantes aux exercices leur permet de comprendre les protocoles de communication et de savoir à quoi s'attendre lors d'événements perturbateurs réels.

(15) Les exercices, les tests de résistance et les incidents réels apportent des enseignements précieux. Pour conserver sa validité, le plan de continuité opérationnelle devrait être régulièrement actualisé de façon à intégrer les enseignements tirés des formations, des exercices, des tests de résistance, des événements réels et des progrès technologiques.

([5]) Communication conjointe au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions sur la stratégie européenne pour une union de la préparation, JOIN(2025) 130 final du 26.3.2025.

([6]) Engagement en faveur d'une meilleure résilience, publié par les chefs d'État et de gouvernement participant à la réunion du Conseil de l'Atlantique Nord tenue à Varsovie les 8 et 9 juillet 2016.

([7]) Il peut s'agir, par exemple, de mises à jour logicielles, de modifications non communiquées du domaine du courrier électronique professionnel, de mises à jour non communiquées des coordonnées, de pénuries persistantes de personnel ou du départ simultané à la retraite d'une grande partie du personnel essentiel dont le remplacement ne peut commencer qu'à la date du départ à la retraite.

(16) Lorsque le PCN fait partie d'une entité qui relève du champ d'application des dispositions applicables de la directive (UE) 2022/2555 du Parlement européen et du Conseil ([8]), il convient de prendre en compte les enseignements tirés du test de résistance lors de la mise en œuvre des mesures de gestion des risques en matière de cybersécurité, en particulier en ce qui concerne la continuité des activités, la gestion des sauvegardes, la reprise des activités et la gestion des crises.

(17) Assurer la continuité opérationnelle de l'autorité nationale compétente en matière de protection civile va au-delà du fonctionnement de son PCN. Dès lors, la présente recommandation peut également servir de référence utile pour le développement de la continuité opérationnelle au sein des organisations nationales et des systèmes de protection civile, conformément au considérant 7 de la décision n° 1313/2013/UE.

(18) La présente recommandation devrait être exhaustive et refléter la diversité des structures et des fonctions des PCN dans les États membres et les États participant au MPCU. Elle devrait être appliquée avec souplesse et adaptée au mandat, au contexte, aux circonstances et au cadre opérationnel de chaque PCN, étant donné que ces derniers possèdent chacun des caractéristiques propres, opèrent dans un cadre juridique distinct et sont confrontés à des problèmes différents, ce qui peut nécessiter des approches sur mesure pour assurer la continuité opérationnelle.

(19) La présente recommandation se fonde sur les résultats des consultations menées avec le groupe d'experts de la Commission sur la continuité opérationnelle 24 h/24 7 j/7 en cas d'événements perturbateurs, créé par la Commission en 2025, et devrait compléter les normes et orientations bien établies existantes relatives à la continuité des activités ([9]),

A ADOPTÉ LA PRÉSENTE RECOMMANDATION:

1. DESTINATAIRES

Les autorités nationales compétentes des États membres et des États participant au MPCU sont destinataires de la présente recommandation.

Les États membres peuvent la juger pertinente pour d'autres centres de crise nationaux et entités gérant les capacités du MPCU.

2. DÉFINITIONS

Aux fins de la présente recommandation, on entend par:

a) «**autorité nationale compétente**»: une autorité désignée par un État membre ou un État participant au MPCU ([10]) dans le cadre du MPCU, visée à l'article 29 de la décision n° 1313/2013/UE;

b) «**point de contact national» (PCN)**: un point de contact pour la liaison avec l'ERCC dans un État membre ou dans un État participant au MPCU, disponible 24 heures sur 24 et sept jours sur sept, désigné conformément à l'article 9, paragraphe 7, de la décision n° 1313/2013/UE et à l'article 3, paragraphe 1, de la décision d'exécution (UE) 2025/704;

c) «**fonctions essentielles**»: les activités, opérations ou services du PCN qui sont indispensables à l'accomplissement de son mandat et de sa mission et qui ne peuvent pas être interrompus ou qui doivent reprendre dans un délai court et prédéfini. Aux fins des présentes lignes directrices, le caractère essentiel d'une fonction est déterminé par l'urgence avec laquelle elle doit être rétablie à la suite d'une perturbation, et pas uniquement par son importance stratégique, opérationnelle ou institutionnelle. En conséquence, les fonctions revêtant une importance stratégique, opérationnelle ou institutionnelle qui peuvent supporter des perturbations ou des retards prolongés sans entraîner de conséquences inacceptables ne sont pas considérées comme des fonctions essentielles;

([8]) Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([9]) Normes internationales: ISO 22301:2019 (Systèmes de management de la continuité d'activité); directive fédérale sur la continuité n° 1 (2017) de la FEMA, directive fédérale sur la continuité n° 2 (2017) de la FEMA, circulaire d'orientation sur la continuité (2018, mise à jour en 2024) de la FEMA, guide utilisateur de la FEMA sur l'analyse des processus opérationnels et des incidences sur les activités (2019); et les orientations concernant les bonnes pratiques (2018) du *Business Continuity Institute*.

([10]) En ce qui concerne les États participants, voir l'article 28 de la décision n° 1313/2013/UE.

d) «**personnel essentiel**»: le personnel travaillant au PCN qui exerce ou soutient des fonctions essentielles, le personnel qui fait partie de l'équipe chargée de gérer un événement perturbateur ou d'y réagir, ou le personnel qui assume ces deux fonctions;

e) «**personnel essentiel rare**»: le personnel essentiel dont le nombre restreint constitue une vulnérabilité pour la continuité opérationnelle en cas d'absence ou d'impossibilité de travailler de ses membres, ceux-ci possédant les certifications, l'habilitation de sécurité, l'autorité, la responsabilité décisionnelle, les droits d'accès, les connaissances, l'expertise ou les compétences linguistiques requises pour mener à bien certaines activités indispensables à la continuité d'une fonction essentielle;

f) «**goulet d'étranglement en matière de personnel**»: une situation dans laquelle la continuité d'une fonction essentielle dépend de la disponibilité d'un ou de plusieurs membres du personnel essentiel rare;

g) «**continuité opérationnelle**»: la capacité d'un PCN à continuer d'assurer ses fonctions essentielles opérationnelles – notamment les activités, opérations ou services – lorsque les ressources nécessaires pour remplir ces fonctions, telles que le personnel essentiel, les informations reçues, les services, les produits, les fournitures, les dispositions budgétaires, les équipements, les systèmes de technologies de l'information et de la communication (TIC) ou les exigences concernant les locaux, sont indisponibles, endommagées, inutilisables ou interrompues;

h) «**plan de continuité opérationnelle**» ou «**plan**»: un document unique ou un ensemble de procédures visant à assurer la continuité opérationnelle du PCN;

i) «**événement perturbateur**»: un incident ou une circonstance qui empêche ou retarde considérablement l'exécution d'une fonction essentielle du PCN;

j) «**rétablissement**»: la remise en état des capacités opérationnelles, des installations, des systèmes et des ressources du PCN à la suite d'une perturbation.

3. RECOMMANDATIONS EN VUE DE LA CONTINUITÉ OPÉRATIONNELLE DES PCN

3.1. Recommandations principales

1. Le PCN devrait élaborer un plan de continuité opérationnelle cohérent et complet ou un ensemble documenté de procédures abordant tous les éléments de la continuité opérationnelle. La section 3.2 contient des recommandations supplémentaires sur le plan de continuité opérationnelle.

2. L'objectif de la planification de la continuité opérationnelle est que le PCN soit à même de remplir ses fonctions essentielles dans des conditions dégradées lors d'événements perturbateurs. À ce titre, la planification de la continuité opérationnelle devrait partir du principe que des événements perturbateurs se produiront et que les conditions normales de fonctionnement pourraient ne pas être rétablies immédiatement, voire, dans certains cas, ne pas être rétablies du tout. Le PCN devrait être capable de maintenir ses fonctions essentielles dans des conditions dégradées en recourant à d'autres procédures, d'autres installations, d'autres canaux de communication et à des ressources réduites jusqu'au rétablissement complet de ses capacités.

3. Lors d'événements perturbateurs, les ressources devraient être affectées en priorité au maintien des fonctions essentielles du PCN. Ce faisant, les fonctions non essentielles peuvent ne pas être maintenues.

4. Les dispositifs de continuité opérationnelle devraient garantir la collecte, l'analyse, la validation et la diffusion ininterrompues des informations opérationnelles nécessaires pour permettre au PCN de conserver une bonne appréciation de la situation et pour appuyer la prise de décision pendant toute la durée de la perturbation.

5. La continuité opérationnelle repose avant tout sur un personnel formé. Si la continuité est favorisée par le plan de continuité opérationnelle, les dispositifs associés et les mesures de secours, elle dépend en définitive de la capacité du personnel à prendre des décisions et à appliquer ces mesures sous la pression.

6. La planification de la continuité opérationnelle devrait reposer sur une compréhension approfondie des dispositifs administratifs et opérationnels de l'organisation à laquelle appartient le PCN. À cette fin, la collaboration entre les services devrait être activement encouragée et facilitée.

7. Le PCN devrait évaluer les sources potentielles de perturbation de ses activités. L'évaluation devrait être axée sur leur potentiel de perturbation des activités du PCN et sur l'élaboration d'un plan d'action visant à assurer la continuité des fonctions essentielles.

8. Lors de l'évaluation des menaces pour la continuité opérationnelle, une attention particulière devrait être portée aux processus sensibles au facteur temps et aux goulets d'étranglement, notamment:

   a) aux sources d'information uniques ou aux informations connues seulement d'un groupe restreint de personnes, y compris les informations classifiées;

   b) aux équipements uniques ou aux prestataires de services uniques dont dépendent les fonctions essentielles;

   c) aux canaux de communication uniques, aux personnes de contact ou décideurs uniques;

   d) à la disponibilité du personnel essentiel rare.

9. Les goulets d'étranglement en matière de personnel, d'installations, de communications, de systèmes TIC, de logistique et de prise de décision devraient être recensés et supprimés. Lorsqu'ils sont inévitables, des mesures appropriées de prévention et d'atténuation devraient être mises en place et testées, notamment celles suggérées à la section 3.9.

10. Chaque perturbation, exercice et test de résistance devrait permettre de tirer des enseignements et d'améliorer les dispositifs de continuité opérationnelle, renforçant ainsi la résilience au fil du temps.

11. Aux fins de la continuité opérationnelle et des tests de résistance pour les PCN dans le cadre du MPCU, il convient de prendre en compte les catégories non exhaustives suivantes d'événements perturbateurs. L'annexe I présente une description de chaque catégorie.

   a) indisponibilité des locaux;

   b) défaillance de l'approvisionnement en électricité;

   c) défaillance ou panne des systèmes TIC;

   d) absence massive de personnel ou absence de personnel essentiel rare.

12. Le PCN devrait être en mesure de poursuivre ses activités en cas de survenue d'un ou plusieurs événements provoquant une rupture de la continuité énumérés au paragraphe 11 ci-dessus.

3.2. **Plan de continuité opérationnelle du PCN**

13. Chaque PCN devrait élaborer un plan de continuité opérationnelle cohérent, complet et écrit, ou un ensemble équivalent de procédures documentées, qui aborde tous les éléments de la continuité opérationnelle et qui intègre et systématise la réaction aux perturbations, notamment les mesures d'atténuation et les accords d'intervention immédiate.

14. Le plan de continuité opérationnelle devrait prévoir des dispositifs de substitution pour l'ensemble des processus essentiels, en particulier ceux sensibles au facteur temps, afin qu'ils puissent être maintenus en cas de défaillance des ressources primaires. Les dispositifs de secours et les dispositifs de substitution devraient être totalement indépendants. Ils ne devraient pas dépendre des mêmes ressources, que ce soit le même bâtiment, la même source d'énergie, la même voie de communication, la même plateforme TIC ou le même prestataire de services. Ils ne devraient pas non plus créer de nouvelles dépendances susceptibles d'introduire de nouveaux risques de perturbation.

15. Le plan de continuité opérationnelle devrait être appliqué régulièrement dans des conditions réalistes. Les plans qui n'ont pas été validés par des formations, des exercices ou des tests de résistance ne devraient pas être considérés comme opérationnels. Le programme de continuité opérationnelle devrait comprendre des formations obligatoires régulières pour le personnel essentiel, des tests et des exercices réguliers impliquant l'activation du plan, ainsi que sa révision et sa mise à jour systématiques, de manière que l'ensemble du personnel et des parties prenantes concernés soient informés des mises à jour et y soient formés.

16. En fonction de la structure de l'organisation, le PCN devrait associer à l'élaboration du plan de continuité opérationnelle des membres du personnel qui ne participent pas directement aux fonctions essentielles, mais qui disposent de l'expertise ou des connaissances nécessaires pour contribuer à une compréhension globale des fonctions de l'organisation.

17. Les PCN devraient envisager d'instaurer, au sein de leur organisation, une fonction de coordination de la continuité consacrée au plan de continuité opérationnelle. En fonction de la taille et de la structure du PCN, cette fonction de coordination de la continuité devrait être exercée par un coordinateur unique, par une équipe spécialisée réunissant des représentants des domaines opérationnels concernés, ou selon d'autres dispositions adaptées au contexte national. Lorsqu'il est constitué, un groupe devrait comprendre des membres disposant d'une expertise dans les domaines opérationnels pertinents pour la mise en œuvre du plan, tels que les systèmes TIC, les locaux de substitution, les ressources humaines ou la logistique. La fonction de coordination de la continuité devrait consister à veiller à la mise en œuvre cohérente du plan de continuité opérationnelle, à sa révision périodique et à sa mise à jour, et à vérifier, entre autres, les ressources et les dispositifs sur lesquels repose le plan.

3.3. **Recensement des fonctions essentielles**

18. Le PCN devrait recenser ses fonctions essentielles et dresser et tenir à jour un inventaire de celles-ci. Outre les fonctions liées au MPCU, telles que la gestion des demandes d'assistance et l'offre et le déploiement de capacités de réaction du MPCU, le PCN peut également être amené à assurer la continuité d'autres fonctions essentielles pour l'organisation. Il peut s'agir notamment d'organiser la coordination avec les autorités nationales ou régionales, d'assurer la liaison avec d'autres organisations internationales, d'émettre des alertes publiques, et de contribuer à la prise de décision à un niveau supérieur.

Pour chaque fonction essentielle, le PCN devrait établir des objectifs de performance opérationnelle qui définissent le niveau maximal acceptable de dégradation des services lors d'événements perturbateurs. Ces objectifs devraient préciser, le cas échéant, la durée de perturbation maximale tolérable, les objectifs de délai de rétablissement, la quantité acceptable de perte d'informations opérationnelles, les niveaux d'effectifs minimaux, la disponibilité des communications et la capacité de prise de décision. Ils devraient guider l'élaboration du plan de continuité opérationnelle et servir de base à l'évaluation de la performance lors des tests de résistance. L'annexe II comprend des exemples d'objectifs de performance opérationnelle.

19. Il est recommandé de classer les fonctions essentielles selon leur niveau de priorité ou le degré d'urgence avec lequel elles doivent être rétablies.

3.4. **Analyse des processus opérationnels et ressources de secours**

20. Sur le fondement de l'inventaire des fonctions essentielles, le PCN devrait procéder à une analyse des processus opérationnels et élaborer des solutions de secours afin d'assurer la continuité de ses fonctions essentielles. L'analyse des processus opérationnels devrait permettre d'acquérir une compréhension approfondie du fonctionnement des fonctions en déterminant, pour chacune d'entre elles:

a) les tâches qui la composent;

b) le calendrier et la séquence des tâches, y compris la durée et les étapes sensibles au facteur temps;

c) les personnes en charge de chaque tâche, y compris le profil, l'expertise ou la formation requis;

d) le flux d'informations, y compris la manière dont les données, les demandes et les résultats circulent entre les acteurs et les systèmes;

e) les personnes chargées de valider ou d'autoriser le ou les processus;

f) les ressources mobilisées et les contributions d'acteurs externes nécessaires, y compris les informations, les ensembles de données, les services, les produits, les fournitures, les dispositions budgétaires, les équipements, les systèmes TIC et les exigences concernant les locaux. Il peut s'agir d'entreprises privées assurant l'approvisionnement en énergie ou fournissant des services de sécurité. Une attention particulière devrait être accordée au niveau de classification des informations, ainsi qu'aux locaux et aux appareils utilisés pour les gérer;

g) les résultats produits par la fonction, notamment les informations, les produits ou services spécifiques, ou les actions de coordination, de validation ou d'autorisation;

h) l'organisation externe (ou les organisations externes) ou les groupes de parties prenantes qui reçoivent les résultats;

i) les dépendances et interdépendances essentielles aux opérations, notamment les relations et accords avec des acteurs externes – les autorités d'autres États membres et des États participant au MPCU, les partenaires de la protection civile, les opérateurs d'infrastructures essentielles, les prestataires de services, les fournisseurs, etc. – en précisant les ressources et résultats attendus;

j) les ressources de secours et les dispositifs de substitution disponibles.

21. Les PCN sont invités à tenir compte du tableau figurant à l'annexe III lorsqu'ils réalisent leur analyse des processus opérationnels.

3.5. **Pratiques recommandées pour les installations et équipements de substitution**

22. Le PCN devrait être en mesure de poursuivre ses activités lorsque ses locaux deviennent temporairement inaccessibles ou inutilisables, notamment en veillant à la disponibilité des équipements essentiels.

23. Les locaux principaux et de substitution et les solutions temporaires devraient être sûrs et présenter un niveau de classification approprié. Ces mesures devraient être proportionnées à la nature des crises affrontées et au niveau de sensibilité ou de classification des informations traitées.

3.6. **Pratiques recommandées pour l'approvisionnement en électricité**

24. Le PCN devrait être en mesure de poursuivre ses activités en cas de coupures locales ou de pannes généralisées.

25. Les locaux principaux et de substitution, y compris les locaux temporaires, devraient disposer d'un approvisionnement en électricité résilient et de systèmes de secours qui permettent au PCN de continuer à fonctionner et à remplir ses fonctions essentielles lors de coupures de courant prolongées.

26. Les mesures prévues pour les PCN devraient être mises en œuvre, le cas échéant, conformément aux plans nationaux de préparation aux risques dans le secteur de l'électricité établis au titre du règlement (UE) 2019/941 du Parlement européen et du Conseil ([11]) et aux plans d'action préventifs et plans d'urgence nationaux établis au titre du règlement (UE) 2017/1938 sur la sécurité de l'approvisionnement en gaz naturel du Parlement européen et du Conseil ([12]), ainsi qu'aux dispositifs nationaux existants de gestion de crise.

3.7. **Pratiques recommandées pour les systèmes TIC**

27. Le PCN devrait veiller à la fiabilité et à la résilience des systèmes TIC qui soutiennent ses fonctions essentielles. Une attention particulière devrait être accordée:

a) à la continuité de l'accès aux bases de données, aux documents et aux courriels, notamment la disponibilité des listes de contacts actualisées, la continuité de la communication avec l'ERCC, les États membres et les États participant au MPCU, et à la continuité des systèmes de traitement et de gestion destinés à la collecte et au suivi des informations et à l'enregistrement des mesures adoptées;

b) à l'intégration technologique, en assurant la compatibilité et l'interopérabilité des systèmes essentiels avec des configurations à distance et des sites de substitution, notamment la capacité de ces sites à se connecter au système commun de communication et d'information d'urgence (CECIS) et à traiter les informations classifiées dans le cadre d'un fonctionnement à distance. Ces dispositifs devraient être vérifiés au moyen de tests appropriés;

c) à la sécurité des informations et des communications, notamment la possibilité d'établir des connexions destinées au traitement d'informations classifiées et d'échanger des communications classifiées tant au niveau national qu'international;

d) aux registres de tous les fournisseurs tiers des appareils et des logiciels utilisés dans le PCN.

([11]) Règlement (UE) 2019/941 du Parlement européen et du Conseil du 5 juin 2019 sur la préparation aux risques dans le secteur de l'électricité et abrogeant la directive 2005/89/CE (JO L 158 du 14.6.2019, p. 1, ELI: http://data.europa.eu/eli/reg/2019/941/oj).

([12]) Règlement (UE) 2017/1938 du Parlement européen et du Conseil du 25 octobre 2017 concernant des mesures visant à garantir la sécurité de l'approvisionnement en gaz naturel et abrogeant le règlement (UE) n° 994/2010 (JO L 280 du 28.10.2017, p. 1, ELI: http://data.europa.eu/eli/reg/2017/1938/oj).

28. Une attention particulière devrait être accordée aux cyberincidents en tant que catégorie distincte de perturbation des TIC. Le PCN devrait envisager d'établir des protocoles de coordination avec l'autorité nationale de cybersécurité, dans le cadre plus large de ses dispositifs de continuité opérationnelle. Ces mesures devraient prévoir des canaux d'alerte précoce, des protocoles conjoints de réaction aux incidents et une clarification des rôles lors d'un cyberincident touchant le PCN.

3.8. **Pratiques recommandées pour les ressources humaines**

29. Le PCN devrait veiller à disposer d'un personnel suffisant qui permette de rester opérationnel en cas d'indisponibilité d'une partie des effectifs et devrait s'assurer que son personnel possède le profil et les compétences nécessaires.

30. Le PCN devrait envisager:

a) de veiller à la disponibilité d'effectifs aux compétences et au parcours appropriés, disposant notamment d'une expérience en matière de gestion de crise et, le cas échéant, de l'habilitation de sécurité requise pour traiter des informations classifiées. Il devrait élaborer et mettre en œuvre des mécanismes de vérification des compétences professionnelles et offrir des programmes complets d'intégration et de formation continue afin de maintenir et de renforcer les compétences du personnel, de façon à ce que celui-ci soit pleinement préparé à réagir efficacement aux activations du MPCU. La formation devrait également porter sur la prévention des perturbations causées par une erreur humaine ou des actes malveillants, notamment sur les aspects essentiels de la cybersécurité et de la sécurité de l'information, tels que le risque posé par l'ingénierie sociale;

b) de dispenser régulièrement des formations pour tenir le personnel informé des dispositifs de continuité opérationnelle et de l'utilisation des équipements et des systèmes TIC dans les locaux principaux et de substitution. Il devrait envisager d'offrir au personnel des PCN des formations complémentaires sur la gestion des catastrophes et des crises de longue durée et sur les opérations du MPCU;

c) d'élaborer des plans pour assurer la rotation du personnel lors de situations d'urgence prolongées, y compris la gestion de la capacité d'intervention rapide. Il devrait mettre sur pied des groupes de travail avec des rôles clairs et des plans de succession afin d'améliorer la coordination en période de crise;

d) de mettre en place des solutions de transport permettant au personnel essentiel de rejoindre le lieu d'exercice de ses fonctions, qu'il s'agisse, selon le cas, du site principal, d'un autre site ou d'une unité mobile;

e) de mettre en place des garanties appropriées pour assurer la protection de la santé et de la sécurité du personnel;

f) d'élaborer des plans favorisant le bien-être du personnel qui prévoient la nourriture, l'eau, le logement, l'accès aux installations des PCN et un soutien psychologique afin d'aider le personnel à gérer le stress et la fatigue. Ces plans devraient permettre la poursuite des opérations dans des environnements confinés et tenir compte de la situation individuelle ou personnelle du personnel essentiel, y compris leurs besoins familiaux, le cas échéant;

g) d'établir des politiques en matière de protection des données et de la vie privée afin que la planification de la continuité respecte la protection des données à caractère personnel pendant et après les incidents.

31. Les fonctions essentielles devraient être soutenues par des dispositifs de continuité opérationnelle appropriés, des formations croisées structurées et systématiques et des exercices réguliers, de sorte qu'elles puissent être exercées par plusieurs membres du personnel formés, en évitant les goulets d'étranglement en matière de personnel. Aucune fonction essentielle ne devrait dépendre exclusivement de la disponibilité d'un seul membre du personnel.

3.9. **Mesures de prévention et d'atténuation pour chaque catégorie d'événement perturbateur**

32. La section suivante fournit une liste indicative des mesures de prévention et d'atténuation recommandées pour chaque catégorie d'événement perturbateur. Bien qu'elles puissent être mises en œuvre en parallèle, chaque État membre devrait choisir les options les plus appropriées et les plus efficaces au regard du mandat de son PCN, de son contexte, de ses circonstances, de ses capacités, de la structure de son cadre opérationnel et juridique, et des causes potentielles de perturbations susceptibles de compromettre les fonctions essentielles de son PCN. La liste n'a pas vocation à être appliquée intégralement et simultanément dans la mesure où, dans certains cas, la mise en œuvre d'une mesure pourrait interférer avec l'application d'une autre mesure ou nécessiter des investissements excessifs.

33. Mesures de prévention et d'atténuation recommandées pour remédier à l'indisponibilité des locaux:

a) répartition géographique du PCN entre deux ou plusieurs centres géographiquement distincts opérant simultanément, qui s'apportent mutuellement assistance en cas d'incapacité à agir ou de dépassement de leurs capacités respectives;

b) relocalisation vers des locaux de substitution gérés par l'autorité du PCN;

c) transfert du personnel essentiel vers des locaux de substitution selon des modalités préétablies (notamment en cas de conditions météorologiques défavorables);

d) travail à distance (impliquant une flexibilité des tâches susceptibles d'être effectuées en dehors de l'emplacement physique du PNC);

e) unités mobiles de commandement et de contrôle susceptibles d'accueillir temporairement le personnel essentiel du PCN;

f) activation de conventions administratives avec d'autres autorités en vue de l'utilisation de leurs locaux;

g) délégation.

34. Mesures de prévention et d'atténuation recommandées pour remédier à une défaillance de l'approvisionnement en électricité:

a) activation de groupes électrogènes et de sources d'alimentation non interruptibles (UPS);

b) conclusion de conventions et d'accords avec les fournisseurs pour l'approvisionnement prioritaire en combustibles;

c) autonomie énergétique et sources d'énergie alternatives pour les fonctions essentielles;

d) maximisation de la capacité électrique disponible;

e) relocalisation vers des locaux de substitution gérés par l'autorité du PCN avec approvisionnement en électricité garanti;

f) travail à distance depuis un bâtiment avec approvisionnement en électricité garanti;

g) unités mobiles de commandement et de contrôle autosuffisantes en électricité;

h) activation de conventions administratives avec d'autres autorités en vue de l'utilisation de leurs locaux avec approvisionnement en électricité garanti;

i) délégation.

35. Mesures de prévention et d'atténuation recommandées pour remédier à une défaillance ou une panne des systèmes TIC:

a) redondance;

b) sauvegardes de données régulières et sécurisées, y compris des copies hors site et hors ligne;

c) systèmes TIC, plateformes et canaux de communication de substitution;

d) équipes d'aide TIC d'urgence ou unités d'intervention technique de garde;

e) procédures de réponse aux incidents de cybersécurité coordonnées avec l'autorité nationale de cybersécurité;

f) copies hors ligne des listes de contacts essentiels, des procédures clés et des documents opérationnels;

g) unités mobiles de commandement et de contrôle ayant accès aux systèmes TIC primaires et de secours;

h) transfert vers des locaux de substitution gérés par l'autorité du PCN et ayant accès aux systèmes TIC primaires et de secours;

i) activation de conventions administratives avec d'autres autorités en vue de l'utilisation de leurs locaux ayant accès aux systèmes TIC.

36. Mesures de prévention et d'atténuation recommandées pour remédier à l'absence massive de personnel et à l'absence de personnel essentiel rare:

a) gestion des heures supplémentaires (solution à court terme);

b) réaffectation des tâches au personnel disponible;

c) groupe prédéfini de personnel formé au sein de l'établissement, disponible rapidement;

d) définir des priorités pour le recrutement du personnel;

e) investissement dans la rétention du personnel essentiel;

f) soutien des familles du personnel essentiel;

g) prévention des goulets d'étranglement en matière de personnel en déléguant l'autorité et en promouvant le partage du leadership.

37. L'annexe IV fournit des orientations techniques pour la mise en œuvre de chaque mesure énumérée.

3.10. **Continuité des opérations en cas d'activation du MPCU**

38. Afin de renforcer les opérations du MPCU et d'assurer la continuité, les mesures suivantes sont recommandées:

a) Lorsque le pays a accès aux services télématiques transeuropéens entre administrations (TESTA) ou à TESTA-EIRIS (qui succède à TESTA), identifier le coordinateur national TESTA du pays. Veiller à ce que le point de contact CECIS du pays dispose des coordonnées du coordinateur national TESTA du pays et à ce que ces coordonnées soient tenues à jour. Veiller à ce que le point de contact CECIS du pays ait une bonne compréhension du plan de continuité opérationnelle de son accès local ou national au portail TESTA à l'intérieur du pays.

b) Élaborer des protocoles visant à distinguer les défaillances de la connectivité TESTA des défaillances de la plateforme CECIS lorsqu'une demande d'aide est formulée par le biais du MPCU, et à permettre de présenter des demandes d'assistance en cas de perturbation des TESTA dans le pays du PCN.

c) Le cas échéant, étudier des dispositions de soutien opérationnel mutuel avec d'autres autorités nationales afin que le PCN puisse continuer à exercer ses fonctions essentielles si une perturbation dégrade considérablement sa capacité de continuité opérationnelle. En particulier, ces dispositions devraient associer les autorités ayant accès aux TESTA, de façon à ce que le PCN puisse accéder au CECIS depuis des locaux de substitution.

d) Le cas échéant, étudier la possibilité d'établir des dispositions administratives bilatérales de soutien opérationnel mutuel avec les pays voisins qui sont des États membres ou des États participant au MPCU, dans les situations où une perturbation dégrade considérablement la capacité de continuité opérationnelle du PCN et où les dispositifs visés au point b) ne sont pas possibles. Ces dispositions devraient permettre au PCN d'utiliser les locaux de ces pays et d'accéder au réseau TESTA.

e) Dispenser une formation sur le CECIS aux nouveaux membres du personnel et programmer des exercices réguliers pour le personnel.

f) En fonction de la structure nationale de protection civile, le plan de continuité devrait comprendre des dispositions visant à assurer une communication fluide entre le PCN et les autres autorités compétentes qui sont habilitées à demander, si nécessaire, l'activation du MPCU.

g) Le plan de continuité opérationnelle devrait tenir compte des parties prenantes nationales possédant et gérant les ressources du MPCU qui ne relèvent pas de l'autorité du PCN mais qui pourraient être mises à disposition, sur demande, aux fins d'une intervention par l'intermédiaire du MPCU.

39. Le plan de continuité opérationnelle devrait être aligné sur la recommandation de la Commission du 29 novembre 2024 sur les lignes directrices de l'UE relatives au soutien fourni par le pays hôte ([13]), en particulier en ce qui concerne les activations du MPCU par le PCN et son rôle dans le soutien fourni par le pays hôte ([14]).

([13]) C(2024) 8339.

([14]) Conformément à l'article 4, point 9, de la décision n° 1313/2013/UE, on entend par «soutien fourni par le pays hôte» toute action entreprise durant les phases de préparation et de réaction par le pays qui bénéficie des secours ou qui les envoie, ou par la Commission, afin d'éliminer les obstacles prévisibles à l'aide internationale fournie via le mécanisme de l'Union. Cela comprend l'appui apporté par des États membres pour faciliter le transit de l'aide sur leur territoire.

3.11. **Activation du plan de continuité opérationnelle**

40. En fonction de la nature et de l'ampleur de la perturbation, le plan de continuité opérationnelle du PCN devrait définir différents niveaux d'activation: une activation partielle, lorsque le PCN continue de fonctionner depuis ses locaux principaux selon des procédures adaptées, et une activation complète, qui nécessite un transfert vers des locaux de substitution ou d'autres dispositifs de substitution.

41. Les critères, les niveaux d'activation et les déclencheurs, ainsi que l'autorité habilitée à autoriser l'activation, devraient être définis au niveau national, conformément à la structure et au cadre opérationnel de chaque PCN. On trouvera un exemple illustrant un flux d'activation à l'annexe V.

42. Les procédures d'activation devraient permettre l'activation en temps utile des dispositifs de continuité en réponse aux perturbations tant réelles qu'anticipées, y compris aux événements survenant en dehors des heures normales de travail et aux événements pour lesquels un avertissement préalable est disponible.

43. Si un incident perturbe la continuité opérationnelle du PCN et déclenche l'activation de son plan de continuité opérationnelle, le PCN devrait envisager d'en informer l'ERCC.

3.12. **Formations, exercices et tests réguliers**

44. Les plans de continuité opérationnelle devraient régulièrement donner lieu à des formations, faire l'objet d'exercices et être testés. Il est également recommandé de programmer régulièrement des sessions de sensibilisation et d'information, ainsi que des sessions de formation et des exercices en lien avec les plans de continuité. D'autres formations régulières, telles que des activités d'intégration destinées aux nouveaux membres du personnel, devraient également intégrer les éléments nécessaires du plan de continuité opérationnelle. La participation des parties prenantes externes susceptibles d'être affectées par une perturbation des activités du PCN devrait également être envisagée dans le cadre de sessions régulières et ciblées de sensibilisation et d'information, ainsi que dans le cadre d'exercices.

45. Le plan de continuité opérationnelle devrait être testé au minimum une fois par an. Il convient d'envisager d'augmenter la fréquence des tests lorsque la structure, le contexte opérationnel ou le profil de risque du PCN le justifie.

3.13. **Rétablissement**

46. Une fois les effets négatifs de l'événement perturbateur atténués, le PCN devrait considérer le retour progressif à un fonctionnement normal comme une phase distincte de la continuité opérationnelle: le rétablissement correspond à la phase durant laquelle le PCN passe des dispositifs de continuité opérationnelle à un fonctionnement normal, ce qui implique la reprise des fonctions importantes (mais non essentielles) qui ont pu être temporairement suspendues.

47. Le plan de continuité opérationnelle devrait définir les conditions d'enclenchement du rétablissement, identifier l'autorité habilitée à autoriser le retour à la normale et préciser les étapes nécessaires pour assurer le retour au fonctionnement normal en toute sécurité.

48. Les points suivants devraient être pris en considération lors de la phase de rétablissement:

a) *Vérification des conditions de rétablissement*. Avant le retour à la normale, le PCN devrait déterminer si l'événement perturbateur à l'origine de la situation a été maîtrisé ou suffisamment atténué; si les locaux principaux, les systèmes TIC et les canaux de communication sont de nouveau pleinement opérationnels; et si l'intégrité des bases de données et des documents a été vérifiée. Une attention particulière devrait être accordée aux données reproduites lors de la perturbation, afin d'éviter de perdre les informations générées pendant le déploiement des dispositifs de continuité opérationnelle.

b) *Rétablissement progressif des fonctions essentielles*. Toutes les fonctions essentielles ne devraient pas être retransférées d'un seul coup. Le PCN devrait envisager de les transférer dans l'ordre de priorité inverse, en commençant par celles pour lesquels une brève interruption lors du retour à la normale est la plus tolérable, tout en maintenant les fonctions de priorité absolue dans le cadre des dispositifs de continuité jusqu'à confirmation de la stabilité de l'environnement normal. Il convient de recourir au fonctionnement en parallèle durant le retour à la normale, afin de réduire le risque de défaillance en cascade.

c) *Reprise des fonctions importantes*. Les fonctions non essentielles qui ont été temporairement suspendues pendant la perturbation ne devraient reprendre qu'une fois que la stabilité des fonctions essentielles a été confirmée en conditions de fonctionnement normal. L'ordre et le rythme de la reprise devraient être adaptés à la disponibilité du personnel, compte tenu du fait que les dispositifs de continuité opérationnelle entraînent souvent une augmentation de sa charge de travail et de son degré de fatigue.

d) *Recherche de vulnérabilités supplémentaires*. Le PCN devrait vérifier que les dispositifs de continuité opérationnelle n'ont pas introduit de nouvelles vulnérabilités avant le retour à la normale.

49. Les PCN devraient également mener les activités suivantes:

a) *Débriefing post-événement*. Afin d'aider à recenser les aspects qui ont fonctionné ou non, le PCN devrait prévoir un débriefing associant toutes les catégories de personnel qui ont participé à la réaction.

b) *Documentation après action*. Le PCN devrait produire, après l'action, un document structuré qui présente la chronologie des événements, l'activation des dispositifs de continuité opérationnelle, l'exécution des fonctions essentielles, les lacunes constatées et les enseignements tirés.

c) *Intégration des enseignements tirés dans le plan de continuité opérationnelle*. Après chaque événement perturbateur déclenchant l'activation du plan de continuité opérationnelle, le PCN devrait fixer un calendrier défini pour mettre à jour le plan, de façon à intégrer les enseignements tirés avant qu'ils ne s'effacent de la mémoire opérationnelle. Le PCN devrait donc mettre en place un processus permettant d'assurer un suivi des lacunes constatées et des mesures correctives et de tester à nouveau les mesures mises à jour, le cas échéant. Lorsqu'il y a lieu, les enseignements tirés devraient également se traduire par des améliorations des activités normales du PCN.

3.14. **Stratégie de communication**

50. La gestion efficace des événements perturbateurs passe par la communication, et chaque PCN devrait élaborer une stratégie de communication solide qui reconnaisse les responsabilités du PCN en matière de communication générale et de communication de crise. Cette stratégie devrait guider les décisions et les actions du PCN en matière de partage d'informations lors de perturbations, afin que toutes les parties concernées ou affectées reçoivent les informations nécessaires et puissent, le cas échéant, agir en conséquence, ce qui contribue à protéger la réputation de l'organisation et à préserver la confiance. L'annexe VI contient des suggestions d'éléments que le PCN doit prendre en considération pour élaborer une stratégie de communication solide.

4. **RECOMMANDATIONS CONCERNANT L'ORGANISATION ET LA CONDUITE D'UN TEST DE RÉSISTANCE**

51. La Commission recommande de soumettre les PCN à des tests de résistance dans le cadre du MPCU. La présente section fournit des orientations sur la manière de concevoir et d'évaluer un test de résistance.

4.1. **Finalité et objectifs**

52. Le test de résistance devrait avoir pour finalité d'évaluer la capacité du PCN à continuer d'exercer ses fonctions essentielles dans des conditions perturbées. À cette fin, le test de résistance devrait prendre la forme d'un exercice de portée limitée visant à évaluer les dispositifs de continuité opérationnelle existants ainsi que l'exercice de fonctions essentielles ciblées du PCN dans des conditions perturbées, y compris en testant à la fois les ressources primaires et les ressources de remplacement.

53. Le test de résistance devrait poursuivre les objectifs généraux suivants:

a) réviser, mettre à jour et valider le plan de continuité opérationnelle, ainsi qu'évaluer l'expertise, les équipements et les dispositions du PCN en matière de continuité opérationnelle;

b) améliorer la compréhension des priorités et des contraintes et faire évoluer les perceptions concernant la continuité opérationnelle du PCN;

c) recenser les faiblesses, les lacunes, les goulets d'étranglement et les dépendances, ainsi que les possibilités d'amélioration du plan de continuité opérationnelle et des ressources nécessaires au maintien des fonctions essentielles, des formations, des équipements et des dispositions connexes du PCN;

d) évaluer la capacité du personnel essentiel du PCN à différents niveaux, notamment celui de la direction, à exercer ses rôles et responsabilités;

e) évaluer la coordination et la communication au sein de l'organisation et avec les partenaires extérieurs dans des conditions perturbées.

54. Lors de la planification du test de résistance, il est recommandé de définir des objectifs spécifiques qui soient mesurables et adaptés aux fonctions essentielles à tester.

55. Le test de résistance ne devrait pas viser à recenser les menaces susceptibles de déclencher des incidents risquant de perturber le fonctionnement normal du PCN.

4.2. **Champ d'application**

56. Le champ d'application du test de résistance devrait préciser les éléments suivants:

a) les objectifs spécifiques du test de résistance;

b) les fonctions essentielles à évaluer;

c) la nature et la durée de la perturbation affectant la continuité du fonctionnement;

d) les ressources mobilisées, y compris les membres du personnel et leurs rôles, les locaux, les équipements et les systèmes TIC;

e) le degré de participation des parties prenantes externes.

4.3. **Scénarios**

57. Une approche fondée sur des scénarios devrait permettre de prévoir les conséquences des incidents (déclencheurs) susceptibles de perturber les activités et, par conséquent, d'entraîner l'activation du plan de continuité opérationnelle du PCN. Il est recommandé de tester différents scénarios et d'en faire varier la complexité, de façon à préparer l'organisation à une série de résultats possibles. Les scénarios doivent être exigeants mais réalistes, afin de fournir des informations utiles sur l'efficacité du plan de continuité opérationnelle. L'annexe VII présente deux exemples de scénarios.

58. Il est recommandé aux PCN de se reporter à la liste non exhaustive suivante de déclencheurs pour activer le plan de continuité opérationnelle des PCN: 1) indisponibilité des locaux, 2) défaillance de l'approvisionnement en électricité, 3) défaillance ou panne des systèmes TIC et 4) absence massive de personnel et absence de personnel essentiel rare.

a) *Déclencheur 1: indisponibilité des locaux*. Le bâtiment abritant le PCN a subi des dommages physiques, est inaccessible ou a été évacué. Ces circonstances le rendent inutilisable pour une durée indéterminée.

b) *Déclencheur 2: défaillance de l'approvisionnement en électricité*. Une défaillance du réseau électrique prive d'électricité le bâtiment dans lequel le PCN exerce ses activités. Cette rupture de l'alimentation électrique dépasse la durée pendant laquelle le groupe électrogène de secours du PCN peut fonctionner sans être ravitaillé en carburant. Si l'autonomie exacte en carburant du groupe électrogène n'est pas connue, la défaillance doit être traitée comme une rupture de durée indéterminée.

c) *Déclencheur 3: défaillance ou panne des systèmes TIC*. Une défaillance du système TIC entrave le fonctionnement efficace du logiciel ou de l'application – ou des applications – du PCN. Elle empêche également l'accès aux bases de données essentielles, rendant les systèmes TIC inutilisables pour une durée indéterminée.

d) *Déclencheur 4: absence massive de personnel et absence de personnel essentiel rare*. Une part importante du personnel se trouve soudainement dans l'incapacité de remplir ses fonctions. Cette pénurie pourrait se traduire par l'absence de personnel essentiel rare et entraîner des retards ou des perturbations dans les activités. L'indisponibilité devrait se prolonger suffisamment longtemps pour que la surcharge de travail dépasse la capacité d'absorption du personnel restant.

59. Les tests de résistance devraient progressivement combiner plusieurs événements perturbateurs afin d'évaluer la capacité du PCN à maintenir ses fonctions essentielles lors de perturbations en cascade ou multiples affectant plusieurs ressources en même temps.

4.4. **Participants**

60. Il est recommandé d'identifier les participants en fonction des objectifs définis, des fonctions essentielles et du scénario du test de résistance.

4.5. **Évaluation, recensement des enseignements tirés et mise en œuvre des améliorations**

61. Il est conseillé de mettre en place un système d'évaluation lors de la planification du test de résistance. Cela aide à recenser les lacunes et les axes d'amélioration du plan de continuité opérationnelle, tout en évaluant la réussite globale de l'exercice. Ce dispositif sert également de base à la planification et aux formations futures sur la continuité opérationnelle du PCN.

62. Il est recommandé de systématiser le format d'évaluation, que ce soit à la suite d'événements réels ou d'exercices ou d'activités de formation, y compris les tests de résistance. Aux fins du test de résistance, il est recommandé aux PCN d'utiliser la grille d'évaluation fournie à l'annexe VIII. Cette grille propose d'évaluer la continuité opérationnelle sous deux angles complémentaires:

a) *conformité avec le plan de continuité opérationnelle*, et

b) *maintien des fonctions essentielles et réalisation des objectifs de performance prédéfinis*.

63. Par ailleurs, le tableau figurant à l'annexe IX vise à aider les PCN à consigner les résultats de l'évaluation, recenser les enseignements tirés et proposer des améliorations. L'annexe X contient un modèle de questionnaire destiné à recueillir les retours d'expérience des participants.

64. Après réalisation d'un test de résistance de leur PCN, les États membres et les États participant au MPCU sont invités à communiquer à l'ERCC les enseignements tirés et les améliorations proposées qui ne présentent pas de caractère sensible.

Fait à Bruxelles, le 29 octobre 2026.

Par la Commission
Hadja LAHBIB
Membre de la Commission

ANNEXE I

Catégorie d'événements perturbateurs

Quatre catégories différentes d'événements perturbateurs peuvent être mises en évidence aux fins de la continuité opérationnelle et des tests de résistance pour les points de contact nationaux (PCN) au sein du mécanisme de protection civile de l'Union (MPCU):

— *Indisponibilité des locaux:* les locaux utilisés par les PCN ne peuvent plus être utilisés en raison d'un incident physique ou opérationnel qui empêche ou limite fortement l'accès au bâtiment ou son utilisation, que ce soit de manière temporaire ou permanente. Il peut par exemple s'agir de voies d'accès principales bloquées, de dommages physiques causés aux bâtiments voisins, de défaillances ou de problèmes affectant des installations et des services de distribution d'eau, de chauffage, des systèmes de ventilation ou des systèmes de sécurité ([1]). Ces incidents peuvent également perturber les activités du PCN si les locaux de ce dernier doivent être évacués ou deviennent inutilisables ou inaccessibles à la suite de leur survenue.

— *Défaillances de l'approvisionnement en électricité:* les locaux du PCN sont touchés par une panne d'alimentation électrique. Une défaillance prolongée peut provoquer des incidents d'alimentation en carburant des groupes électrogènes de secours. Elle peut également avoir une incidence sur les systèmes tributaires de l'électricité, notamment les systèmes TIC.

— *Défaillance ou panne des systèmes TIC:* les logiciels ou les applications du PCN ne sont pas en mesure de fonctionner efficacement. Ces défaillances peuvent avoir des conséquences diverses, comme des problèmes d'authentification empêchant l'accès aux systèmes, une grave dégradation des performances, la corruption ou l'indisponibilité des données, la défaillance des interfaces reliées aux systèmes externes, des dysfonctionnements après une mise à jour, ou un incident de cybersécurité tel qu'une usurpation d'identité numérique pour accéder au système principal d'un PCN, entraînant la diffusion d'informations manipulées par le point de contact.

— *Absence massive de personnel ou pénurie de personnel essentiel:* un nombre important de membres du personnel essentiel sont dans l'impossibilité d'accéder aux locaux ou de travailler pour l'une ou l'autre raison. La situation est aggravée lorsque les fonctions essentielles dépendent d'une seule personne ou d'un groupe restreint de personnel essentiel rare, dont l'absence imprévue ou l'indisponibilité provoque des perturbations.

Ces quatre catégories d'événements perturbateurs fournissent un cadre visant à déterminer les mesures nécessaires pour atténuer les perturbations. Toutefois, des événements perturbateurs peuvent également être déclenchés par d'autres incidents tels qu'un afflux soudain d'informations qui dépasse les capacités dont dispose le PCN pour les gérer, ou la diffusion de fausses informations qui obligent le PCN à mobiliser des ressources à des fins de vérification et de diffusion d'informations exactes.

En outre, les incidents perturbateurs peuvent être interconnectés, et un seul événement peut toucher plusieurs zones en même temps. Ainsi, un incendie peut rendre les locaux inaccessibles tout en provoquant une panne d'alimentation et en endommageant les systèmes TIC et les données. Par ailleurs, ces événements peuvent résulter d'actes intentionnels ou malveillants, comme un cyberincident ou des activités hybrides, et de plusieurs incidents simultanés, ce qui décuple leurs effets. En conséquence, les PCN doivent élaborer un plan d'action complet qui aborde chaque catégorie individuellement, étudie leurs effets combinés, prévoit la possibilité de la survenue de perturbations simultanées et la manière de s'y préparer, afin d'assurer la continuité de leurs opérations.

([1]) Les défaillances de l'approvisionnement en électricité ou les perturbations ou défaillances des systèmes TIC ne relèvent pas de cette catégorie.

ANNEXE II

Exemples d'objectifs de performance opérationnelle

Capacités	Objectif indicatif de performance opérationnelle (à évaluer et à adapter en fonction des exigences nationales)
Appréciation initiale de la situation	dans les 15 minutes
Activation de mécanismes de continuité des activités	dans les 30 minutes
Activation de modes de communication de substitution	dans les 30 minutes
Mise en place d'un poste de commandement opérationnel de substitution	dans les 2 heures
Capacités d'aide à la décision	ininterrompues dans la mesure du possible
Autonomie en carburant	72 heures minimum
Autonomie en eau et en nourriture	72 heures minimum
CECIS (système commun de communication et d'information d'urgence) opérationnel	dans les 60 minutes
Premier rapport de situation opérationnelle à envoyer à l'ERCC	au cours du premier cycle de rapports opérationnels

ANNEXE III

Tableau d'appui pour l'analyse des processus opérationnels

Fonction essentielle 1	*Nom de la fonction.*
Description	*Description de la fonction et des tâches qu'elle comporte.*
Ressources	*Liste des ressources (informations, ensembles de données, services, produits, fournitures, dispositions budgétaires, équipements, systèmes TIC et exigences concernant les locaux) nécessaires pour remplir cette fonction et des entités externes qui les fournissent, le cas échéant.*
Production	*Liste des informations, produit(s), service(s) ou action(s) générés cette fonction, ainsi que des organisation(s), entité(s) ou groupe(s) concerné(s) qui les reçoi(ven)t.*
Responsabilité (pour la validation ou l'autorisation)	*Liste des postes associés à un rôle de validation ou d'autorisation nécessaire pour remplir cette fonction, le cas échéant.*
Personnel critique	*Liste des postes occupés par les membres du personnel exerçant une fonction critique, et profil, expertise et formation de ces derniers, le cas échéant (par exemple, habilitation de sécurité).*
Installations	*Liste des implantations/locaux où est exercée la fonction critique.*
Équipements et systèmes	*Liste des équipements, systèmes et dispositions nécessaires à l'exercice de cette fonction. Par exemple, locaux sécurisés, ordinateurs pour les communications cryptées, murs d'images, salles pour les réunions à haut niveau, équipements pour la visioconférence ou ordinateurs permettant l'accès au réseau de communication «Services télématiques transeuropéens entre administrations» (TESTA).*
Registres essentiels	*Liste des données et des informations nécessaires à l'exercice de la fonction.*
Dépendances et interdépendances	*Liste des relations ou accords entre les éléments qui précèdent. Le cas échéant, nature des relations ou accords, services essentiels nécessaires (par exemple, alimentation électrique, TIC), incidences en cas de perturbation du service ou de l'approvisionnement, et accords conclus avec les entités qui fournissent ces services ou ces fournitures. L'évaluation devrait également décrire les interdépendances entre les différents éléments, notamment les effets en cascade lorsque la perturbation d'un service (par exemple, l'électricité ou les TIC) affecte d'autres services et que l'incidence opérationnelle s'en trouve amplifiée.*
Sauvegardes	*Liste des ressources ou dispositifs de substitution qui seraient activés pour prendre le relais et garantir le fonctionnement si les ressources ou dispositifs principaux venaient à être affectés par l'événement perturbateur.*

ANNEXE IV

Orientations pour l'application de mesures d'atténuation et de prévention

La présente section fournit des orientations pour l'application de mesures d'atténuation et de prévention, exposées selon les différentes catégories d'événements perturbateurs. Afin d'éviter les répétitions, les mesures applicables à plusieurs de ces catégories ne sont détaillées qu'une seule fois, dans la première catégorie concernée.

— Indisponibilité des locaux:

— *Répartition géographique du PCN entre deux ou plusieurs centres géographiquement distincts opérant simultanément, qui s'apportent mutuellement assistance, en cas d'incapacité à agir ou de dépassement de leurs capacités respectives*. Chaque implantation devrait fonctionner 24 heures sur 24 et être entièrement équipée pour gérer toute la charge de travail au cas où l'un des autres sites ou l'ensemble de ceux-ci deviennent temporairement non opérationnels. En outre, les sites devraient être choisis sur la base d'une analyse des risques concernant les différentes zones de risque et l'accessibilité, avec des sites primaires et des sites de substitution situés dans différentes zones de risque et accessibles par différentes voies de transport. Par exemple, dans les zones sujettes aux tremblements de terre, les sites devraient être répartis sur des plaques tectoniques différentes; dans les zones sujettes aux inondations, ils devraient être établis à des niveaux d'élévation sensiblement différents ou dans des bassins hydrographiques différents.

— *Transfert vers des locaux de substitution gérés par l'autorité du PCN*. Envisager la mise en place d'au moins deux sites de substitution. L'un d'entre eux devrait être situé à proximité des locaux principaux afin de faciliter un transfert et une reprise des fonctions essentielles les plus rapides possible. L'autre site de remplacement devrait être suffisamment éloigné du premier, de manière à garantir que des événements perturbateurs majeurs tels que des inondations ou des tempêtes de neige n'aient pas d'incidence sur les deux sites simultanément. Veiller à la sécurité des informations et des communications et à la compatibilité des équipements et des systèmes TIC essentiels tels que le CECIS ou les équipements nécessaires aux communications classifiées, tant sur les sites principaux que sur les sites de substitution.

— *Transfert du personnel essentiel vers des locaux de substitution selon des modalités préétablies (notamment en cas de conditions météorologiques défavorables)*. Afin de garantir la disponibilité d'un personnel suffisant, prendre des dispositions pour transférer le personnel essentiel en cas d'activation du plan de continuité opérationnelle, en prévoyant un transfert vers des locaux de substitution, ou en recourant à des unités mobiles éloignées. Prendre en considération les perturbations potentielles sur les axes de transport telles que des encombrements et des blocages dus à de mauvaises conditions météorologiques, à des défaillances des infrastructures, à des troubles civils ou à d'autres causes.

— *Travail à distance (impliquant une flexibilité des tâches susceptibles d'être effectuées en dehors de l'emplacement physique du PNC)*. Déterminer quelles fonctions essentielles ou actions relevant de ces fonctions peuvent être exécutées à distance. Le fait que ces fonctions/actions ne dépendent pas d'équipements ou de systèmes accessibles exclusivement sur les sites physiques principaux permettrait cette exécution à distance. Envisager la mise en place d'un plan ou d'un système d'urgence permettant de restructurer les tâches du personnel, en permettant à certains membres du personnel de travailler depuis leur domicile et en en relocalisant d'autres dans des locaux de substitution.

— *Unités mobiles de commandement et de contrôle qui pourraient accueillir temporairement le personnel essentiel du PCN*. Ces unités devraient soutenir l'exécution des fonctions essentielles depuis un environnement mobile, notamment en veillant à l'accessibilité des systèmes d'information opérationnels et du CECIS. Leurs équipements et le degré d'autosuffisance requis devraient être définis afin de garantir l'état de préparation opérationnelle voulu. Ces unités devraient être conçues pour soutenir les opérations en apportant une assistance temporaire aux sites principaux pendant une période prédéfinie.

— *Activation de conventions administratives avec d'autres autorités en vue de l'utilisation de leurs locaux*. Conclure des accords avec d'autres autorités nationales ou infranationales en vue d'une utilisation partagée temporaire de leurs locaux. Évaluer la configuration, les systèmes, les équipements et les mesures de sécurité nécessaires aux fins d'une exécution efficace des fonctions essentielles. Veiller à ce que ces accords prévoient des exercices et des tests réguliers pour valider l'état de préparation et l'adéquation de ces installations de substitution.

— *Délégation*. Veiller à ce que des dispositions soient prises en vue de la mise en place d'un système permettant de déléguer les fonctions voulues à d'autres autorités nationales.

— Défaillances de l'approvisionnement en électricité:

— *Activation de groupes électrogènes et de systèmes d'alimentation sans interruption (UPS)*. Fournir des générateurs et des systèmes UPS dimensionnés suffisamment puissants pour garantir la continuité des fonctions essentielles du PCN pendant une période minimale définie. Leur capacité devrait être suffisante pour répondre aux besoins opérationnels en cas de pannes d'alimentation prolongées. Les générateurs et les systèmes UPS devraient être testés régulièrement afin de garantir l'état de préparation opérationnelle voulu.

— *Conventions et accords d'approvisionnement prioritaire en combustibles avec les fournisseurs*. Les conventions d'approvisionnement en combustibles devraient garantir la continuité des opérations et être fondées sur la capacité de stockage de combustible sur site et la consommation de combustible attendue. Des mesures supplémentaires peuvent inclure la disponibilité de réservoirs de combustible mobiles équipés de systèmes de pompage et/ou des accords d'approvisionnement prioritaires avec des fournisseurs situés à proximité.

— *Autonomie énergétique et sources d'énergie alternatives pour les fonctions essentielles*. Le PCN devrait, dans la mesure du possible, être en mesure de fonctionner indépendamment du réseau électrique national. En cas de panne du réseau pendant plusieurs jours, comme cela peut se produire lors de catastrophes majeures, la continuité pourrait être maintenue grâce à des sources d'énergie diversifiées et à un microréseau autonome, par exemple, un microréseau d'énergie éolienne ou solaire. Envisager la mise en place de sources d'énergie alternatives, comme des panneaux photovoltaïques avec accumulateur, d'une puissance suffisante pour garantir les fonctions essentielles du PCN.

— *Maximisation de la capacité électrique disponible*. Établir des protocoles internes pour maximiser la capacité électrique disponible en limitant l'utilisation d'équipements non essentiels et en mettant progressivement hors tension les éléments qui ne sont pas nécessaires pour soutenir les fonctions essentielles, ce qui permet d'augmenter l'autonomie électrique de secours sans investissements supplémentaires.

— *Transfert vers des locaux de substitution gérés par l'autorité du PCN et alimentés en électricité* (les recommandations pertinentes figurent sous «Indisponibilité des locaux»).

— *Travail à distance à partir d'un bâtiment dont l'alimentation électrique est garantie* (les recommandations pertinentes figurent sous «Indisponibilité des locaux»).

— *Unités mobiles de commandement et de contrôle autosuffisantes en électricité* (les recommandations pertinentes figurent sous «Indisponibilité des locaux»)

— *Activation de conventions administratives avec d'autres autorités en vue de l'utilisation de leurs locaux, prévoyant un approvisionnement en électricité garanti* (les recommandations pertinentes figurent sous «Indisponibilité des locaux»).

— *Délégation* (les recommandations pertinentes figurent sous «Indisponibilité des locaux»).

— Défaillance ou panne des systèmes TIC:

— *Redondances*. Les redondances empêchent la défaillance d'un composant d'interrompre la fonction qu'il assure. Le PCN devrait mettre en place des redondances à des niveaux complémentaires: i) les équipements (duplication des composants essentiels), ii) la connectivité (fournisseurs multiples et voies d'accès diverses, et iii) les applications et les données (reproduction de bases de données et de documents essentiels sur un site secondaire). Les dispositifs de redondance devraient être dotés d'une capacité suffisante pour soutenir les opérations en cas de défaillance de l'environnement TIC principal et devraient être testés périodiquement afin de garantir une préparation et un basculement fluide en cas de perturbation. Ils doivent éviter les dépendances partagées avec le système primaire, telles que la même source d'énergie, le même fournisseur ou la même infrastructure physique, pour éviter les pannes simultanées.

— Les lignes en fibre optique sont très vulnérables aux déplacements terrestres, ce qui peut entraîner une atténuation ou une perte du signal et des interruptions de service. Pour atténuer ce risque, le relais satellitaire est la mesure de redondance standard recommandée, permettant au réseau de secours de conserver la même appréciation de la situation que le réseau primaire. La mise en miroir des données géographiques devrait être de type actif-actif, les environnements primaires et de secours étant synchronisés de manière à ce que les deux puissent se relayer de manière fluide. Cette approche redondante et de type miroir favorise une disponibilité et des performances élevées des réseaux de fibre optique.

— *Sauvegardes de données régulières et sécurisées, y compris des copies hors site et hors ligne*. Établir et maintenir une politique de sauvegarde structurée pour toutes les données et configurations qui sont essentielles aux opérations des PCN. Cette politique devrait définir les éléments devant être sauvegardés, la fréquence de sauvegarde, les emplacements de stockage (y compris les copies hors site ou hors ligne) ainsi que le responsable de leur gestion. Les sauvegardes devraient être cryptées et protégées contre tout accès non autorisé.

— *Systèmes TIC et canaux de communication de substitution*. Mettre en place des outils et canaux de substitution qui peuvent être utilisés en cas de panne des systèmes ou réseaux TIC primaires. Il peut s'agir de communications par satellite, d'unités de radio mobile à haute fréquence (HF), à très haute fréquence (VHF) ou à ultra-haute fréquence (UHF), de lignes téléphoniques analogiques, d'applications de messagerie sécurisée ou de plateformes web hébergées en dehors de l'infrastructure principale. Le personnel doit savoir quand et comment passer à ces solutions de substitution.

— *Équipes d'aide TIC d'urgence/unités d'intervention technique de garde*. Permettre un accès rapide à l'aide TIC, que celle-ci soit fournie en interne (au sein de l'organisation) ou par un prestataire externe, en définissant des modalités claires de disponibilité et de réaction afin que l'assistance technique puisse être mobilisée rapidement en cas de besoin, pour assurer une récupération rapide des systèmes TIC.

— *Procédures de réponse aux incidents de cybersécurité coordonnées avec l'autorité nationale de cybersécurité*. Établir des protocoles de coordination avec l'autorité nationale de cybersécurité, y compris des canaux d'alerte précoce, des procédures conjointes de réaction aux incidents, et des rôles et responsabilités clairement définis lors d'un cyberincident touchant le PCN.

— *copies hors ligne des listes de contacts essentiels, des procédures clés et des documents opérationnels*. Des informations telles que les listes de contacts, les procédures en cas d'incident et les procédures clés devraient être disponibles dans des formats qui peuvent être utilisés sans nécessiter d'accès aux principaux systèmes TIC.

— *Unités mobiles de commandement et de contrôle ayant accès aux systèmes TIC primaires et de secours* (les recommandations pertinentes figurent sous «Indisponibilité des locaux»)

— *Transfert vers des locaux de substitution gérés par l'autorité du PCN et ayant accès aux systèmes TIC primaires et de secours* (les recommandations pertinentes figurent sous «Indisponibilité des locaux»)

— *Activation de conventions administratives avec d'autres autorités en vue de l'utilisation de leurs locaux ayant accès aux systèmes TIC* (les recommandations pertinentes figurent sous «Indisponibilité des locaux»)

— Absence massive de personnel et pénurie de personnel essentiel:

— *Gestion des heures supplémentaires (solution à court terme)*. Établir un protocole pour les heures supplémentaires qui définit: des seuils clairs déclenchant le recours aux heures supplémentaires; la ou les personnes pouvant l'autoriser; les limites (durée maximale du service, durée maximale hebdomadaire et nombre maximal de jours consécutifs); les périodes minimales de repos entre chaque service et au terme de la durée maximale hebdomadaire ou du nombre maximal de jours consécutifs; un système de rotation équitable afin que le même personnel ne soit pas sollicité de manière répétée; un système d'enregistrement des heures supplémentaires; une rémunération supplémentaire préétablie; et un soutien pratique pendant les heures supplémentaires (par exemple, repas, aires de repos et transport vers le domicile si nécessaire).

— *Réaffecter des fonctions essentielles au personnel disponible*. Préparer des dispositions d'urgence précisant comment les fonctions essentielles seront réaffectées en l'absence de personnel clé. Il s'agit notamment d'identifier le personnel de remplacement pour chaque rôle essentiel et de simplifier les procédures dans la mesure du possible.

— *Un groupe prédéfini de personnel formé au sein de l'établissement, disponible rapidement*. Mettre en place un système visant à mobiliser le personnel de secours en puisant dans une réserve prédéfinie, en définissant des règles claires précisant qui peut mobiliser le personnel de secours et comment, y compris les critères d'activation, le(s) canal/canaux de communication pour la mobilisation, les exigences en matière de personnel (telles que l'habilitation de sécurité, la formation ou l'expertise) et les modalités de traitement du temps de repos ou des heures supplémentaires, et prévoir des réexamens réguliers pour s'assurer du bon fonctionnement du système. Veiller à ce que ces règles soient bien connues du personnel de cette réserve.

— Cette réserve peut être constituée par les moyens suivants: i) formation transversale du personnel d'autres unités — mettre en œuvre des programmes de formation transversale afin que plusieurs membres du personnel puissent exercer les mêmes fonctions essentielles, en mettant l'accent sur les rôles pour lesquels une pénurie a été constatée; et ii) une «réserve dormante» d'anciens membres essentiels du personnel des PCN — transférer du personnel en dehors des tâches des PCN vers d'autres départements après une période déterminée afin de créer une réserve dormante de personnel de réserve. Le maintien de cette réserve dormante permet une forte augmentation des effectifs et une activation rapide, en contournant les mois de formation et d'habilitation de sécurité généralement requis pour ces rôles sensibles. Dans les deux cas, des dispositions devraient être formalisées pour faire en sorte que le personnel appartenant à la réserve conserve son expertise au moyen de formations périodiques de remise à niveau et puisse être rapidement mobilisé en cas de crise majeure.

— *Définir des priorités dans le recrutement du personnel*. Le fonctionnement continu 24 h/24 et 7 jours sur 7 des PCN nécessite des effectifs stables. Le PCN peut envisager de donner la priorité, en matière de recrutement, aux postes de soutien aux fonctions essentielles et d'anticiper les pénuries prévisibles de personnel (par exemple, départs simultanés à la retraite ou expiration de contrats à durée déterminée), afin de lancer les procédures de recrutement suffisamment à l'avance. Les mesures possibles peuvent inclure l'élaboration de procédures de recrutement accélérées; en outre, la formation continue du personnel existant peut favoriser la stabilité du personnel, en permettant la mobilité interne, le développement des compétences et la succession pour les fonctions essentielles.

— *Investissement dans la rétention du personnel essentiel*. Afin de conserver le personnel travaillant dans les PCN, la motivation devrait être soutenue par une combinaison d'avantages et d'incitations. Les incitations non financières peuvent inclure des congés prolongés après une certaine période de service, des modalités d'affectation flexibles soumises à des exigences minimales en matière de couverture de service, des zones de repos sur site, des mesures de soutien familial (par exemple, l'accès à des services de garde d'enfants) et l'accès à des services gratuits ou à prix réduit en matière de transports publics, de soins de santé, de culture ou de sport.

— *Soutien des familles du personnel essentiel*. La disponibilité des membres du personnel essentiel peut dépendre des membres de leur famille, en particulier si ces derniers sont vulnérables ou laissés seuls sans assistance. Envisager de mettre en place, le cas échéant, des dispositions visant à protéger les familles du personnel essentiel des PCN, en donnant la priorité à leur sécurité afin que les membres du personnel puissent rester opérationnels.

— *Prévenir les pénuries de personnel en déléguant l'autorité et en promouvant le partage des responsabilités*. Veiller à ce que les responsabilités et les tâches soient clairement définies. Établir des protocoles pour l'autorité délégante. Identifier les remplaçants et leurs fonctions respectives. Ces remplaçants sont censés intervenir en cas d'indisponibilité des décideurs responsables des fonctions essentielles. Précisez les circonstances et l'ordre dans lequel ils assumeraient ces rôles. Lorsque la décision et les responsabilités le permettent, assurer le renforcement des capacités et une formation régulière permettant d'exercer l'autorité en cas de perturbation. Examiner si la répartition ou le partage des responsabilités entre plusieurs membres du personnel à l'aide d'un système de rotation est faisable et utile pour éviter les pénuries de personnel. Envisager de tenir à jour un manuel à l'intention des nouveaux membres du personnel, conçu pour permettre aux collègues moins expérimentés de gérer un large éventail de tâches de manière indépendante tout en veillant au respect des normes et protocoles établis.

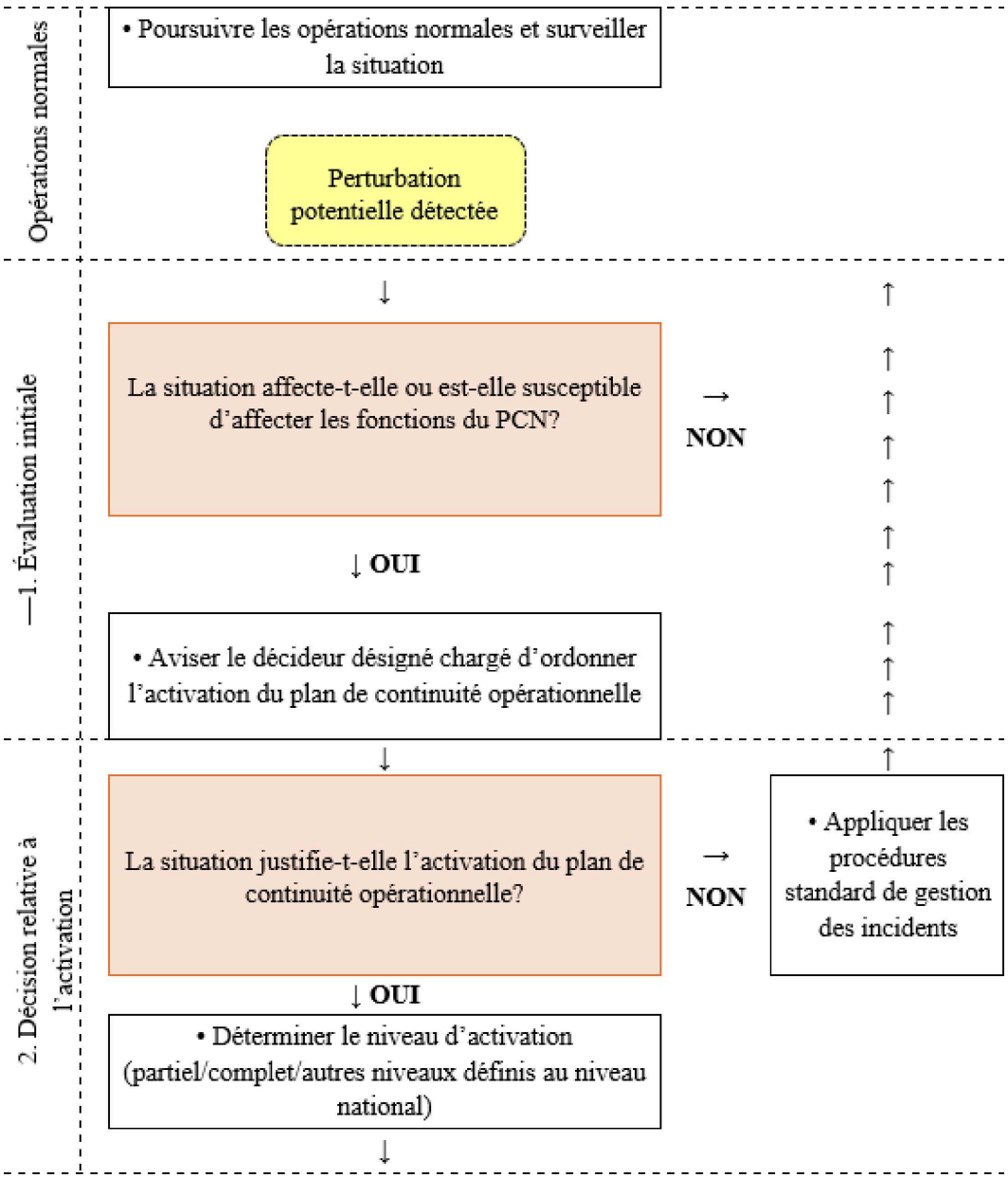
ANNEXE V

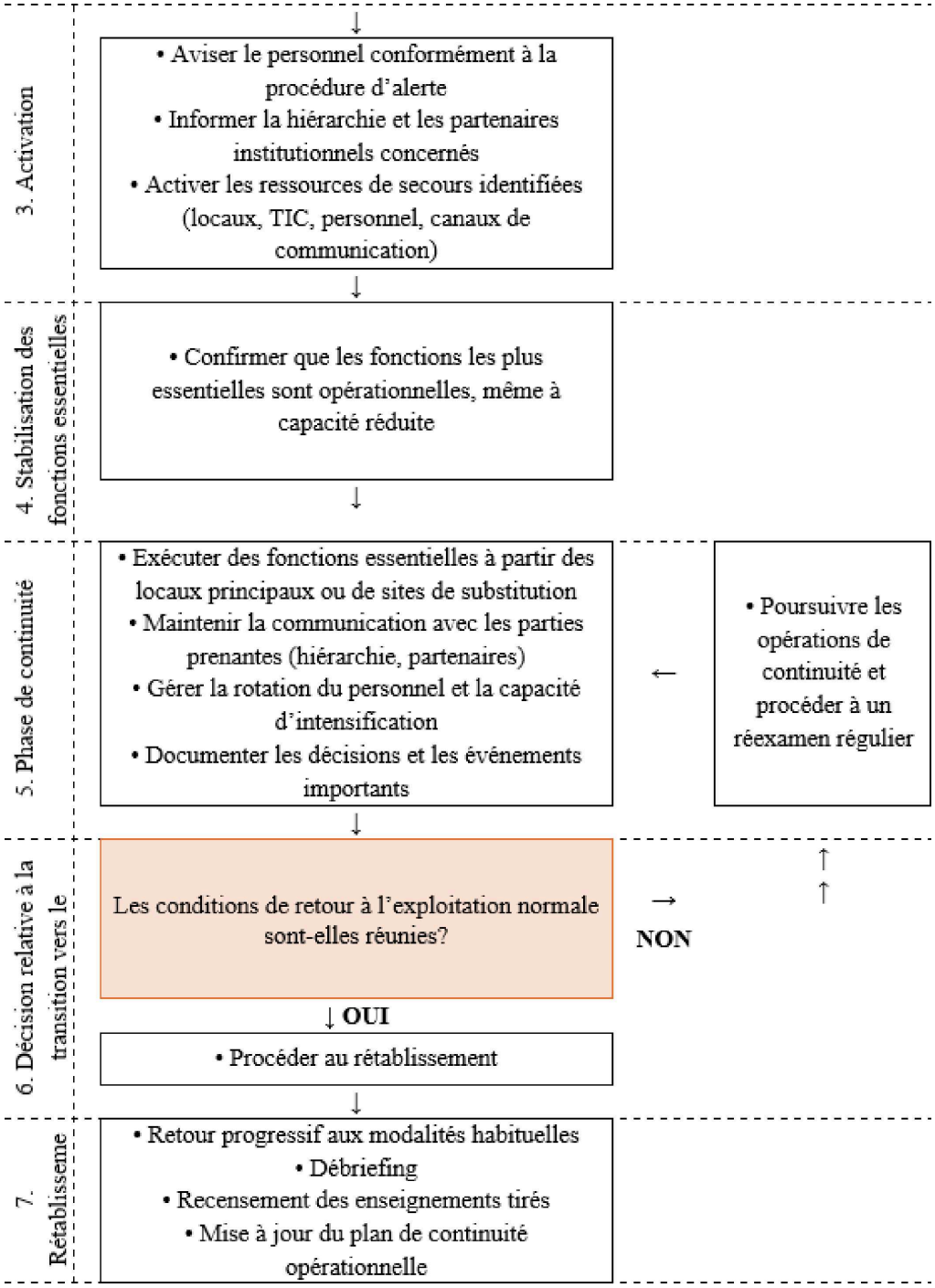
Outils de référence opérationnels

La présente annexe fournit un outil de référence opérationnel que les PCN devraient envisager d'utiliser lors de l'élaboration ou de la révision de leur plan de continuité opérationnelle.

Illustration du flux d'activation

Le flux ci-dessous est un exemple de la manière dont l'activation d'un plan de continuité opérationnelle peut être organisée, depuis le moment où une perturbation potentielle est détectée jusqu'au moment où le PCN entre dans une phase de continuité stable. Il est structuré autour de points de décision, et non de délais prescrits.




3. Activation
• Aviser le personnel conformément à la procédure d'alerte
• Informer la hiérarchie et les partenaires institutionnels concernés
• Activer les ressources de secours identifiées (locaux, TIC, personnel, canaux de communication)
4. Stabilisation des fonctions essentielles
• Confirmer que les fonctions les plus essentielles sont opérationnelles, même à capacité réduite
5. Phase de continuité
• Exécuter des fonctions essentielles à partir des locaux principaux ou de sites de substitution
• Maintenir la communication avec les parties prenantes (hiérarchie, partenaires)
• Gérer la rotation du personnel et la capacité d'intensification
• Documenter les décisions et les événements importants
←
• Poursuivre les opérations de continuité et procéder à un réexamen régulier
6. Décision relative à la transition vers le
Les conditions de retour à l'exploitation normale sont-elles réunies?
→ NON
↓ OUI
• Procéder au rétablissement
7. Rétablisseme
• Retour progressif aux modalités habituelles
• Débriefing
• Recensement des enseignements tirés
• Mise à jour du plan de continuité opérationnelle

ANNEXE VI

Principaux points à aborder lors de l'élaboration d'une stratégie de communication ([1])

— Recenser les différents groupes cibles, sous la responsabilité de l'organisation en matière de communication, susceptibles d'être touchés par la perturbation des activités du PCN ou qui devraient être informés si l'organisation subit un événement perturbateur, et notamment:

  (a) les niveaux supérieurs de l'organisation, y compris le niveau décisionnel;

  (b) le personnel de l'organisation;

  (c) les parties prenantes qui contribuent aux fonctions essentielles de l'organisation;

  (d) les parties prenantes qui sont destinataires des fonctions essentielles de l'organisation;

  (e) les médias;

  (f) le grand public.

— Pour chaque groupe cible, définir l'objectif de la communication en cas d'événement perturbateur. Chaque groupe pourrait avoir besoin d'un type, d'un format et d'un contenu d'information différents. Le(s) canal/canaux de communication utilisé(s) pourrai(en)t également différer.

— Rédiger des messages préétablis qui soient clairs, concis, cohérents et pérennes pour tous les destinataires et tous les canaux. Veiller à ce qu'ils soient adaptés au groupe cible, en répondant à leurs besoins spécifiques en matière d'information.

— Identifier différents canaux de communication pour chaque groupe cible afin d'assurer une communication efficace si la perturbation a une incidence sur les canaux standard.

— Privilégier l'information proactive par rapport à l'information réactive.

— Lorsque la stratégie de communication prévoit la possibilité de diffuser des messages par l'intermédiaire de la télévision et de la radio publiques, coordonner la chronologie de ces messages avec les émissions d'information afin d'assurer une intégration efficace et une large diffusion au sein de la population.

— Dans le cadre de la stratégie de communication, envisager de préassigner le rôle de responsable de l'information à un poste donné, en précisant les tâches à assumer avant, pendant et après un événement perturbateur.

([1]) Ces propositions de points à aborder en vue de l'élaboration d'une stratégie de communication ne tiennent pas compte de la gestion de la mésinformation ou de la désinformation.

ANNEXE VII

Exemples de scénarios

Exemple de scénario 1

Le problème: *panne de courant suivie d'une perte de données.*

Le lieu: *la panne de courant affecte la zone où se trouvent les principaux locaux du PCN.*

La durée: *24 heures.*

Description du problème: *les travaux de réparation à proximité des locaux du PCN ont causé des dommages au réseau de distribution d'électricité. La panne soudaine de courant a causé des dommages aux systèmes informatiques du PCN, entraînant une perte de données. Les travaux de rétablissement du courant devraient durer 24 heures. La panne informatique dure 24 heures.*

Exemple de scénario 2

Le problème: *inaccessibilité des locaux en raison de la persistance de la couverture neigeuse.*

Le lieu: *l'ensemble de la zone où se trouvent les locaux est concerné.*

La durée: *plus d'une semaine.*

Description du problème: *une importante tempête de neige a frappé la zone où se trouvent les locaux du PCN, les rendant inaccessibles par la route et les transports publics. Les chutes de neige sont si importantes que les chasse-neige ne suffisent pas à déblayer toutes les routes principales pendant les 24 premières heures, la priorité étant donnée à l'accès aux hôpitaux. Il a été demandé à la population de ne pas emprunter les rues. Pendant au moins 48 heures, l'accès aux installations du PCN par transport public ou véhicule privé est impossible. La vague de froid se poursuit dans la région pendant plus d'une semaine et la couverture neigeuse sur les routes secondaires se maintient pendant une semaine. Par conséquent, un tiers des membres du personnel appelés à travailler dans les jours qui suivent en sont empêchés pendant une semaine, car leur lieu de résidence est éloigné et les routes secondaires sont les dernières à être déblayées.*

En outre, le personnel essentiel en service le jour des chutes de neige est bloqué dans les locaux pendant les 48 premières heures. Environ un tiers d'entre eux a déjà atteint le quota hebdomadaire maximal d'heures de travail, et un autre tiers atteindra ce quota dans un délai de 24 heures. Par conséquent, ils sont en droit d'obtenir une période de repos suffisante. Ils ont également besoin d'un soutien pour répondre à leurs besoins fondamentaux (nourriture, hygiène personnelle) et, dans certains cas, de mesures de soutien à leurs familles et/ou d'évacuation.

ANNEXE VIII

Cadre d'évaluation proposé pour les tests de résistance

Les résultats du test de résistance devraient être évalués au regard de deux dimensions distinctes mais complémentaires:

— *Conformité avec le plan de continuité opérationnelle*. Il s'agit d'évaluer dans quelle mesure le PCN a mis en œuvre les dispositifs de continuité opérationnelle applicables pendant le test de résistance, y compris les structures décisionnelles pour l'activation, l'escalade et le rétablissement, la coordination et la communication internes et externes, les dispositifs de transfert et l'utilisation de ressources de secours.

— *Maintien des fonctions essentielles et réalisation des objectifs de performance opérationnelle mesurables prédéfinis*. Il s'agit d'évaluer si les fonctions essentielles du PCN ont été maintenues ou rétablies dans des limites prédéfinies acceptables, s'il y a eu des effets négatifs sur d'autres fonctions non essentielles du PCN et si le test de résistance a permis d'atteindre les objectifs de performance mesurables prédéfinis. Des exemples d'objectifs de performance opérationnelle sont fournis à l'annexe II.

Les deux dimensions devraient être évaluées séparément afin de déterminer plus précisément les points à améliorer. Cette distinction aide à garantir que la conformité avec le plan de continuité opérationnelle soit évaluée séparément de l'efficacité des résultats opérationnels. Le rapport d'évaluation doit présenter ses résultats sous la forme de deux notes complémentaires: l'une reflétant la conformité avec le plan de continuité opérationnelle et l'autre le maintien des fonctions essentielles et la réalisation des objectifs de performance opérationnelle mesurables prédéfinis.

Grille d'évaluation de la conformité avec le plan de continuité opérationnelle

Note (0-3)	Description
0: non-conformité	*L'exercice n'a montré que peu ou pas de conformité avec les dispositions de continuité opérationnelle. Les procédures essentielles étaient absentes, mal exécutées ou ignorées.*
1: conformité partielle	*Certains points des dispositions relatives à la continuité ont été appliqués, mais d'autres points importants n'ont pas été correctement respectés, ont été appliqués trop tard ou se sont révélés insuffisants dans la pratique. Le test a révélé d'importantes faiblesses et d'importants axes d'amélioration du plan.*
2: conformité globale, seuls des écarts mineurs recensés	*Le test de résistance a été largement mis en œuvre conformément au plan de continuité opérationnelle. Les écarts par rapport au plan étaient limités. Le test a révélé quelques faiblesses et axes d'amélioration du plan.*
3: entière conformité	*Le plan de continuité opérationnelle a été intégralement suivi au cours du test de résistance.*

Grille d'évaluation du maintien des fonctions essentielles et de la réalisation des objectifs de performance opérationnelle mesurables prédéfinis

Note (0-3)	Description
0: objectifs non atteints	*Les fonctions essentielles des PCN ont été suspendues ou retardées au-delà des limites prédéfinies acceptables. D'autres fonctions non essentielles du PCN ont été fortement et négativement affectées. Les objectifs de performance mesurables prédéfinis n'ont pas été atteints.*
1: objectifs atteints, mais présence de difficultés majeures	*Une ou plusieurs fonctions essentielles n'ont été rétablies qu'après un retard important dépassant les limites acceptables. Le test de résistance peut également avoir provoqué des perturbations importantes ou avoir nui à d'autres fonctions du PCN. Les objectifs de performance mesurables prédéfinis n'ont été atteints que partiellement ou avec des difficultés majeures.*

Note (0-3)	Description
2: objectifs atteints, présence d'écarts mineurs	*Les fonctions essentielles ont été maintenues ou rétablies dans des marges de tolérance acceptables (et les limites acceptables prédéfinies dépassées pendant une durée limitée) sans incidence significative sur les autres fonctions des PCN. Les objectifs de performance mesurables prédéfinis ont été largement atteints et seuls des écarts mineurs par rapport aux limites établies ont été recensés.*
3: objectifs pleinement atteints	*Les fonctions essentielles évaluées par le test de résistance ont été maintenues ou rétablies sans retard dépassant les limites acceptables prédéfinies et sans incidence négative sur les autres fonctions des PCN. Les objectifs de performance mesurables prédéfinis ont été pleinement atteints.*

ANNEXE IX

Évaluation du test de résistance, recensement des enseignements et propositions d'amélioration [1]

Dans le cadre du processus d'évaluation, il est recommandé de définir des stratégies visant à améliorer les domaines qui n'ont pas été abordés de manière adéquate lors du test de résistance. En outre, les PCN devraient envisager d'intégrer les éléments positifs que l'exercice a révélés mais qui ne sont pas inclus dans le plan de continuité opérationnelle actuel.

Le tableau suivant vise à faciliter la compilation et l'alignement des éléments de l'évaluation, le recensement des enseignements tirés et les propositions d'amélioration au terme du test de résistance.

Conformité avec le plan de continuité opérationnelle	*Note (0-3)* … *Description...*
Maintien des fonctions essentielles et réalisation des objectifs de performance opérationnelle mesurables prédéfinis	*Note (0-3)* … *Description...*
Constatations et observations	…
Lacunes et enseignements tirés	…
Propositions d'amélioration	…
Actions nécessaires à la mise en œuvre	…

[1] Ce tableau d'évaluation se fonde sur la boîte à outils sur la continuité des ressources mise au point par l'Agence fédérale de gestion des situations d'urgence (FEMA) pour aider les populations et les autorités/organisations locales à élaborer des plans de continuité opérationnelle et a été adapté à l'exercice de test de résistance.

ANNEXE X

Formulaire de retour d'information du participant

Le questionnaire suivant est recommandé comme modèle pour recueillir les réactions des participants aux tests de résistance. Il convient d'adapter les questions à la portée et à l'objet spécifiques du test de résistance. À l'aide des réponses à ces questions ou à des questions similaires auprès des participants aux tests de résistance, des observateurs ou du personnel concerné par des événements perturbateurs réels, il est possible de recenser les enseignements et les lacunes, qui peuvent ensuite être utilisés pour mettre à jour le plan de continuité opérationnelle du PCN.

Activation du plan de continuité opérationnelle:

— Les protocoles établis ont-ils été respectés?

— Dans la négative, quelles étaient les raisons de l'écart, et s'agissait-il d'une erreur/d'un problème ou d'un ajustement positif/optimisant?

— Dans quelle mesure l'exécution des protocoles était-elle efficace?

— Quelles difficultés ont été rencontrées?

— La communication était-elle claire et efficace lors de l'activation?

— L'ensemble du personnel essentiel a-t-il été informé et mobilisé en temps utile?

Reprise opérationnelle, continuité et performances des fonctions essentielles:

— Quel a été le temps nécessaire pour reprendre les fonctions essentielles dont vous êtes responsable?

— Toutes les fonctions essentielles ont-elles été exécutées de manière efficace et dans les délais prévus? Évaluez la qualité des résultats fournis dans les conditions du test.

— Des retards ou des inefficacités ont-ils été constatés dans l'exécution de ces fonctions?

— A-t-il été nécessaire d'accorder la priorité à certaines fonctions essentielles au cours de l'exercice?

— Comment la hiérarchisation des priorités a-t-elle été décidée et communiquée?

— La hiérarchisation des priorités a-t-elle permis d'assurer la continuité et l'efficacité?

Équipements et systèmes TIC:

— Tous les équipements de secours nécessaires étaient-ils disponibles et pleinement opérationnels?

— Les systèmes de secours pour l'approvisionnement en électricité ont-ils été testés et étaient-ils pleinement opérationnels?

— Les outils et canaux de communication de secours ont-ils été testés et étaient-ils pleinement fonctionnels?

— D'autres services et fournitures essentiels étaient-ils disponibles, ont-ils été testés et étaient-ils pleinement opérationnels?

— Des retards ou des inefficacités causés par les systèmes TIC ont-ils été constatés?

— Dans quelle mesure les problèmes ont-ils été résolus?

Autres installations:

— L'autre emplacement est-il adéquat en termes de taille, d'agencement et d'équipement pour vous permettre de travailler pendant une longue période (plusieurs jours)? Si tel n'est pas le cas, pourquoi et que pourrait-on faire pour l'améliorer?

Communication et coordination:

— Tous les participants, y compris la hiérarchie et les équipes ou collègues concernés, ont-ils été correctement informés?

— La communication et la coordination internes ont-elles été effectivement maintenues tout au long de l'exercice, y compris avec la hiérarchie?

— La communication et la coordination avec l'ERCC ont-elles été effectivement maintenues tout au long de l'exercice?

— Le cas échéant, dans quelle mesure la communication avec l'ERCC depuis le site de secours a-t-elle été efficace?

— Comment les informations ont-elles été échangées et consignées au cours du transfert ou de la perturbation?

Formation et bien-être du personnel:

— Pensez-vous que la formation à la continuité opérationnelle vous a bien préparé(e) à l'exercice?

— Avez-vous été bien informé(e) de l'exercice une fois que celui-ci avait commencé?

— Les rôles ont-ils été clairement définis au cours de l'exercice?

— L'exercice a-t-il été utile à des fins de formation du personnel?

— Vos besoins personnels et familiaux ont-ils été pris en considération, par exemple vos besoins en matière de transport, de repos, d'eau ou de nourriture?

Autres observations générales:

— Quels aspects de l'exercice ont rencontré le plus de succès?

— Quelles ont été les principales difficultés rencontrées?

— L'exercice a-t-il atteint ses objectifs?

— Sur la base de l'expérience acquise au cours de l'exercice, comment évaluez-vous la capacité du PCN à poursuivre ses activités dans les mêmes conditions pendant 1 semaine?

— Veuillez recenser les éventuelles ressources ou aides supplémentaires nécessaires pour un événement perturbateur similaire d'une durée plus longue que celle de l'exercice.

— Veuillez identifier les améliorations à apporter à la formation et aux exercices futurs.