COMMISSION
EUROPÉENNE

Bruxelles, le 23.6.2020
COM(2020) 255 final

ANNEX

ANNEXE

de la

proposition de décision du Conseil

relative à la position à prendre, au nom de l'Union européenne, au sein du comité mixte institué par l'accord entre l'Union européenne et la Confédération suisse sur le couplage de leurs systèmes d'échange de quotas d'émission de gaz à effet de serre en ce qui concerne l'adoption de procédures opérationnelles communes

DÉCISION Nº 1/2020 DU COMITÉ MIXTE INSTITUÉ PAR L'ACCORD ENTRE L'UNION EUROPÉENNE ET LA CONFÉDÉRATION SUISSE SUR LE COUPLAGE DE LEURS SYSTÈMES D'ÉCHANGE DE QUOTAS D'ÉMISSION DE GAZ À EFFET DE SERRE

du ...

relative à des procédures opérationnelles communes (POC)

LE COMITÉ MIXTE,

vu l'accord entre l'Union européenne et la Confédération suisse sur le couplage de leurs systèmes d'échange de quotas d'émission de gaz à effet de serre[1] (ci-après l'«accord»), et notamment son article 3,

considérant ce qui suit:

(1) La décision nº 2/2019 du comité mixte du 5 décembre 2019 a modifié les annexes I et II de l'accord, de sorte que les conditions requises pour le couplage prévues dans ledit accord sont réunies.

(2) À la suite de l'adoption de la décision nº 2/2019 du comité mixte et conformément à l'article 21, paragraphe 3, de l'accord, les parties ont échangé leurs instruments de ratification ou d'approbation, ayant estimé que toutes les conditions de couplage prévues dans l'accord étaient remplies.

(3) Conformément à l'article 21, paragraphe 4, de l'accord, ce dernier est entré en vigueur le 1er janvier 2020.

(4) Conformément à l'article 3, paragraphe 6, de l'accord, il convient que l'administrateur du registre suisse et l'administrateur central de l'Union établissent des procédures opérationnelles communes (POC) concernant les aspects techniques ou d'une autre nature nécessaires au fonctionnement du couplage entre le journal des transactions de l'Union européenne (EUTL) du registre de l'Union et le journal complémentaire des transactions suisse (SSTL) du registre suisse et tenant compte des priorités de la législation interne. Ces POC devraient prendre effet après qu'elles auront été adoptées par décision du comité mixte.

(5) Conformément à l'article 13, paragraphe 1, de l'accord, il convient que le comité mixte arrête des lignes directrices techniques pour assurer la bonne mise en œuvre de l'accord, y compris concernant les aspects techniques ou d'une autre nature nécessaires au fonctionnement du couplage et tenant compte des priorités de la législation interne. Ces lignes directrices techniques peuvent être élaborées par un groupe de travail institué conformément à l'article 12, paragraphe 5, de l'accord. Le groupe de travail devrait au moins comprendre l'administrateur du registre suisse et l'administrateur central du registre de l'Union et devrait en outre assister le comité mixte dans ses fonctions conformément à l'article 13 de l'accord.

(6) Compte tenu de la nature technique des lignes directrices et de la nécessité de les adapter aux évolutions en cours, il y a lieu de soumettre au comité mixte, pour information ou approbation, le cas échéant, les lignes directrices techniques élaborées par l'administrateur du registre suisse et l'administrateur central de l'Union,

[1] JO L 322 du 7.12.2017, p. 3.

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

Les procédures opérationnelles communes (POC) annexées à la présente décision sont adoptées.

Article 2

Un groupe de travail est institué en vertu de l'article 12, paragraphe 5, de l'accord. Il assiste le comité mixte afin de garantir la bonne application de l'accord, et en particulier l'élaboration de lignes directrices techniques pour la mise en œuvre des POC.

Le groupe de travail comprend au moins l'administrateur du registre suisse et l'administrateur central du registre de l'Union.

Article 3

La présente décision entre en vigueur le jour de son adoption.

Fait à Bruxelles, en langue anglaise, le XX 2020.

Par le comité mixte

Le secrétaire pour l'Union européenne	*Le président*	*Le secrétaire pour la Suisse*

APPENDICE

ANNEXE

PROCÉDURES OPÉRATIONNELLES COMMUNES (POC)

établies conformément à l'article 3, paragraphe 6, de l'accord entre l'Union européenne et la Confédération suisse sur le couplage de leurs systèmes d'échange de quotas d'émission de gaz à effet de serre
– Procédures relatives à une solution provisoire

1. GLOSSAIRE

Tableau 1-1 Sigles et définitions

Sigle/Terme	Définition
Autorité de certification (AC)	Entité chargée de délivrer des certificats numériques
CH	Confédération suisse
SEQE	Système d'échange de quotas d'émission
UE	Union européenne
IMT	Équipe de gestion des incidents
Ressource d'information	Information utile à une entreprise ou une organisation
TI	Technologies de l'information
ITIL	Bibliothèque pour l'infrastructure des technologies de l'information
ITSM	Gestion des services informatiques
NTC	Normes techniques de couplage
Registre	Système de comptabilisation des quotas délivrés au titre du SEQE, qui conserve la trace des changements de propriété des quotas détenus sur des comptes électroniques
DDC	Demande de changement
LIS	Liste d'informations sensibles
DDS	Demande de service
Wiki	Site web qui permet aux utilisateurs d'échanger des informations et des connaissances en ajoutant ou en adaptant directement des contenus au moyen d'un logiciel de navigation

2. INTRODUCTION

L'accord entre l'Union européenne et la Confédération suisse sur le couplage de leurs systèmes d'échange de quotas d'émission de gaz à effet de serre du 23 novembre 2017 (ci-après l'«accord») prévoit la reconnaissance mutuelle des quotas d'émission qui peuvent être utilisés à des fins de conformité dans le cadre du système d'échange de quotas d'émission de l'Union (ci-après le «SEQE-UE») ou du système d'échange de quotas d'émission de la Suisse (ci-après le «SEQE Suisse»). Pour rendre opérationnel le couplage entre le SEQE-UE et le SEQE suisse, un lien direct est établi entre le journal des transactions de l'Union européenne (EUTL) du registre de l'Union et le journal complémentaire des transactions suisse (SSTL) du registre suisse, ce qui permettra le transfert de registre à registre des quotas d'émission délivrés au titre de chaque SEQE (article 3, paragraphe 2, de l'accord). Afin de rendre effectif le couplage entre le SEQE-UE et le SEQE suisse, une solution provisoire est mise en place avant mai 2020 ou dès que possible après cette date. Les parties coopèrent pour remplacer dès que possible la solution provisoire par un couplage permanent des registres (annexe II de l'accord).

Conformément à l'article 3, paragraphe 6, de l'accord, l'administrateur du registre suisse et l'administrateur central de l'Union établissent des procédures opérationnelles communes (POC) concernant les sujets techniques ou d'une autre nature nécessaires au fonctionnement du couplage et tenant compte des priorités de la législation interne. Les POC établies par les administrateurs prennent effet une fois qu'elles ont été adoptées par décision du comité mixte.

Les POC décrites dans le présent document doivent être adoptées par le comité mixte en vertu de sa décision nº 1/2020. Par la présente décision, le comité mixte charge l'administrateur du registre suisse et l'administrateur central de l'Union d'élaborer de nouvelles lignes directrices techniques visant à rendre opérationnel le couplage et de veiller à ce que ces lignes directrices soient constamment adaptées au progrès technique et aux nouvelles exigences en matière de sécurité et de sûreté du lien, ainsi qu'au fonctionnement efficace et efficient de celui-ci.

2.1. Champ d'application

Le présent document représente la conception commune des parties à l'accord en ce qui concerne l'établissement des procédures de base régissant le couplage entre les registres du SEQE-UE et du SEQE suisse. Il présente les procédures générales requises pour le fonctionnement du couplage, mais des lignes directrices techniques plus détaillées seront nécessaires pour rendre ce couplage effectif.

Pour assurer le bon fonctionnement du couplage, des spécifications techniques devront être adoptées afin que le lien devienne véritablement opérationnel. Conformément à l'article 3, paragraphe 7, de l'accord, ces aspects sont décrits en détail dans le document relatif aux normes techniques de couplage (NTC) qui doit être adopté séparément par décision du comité mixte.

L'objectif des POC est de faire en sorte que les services informatiques liés au fonctionnement du couplage entre les registres du SEQE de l'UE et du SEQE suisse soient assurés de manière efficace et efficiente, notamment pour répondre aux demandes de service, remédier aux interruptions de service, résoudre les problèmes et exécuter les opérations de routine conformément aux normes internationales en matière de gestion des services informatiques.

Pour la solution provisoire qui a été acceptée, seules sont nécessaires les POC suivantes, décrites dans le présent document:

- Gestion des incidents

- Gestion des problèmes
- Exécution des demandes
- Gestion des changements
- Gestion des mises en production
- Gestion des incidents de sécurité
- Gestion de la sécurité de l'information

Ultérieurement, lors du déploiement du lien permanent entre les registres, les POC devront être adaptées et complétées autant que de besoin.

2.2. Destinataires

Les destinataires des présentes POC sont les équipes de support du registre de l'UE et du registre suisse.

3. APPROCHE ET NORMES

Les principes suivants valent pour toutes les POC:

- L'UE et la Confédération suisse conviennent de définir les POC sur la base d'ITIL – Information Technology Infrastructure Library (Bibliothèque pour l'infrastructure des technologies de l'information, version 3). Les pratiques issues de ce référentiel sont reprises et adaptées aux besoins spécifiques liés à la solution provisoire.
- La communication et la coordination entre les deux parties qui sont nécessaires à l'exécution des POC s'effectuent par le truchement des centres de services du registre suisse et du registre de l'UE. Les tâches sont toujours assignées au sein d'une seule partie.
- En cas de désaccord sur la manière d'aborder une POC, les deux centres de services analysent et règlent la question entre eux. Si aucun accord ne peut être trouvé, la recherche d'une solution commune est transférée au niveau supérieur.

Niveaux successifs de traitement	**UE**	**CH**
1er niveau	Centre de services de l'UE	Centre de services suisse
2e niveau	Responsable des opérations de l'UE	Gestionnaire des applications du registre suisse
3e niveau	Comité mixte (qui peut déléguer cette responsabilité en vertu de l'article 12, paragraphe 5, de l'accord)	
4e niveau	Comité mixte, si le 3e niveau est délégué	

- Chaque partie est libre de déterminer les procédures applicables au fonctionnement de son propre système de registre, en tenant compte des exigences et des interfaces liées à ces POC.
- Un outil de gestion des services informatiques (ITSM) est utilisé à l'appui des POC, en particulier celles relatives à la gestion des incidents, à la gestion des problèmes et à l'exécution des demandes, et pour la communication entre les parties.

- En outre, l'échange d'informations par courrier électronique est autorisé.
- Les deux parties veillent à ce que les exigences en matière de sécurité de l'information soient respectées, conformément aux instructions relatives au traitement.

4. GESTION DES INCIDENTS

Le processus de gestion des incidents a pour objectif de rétablir le plus vite possible le niveau de fonctionnement normal des services informatiques et de limiter au maximum l'interruption des activités.

La gestion des incidents devrait également permettre de garder une trace des incidents pour faciliter la production de rapports, et se combiner à d'autres processus en vue d'une amélioration continue du système.

- D'un point de vue global, la gestion des incidents recouvre les activités suivantes:
- détection et enregistrement des incidents
- classification et support initial
- enquête et diagnostic
- résolution et rétablissement du service
- clôture de l'incident

Tout au long du cycle de vie de l'incident, le processus de gestion des incidents doit permettre d'assurer le traitement continu de la propriété, la surveillance, le suivi et la communication.

4.1. Détection et enregistrement des incidents

Un incident peut être détecté par un groupe de support, au moyen d'outils de suivi automatisés ou lors d'une surveillance de routine effectuée par le personnel technique.

Une fois détecté, l'incident doit être enregistré et un identificateur unique doit lui être attribué afin de permettre le suivi et la surveillance de l'incident. L'identificateur unique d'un incident est l'identificateur attribué dans le système de tickets commun par le centre de services de la partie (UE ou CH) qui a signalé l'incident; il doit figurer dans toutes les communications liées à l'incident.

Pour tous les incidents, le point de contact devrait être le centre de services de la partie qui a ouvert le ticket.

4.2. Classification et support initial

La classification des incidents vise à comprendre et à repérer quel système et/ou service est défaillant et dans quelle mesure. Pour être efficace, la classification doit renvoyer l'incident vers la bonne ressource du premier coup, de façon à permettre une résolution plus rapide des incidents.

La phase de classification vise à établir le type d'incident et l'ordre de priorité de celui-ci en fonction de ses répercussions et de son degré d'urgence, afin qu'il soit traité selon les délais prescrits pour chaque niveau de priorité.

Si l'incident est susceptible de porter atteinte à la confidentialité ou à l'intégrité de données sensibles et/ou à la disponibilité du système, il est également déclaré comme un incident lié à la sécurité et traité selon la procédure définie dans la rubrique «Gestion des incidents de sécurité» du présent document.

Lorsque c'est possible, le centre de services qui a ouvert le ticket effectue un premier diagnostic. Pour ce faire, il vérifie si l'incident correspond à une erreur connue. Si oui, la méthode pour résoudre ou contourner le problème est déjà connue et documentée.

Si le centre de services parvient à résoudre l'incident, il clôture ce dernier à ce stade, le but premier de la gestion des incidents (soit le rétablissement rapide du service pour l'utilisateur final) ayant été atteint. S'il n'y parvient pas, il transfère l'incident au groupe de résolution approprié pour une enquête et un diagnostic plus poussés.

4.3. Enquête et diagnostic

Le processus d'enquête et de diagnostic est appliqué lorsque l'incident n'a pas pu être résolu par le centre de services dans le cadre du diagnostic initial et a donc été transféré au niveau de traitement approprié. La remontée des incidents fait partie intégrante du processus d'enquête et de diagnostic.

Une pratique courante à ce stade consiste à tenter de reproduire l'incident dans des conditions contrôlées. L'important, lorsque le processus d'enquête et de diagnostic est appliqué, est de bien comprendre dans quel ordre les événements qui ont conduit à l'incident se sont produits.

La remontée de l'incident intervient lorsqu'il apparaît que celui-ci ne peut être résolu au niveau de support actuel et doit être transféré à un groupe de support de plus haut niveau ou à l'autre partie. Cette remontée peut être horizontale (fonctionnelle) ou verticale (hiérarchique).

Le centre de services qui a enregistré l'incident et lancé la procédure de résolution est chargé de transférer l'incident à la ressource appropriée, et assure le suivi global de l'incident et son assignation.

La partie à laquelle l'incident a été transféré est chargée de veiller à l'exécution en temps utile des actions demandées et de fournir un retour d'information à son propre centre de services.

4.4. Résolution et rétablissement du service

Le processus de résolution de l'incident et de rétablissement du service est appliqué une fois que l'incident est pleinement compris. La résolution d'un incident signifie qu'on a trouvé un moyen de remédier au problème. L'application de cette solution correspond à la phase de rétablissement du service.

Une fois l'interruption de service résolue par les ressources appropriées, l'incident est renvoyé au centre de services qui a enregistré l'incident; ce dernier vérifie auprès de l'auteur du signalement de l'incident que l'erreur a été corrigée et que l'incident peut être clôturé. Les résultats du traitement de l'incident sont consignés en vue d'une utilisation future.

Le rétablissement du service peut être exécuté par le personnel de support informatique ou moyennant une série d'instructions fournies à l'utilisateur.

4.5. Clôture de l'incident

Dernière étape du processus de gestion des incidents, la clôture intervient peu après la résolution de l'incident.

Parmi la liste des opérations qui doivent être exécutées durant la phase de clôture figurent notamment:

- la vérification de la catégorisation initiale de l'incident;
- la saisie complète de toutes les informations se rapportant à l'incident;

- la documentation complète de l'incident et la mise à jour correspondante de la base de connaissances;
- la communication d'un message approprié à chaque partie prenante directement ou indirectement concernée par l'incident.

Un incident est formellement clôturé dès l'instant où la phase de clôture a été exécutée par le centre de services et communiquée à l'autre partie.

Une fois l'incident clôturé, il n'est pas rouvert. Si le même incident survient peu de temps après, l'incident initial n'est pas rouvert, un nouvel incident doit être créé.

Si l'incident fait l'objet d'un suivi à la fois par le centre de services de l'UE et par le centre de services suisse, il incombe au centre de services qui a ouvert le ticket de clôturer définitivement l'incident.

5. GESTION DES PROBLEMES

Il convient d'appliquer cette procédure à chaque fois qu'un problème est détecté, déclenchant ainsi le processus de gestion des problèmes. La gestion des problèmes a essentiellement pour but d'améliorer la qualité du système et de réduire le nombre d'incidents signalés. Un problème peut être la cause d'un ou de plusieurs incidents. Lorsqu'un incident est signalé, l'objectif du processus de gestion des incidents est de rétablir le service dans les plus brefs délais, éventuellement à l'aide de solutions de contournement. Lorsqu'un problème est enregistré, l'objectif est d'en trouver la cause profonde afin de déterminer quel changement permettra de garantir que ce problème et les incidents qui en découlent ne se produisent plus à l'avenir.

5.1. Identification et enregistrement du problème

Suivant la partie qui a ouvert le ticket, le point de contact pour toutes les questions liées au problème sera le centre de services de l'UE ou de la Confédération suisse.

L'identificateur unique d'un problème est l'identificateur attribué par l'outil de gestion des services informatiques (ITSM). Cet identificateur doit figurer dans toutes les communications liées au problème.

Le processus de gestion des problèmes peut être déclenché par un incident ou être lancé délibérément pour résoudre des défaillances détectées à un niveau quelconque du système.

5.2. Hiérarchisation des problèmes

Comme les incidents, les problèmes peuvent être catégorisés en fonction de leur gravité et de leur ordre de priorité afin de faciliter leur suivi, en tenant compte de l'impact et de la fréquence des incidents liés à ces problèmes.

5.3. Enquête et diagnostic

Chaque partie peut signaler un problème, et le centre de services de cette partie est alors chargé d'enregistrer le problème, de l'assigner à la ressource appropriée et d'en assurer le suivi global.

Le groupe de résolution auquel le problème a été transféré est chargé de le traiter dans les meilleurs délais et en communiquant avec le centre de services.

Les deux parties sont chargées, sur demande, de veiller à l'exécution des actions assignées et de fournir un retour d'information à leurs centres de services respectifs.

5.4. Résolution

Le groupe de résolution auquel le problème est assigné est chargé de résoudre ce dernier et de fournir des informations pertinentes au centre de services de sa propre partie.

Les résultats du traitement du problème sont consignés en vue d'une utilisation future.

5.5. Clôture du problème

Un problème est formellement clôturé lorsqu'il a été résolu par l'application du changement. La clôture du problème est exécutée par le centre de services qui a enregistré le problème et qui a informé le centre de services de l'autre partie.

6. EXECUTION DES DEMANDES

Le processus d'exécution des demandes correspond au traitement de bout en bout d'une demande de service nouveau ou existant, à partir du moment où elle est enregistrée et approuvée jusqu'au moment où elle est clôturée. Les demandes de service sont généralement simples, prédéfinies, reproductibles, fréquentes, pré-approuvées et en rapport avec les procédures.

Les principales étapes à suivre sont décrites ci-après.

6.1. Introduction de la demande

Les informations relatives à une demande de service sont soumises au centre de services de l'UE ou au centre de services suisse par courrier électronique, par téléphone ou par l'intermédiaire de l'outil de gestion des services informatiques (ITSM) ou de tout autre moyen de communication reconnu.

6.2. Enregistrement et analyse de la demande

Pour toutes les demandes de service, le point de contact devrait être le centre de services de l'UE ou le centre de services suisse, selon la partie qui est à l'origine de la demande de service. Le centre de services concerné est chargé d'enregistrer et d'analyser avec la diligence requise la demande de service.

6.3. Approbation de la demande

L'agent du centre de services de la partie qui est à l'origine de la demande de service vérifie si une approbation quelconque de l'autre partie est nécessaire et, si oui, demande cette approbation. Si la demande de service n'est pas approuvée, le centre de services met à jour et clôture le dossier.

6.4. Exécution de la demande

Cette étape correspond au traitement effectif et efficace des demandes de service. Il convient d'opérer une distinction entre les cas suivants:

- L'exécution de la demande de service ne concerne qu'une des parties. Dans ce cas, cette partie émet les ordres d'exécution et coordonne l'ensemble du processus.
- L'exécution de la demande de service concerne tant l'UE que la Confédération suisse. Dans ce cas, les centres de services émettent les ordres d'exécution dans les domaines qui relèvent de leur compétence. Le traitement de la demande de service fait l'objet d'une coordination entre les deux centres de services. La responsabilité globale du processus incombe au centre de services qui a reçu et introduit la demande de service.

Une fois la demande de service traitée, son statut doit être modifié en conséquence.

6.5. Remontée des demandes

Au besoin, le centre de services peut transférer les demandes de service pendantes à la ressource appropriée (tierce partie).

Les transferts se font vers les tierces parties respectives: le centre de services de l'UE devra passer par le centre de services suisse pour le transfert d'une demande à une tierce partie suisse, et vice versa.

La tierce partie à laquelle la demande de service a été transférée est chargée de traiter celle-ci dans les meilleurs délais et en communiquant avec le centre de services qui a transféré la demande de service.

Le centre de services qui a enregistré la demande de service est chargé du suivi global de la demande et de l'assignation d'une demande de service.

6.6. Vérification de l'exécution des demandes

Le centre de services responsable soumet le dossier de la demande de service à un dernier contrôle de qualité avant de le clôturer. Le but est de s'assurer que la demande de service a bien été traitée et que toutes les informations requises pour décrire le cycle de vie de la demande ont été fournies de manière suffisamment détaillée. En outre, les résultats du traitement de la demande sont consignés en vue d'une utilisation future.

6.7. Clôture de la demande

Si les parties auxquelles la demande de service a été assignée conviennent que celle-ci a été exécutée et que le demandeur considère que l'affaire est réglée, la demande est dite «clôturée».

Une demande de service est formellement clôturée dès l'instant où le centre de services qui a enregistré la demande de service a exécuté la phase de clôture de la demande et informé le centre de services de l'autre partie.

7. GESTION DES CHANGEMENTS

L'objectif est de faire en sorte que des méthodes et des procédures normalisées soient utilisées pour prendre en charge de manière efficace et rapide tous les changements intéressant l'infrastructure informatique, afin de réduire au minimum le nombre des incidents et leurs conséquences sur le service. Les changements de l'infrastructure informatique peuvent constituer une réponse à des problèmes ou à des exigences imposées de l'extérieur, comme des modifications de la législation, ou être mis en œuvre de manière proactive dans le cadre d'efforts visant à améliorer l'efficience et l'efficacité ou à permettre des initiatives «business» ou en rendre compte.

Le processus de gestion des changements comprend différentes étapes au cours desquelles sont enregistrées toutes les informations relatives à une demande de changement, en vue de permettre un suivi ultérieur. Ces processus garantissent que le changement sera validé et testé avant la phase de déploiement. Le processus de gestion des mises en production assure le bon déroulement du déploiement.

7.1. Demande de changement

Une demande de changement (DDC) est soumise à l'équipe de gestion des changements pour validation et approbation. Pour toutes les demandes de changement, le point de contact devrait être le centre de services de l'UE ou le centre de services suisse, en fonction de la partie qui

est à l'origine de la demande. Ce centre de services sera chargé d'enregistrer la demande et de l'analyser avec la diligence requise.

Les demandes de changement peuvent avoir pour origine:

- un incident entraînant un changement;
- un problème existant qui se traduit par un changement;
- un nouveau changement demandé par un utilisateur final;
- un changement résultant d'une maintenance continue;
- des modifications de la législation.

7.2. Évaluation et planification des changements

Cette étape traite des activités d'évaluation et de planification des changements. Elle comprend des activités de hiérarchisation et de planification qui visent à réduire au minimum les risques et les incidences.

Si l'exécution de la DDC concerne à la fois l'UE et la Suisse, la partie qui a enregistré la DDC vérifie l'évaluation et la planification du changement avec l'autre partie.

7.3. Approbation des changements

Toute demande de changement enregistrée doit être approuvée au niveau de traitement approprié.

7.4. Exécution des changements

L'exécution des changements fait partie de la gestion des mises en production. Les équipes de gestion des mises en production des deux parties suivent leurs propres procédures qui consistent en activités de planification et en tests. La vérification du changement intervient une fois que son exécution est achevée. Pour faire en sorte que tout se déroule comme prévu, le processus existant de gestion des changements est constamment revu et mis à jour chaque fois que nécessaire.

8. GESTION DES MISES EN PRODUCTION

Une mise en production représente un ou plusieurs changements apportés à un service informatique, réunis dans un plan de mise en production, qui doivent être autorisés, préparés, construits, testés et déployés simultanément. Une mise en production unique peut correspondre à la correction d'un bogue, à un changement de matériel ou d'autres composants, à des changements de logiciels, à des mises à niveau de versions d'applications, à des modifications de la documentation et/ou des processus. Le contenu de chaque mise en production est géré, testé puis déployé comme une entité unique.

La gestion des mises en production a pour but de planifier, construire, tester et valider, et de donner la capacité de fournir les services désignés, qui permettront de satisfaire les exigences des parties prenantes et de réaliser les objectifs visés. Les critères d'acceptation de tous les changements apportés au service seront définis et documentés lors de la coordination de la conception et fournis aux équipes de gestion des mises en production.

La mise en production consiste en général en un certain nombre de solutions à des problèmes et d'améliorations d'un service. Elle contient les logiciels nouveaux ou modifiés requis et tout matériel nouveau ou modifié nécessaire à l'exécution des changements approuvés.

8.1. Planification de la mise en production

La première étape du processus consiste à regrouper les changements autorisés dans des packages de mise en production et à définir l'ampleur et le contenu des mises en production. Sur la base de ces informations, le sous-processus de planification de la mise en production consiste à élaborer un calendrier pour la construction, les tests et le déploiement de la mise en production.

La planification doit définir:

- l'ampleur et le contenu de la mise en production;
- l'évaluation des risques et le profil de risque de la mise en production;
- le client/les utilisateurs concernés par la mise en production;
- l'équipe responsable de la mise en production;
- la stratégie de livraison et de déploiement;
- les ressources pour la mise en production et le déploiement.

Les deux parties s'informent mutuellement de leur planification des mises en production et de leurs fenêtres de maintenance. Si une mise en production concerne à la fois l'UE et la Suisse, les deux parties coordonnent la planification et définissent une fenêtre de maintenance commune.

8.2. Construction et test du package de mise en production

L'étape de construction et de test du processus de gestion des mises en production vise à établir les modalités d'exécution de la mise en production ou du package de mise en production, en veillant à rester dans des environnements sous contrôle avant d'apporter tout changement à la production, ainsi qu'à tester l'ensemble des changements dans tous les environnements mis en production.

Si une mise en production concerne à la fois l'UE et la Suisse, les deux parties coordonnent les plans de livraison et de tests, et notamment les aspects suivants:

- comment et à quel moment les unités de mise en production et les composants de service sont livrés;
- quels sont les délais d'exécution habituels; que se passe-t-il en cas de retard;
- comment suivre l'avancement de la livraison et obtenir une confirmation;
- les indicateurs permettant d'assurer le suivi et de déterminer la réussite du déploiement d'une mise en production;
- les cas de test courants pour les fonctionnalités et les changements concernés.

À la fin de ce sous-processus, tous les composants requis de la mise en production sont prêts à entrer dans la phase de déploiement proprement dit.

8.3. Préparation du déploiement

Le sous-processus de préparation garantit que les plans de communication sont définis correctement et que les notifications sont prêtes à être envoyées à toutes les parties prenantes et à tous les utilisateurs finals concernés, et que la mise en production est intégrée dans le processus de gestion des changements afin que tous les changements soient effectués de manière contrôlée et soient approuvés par les entités requises.

Si une mise en production concerne à la fois l'UE et la Suisse, les deux parties coordonnent les activités suivantes:

- enregistrement de la demande de changement pour programmer et préparer le déploiement dans l'environnement de production;
- création du plan d'exécution;
- approche de retour en arrière, afin de pouvoir revenir à l'état antérieur en cas d'échec d'un déploiement;
- envoi de notifications à toutes les parties concernées;
- demande d'approbation de l'exécution de la mise en production au niveau de traitement approprié.

8.4. Retour en arrière de la mise en production

Si le déploiement a échoué ou si les tests ont permis de constater que le déploiement n'a pas abouti ou n'a pas satisfait aux critères d'acceptation/de qualité convenus, les équipes de gestion des mises en production de chaque partie devront rétablir l'état antérieur. Toutes les parties prenantes concernées devront être informées, y compris les utilisateurs finals concernés/ciblés. Dans l'attente d'une approbation, le processus peut être relancé à n'importe quelle étape précédente.

8.5. Vérification et clôture de la mise en production

Lors de la vérification d'un déploiement, les actions suivantes devraient être prévues:

- obtenir un retour d'information sur la satisfaction des clients et des utilisateurs et sur la qualité du service à la suite du déploiement (recueillir le retour d'information et en tenir compte pour l'amélioration continue du service);
- examiner les critères de qualité qui n'ont pas été remplis;
- vérifier que les actions, les corrections et changements nécessaires ont été menés à terme;
- s'assurer de l'absence de problèmes d'aptitude, de ressources, de capacité ou de performance à la fin du déploiement;
- vérifier que les problèmes, les erreurs et les solutions de contournement connues sont documentés et acceptés par le client, les utilisateurs finals, le soutien opérationnel et les autres parties concernées;
- assurer un suivi des incidents et des problèmes causés par le déploiement (fournir un soutien précoce aux équipes opérationnelles si la mise en production a entraîné une augmentation de la charge de travail);
- mettre à jour la documentation de support (c'est-à-dire les documents d'information techniques);
- transférer formellement le déploiement de la mise en production à l'exploitation des services;
- consigner les enseignements tirés;
- récupérer le document récapitulatif de la mise en production auprès des équipes d'implémentation;

- clôturer formellement la mise en production après avoir vérifié l'enregistrement de la demande de changement.

9. GESTION DES INCIDENTS DE SECURITE

La gestion des incidents de sécurité est un processus de traitement des incidents de sécurité qui permet de communiquer avec les parties prenantes susceptibles d'être concernées; d'évaluer et de hiérarchiser les incidents; de réagir pour remédier à tout manquement réel, suspecté ou potentiel relatif à la confidentialité, à la disponibilité ou à l'intégrité des ressources d'information sensibles.

9.1. Catégorisation des incidents liés à la sécurité de l'information

Tous les incidents ayant une incidence sur le lien entre le registre de l'Union et le registre suisse sont analysés afin de déterminer d'éventuels manquements relatifs à la confidentialité, à l'intégrité ou à la disponibilité des informations sensibles enregistrées sur la liste des informations sensibles (LIS).

Le cas échéant, l'incident doit être caractérisé en tant qu'incident lié à la sécurité de l'information, immédiatement enregistré dans l'outil de gestion des services informatiques (ITSM) et géré comme tel.

9.2. Traitement des incidents liés à la sécurité de l'information

Les incidents de sécurité sont placés sous la responsabilité du 3^{e} niveau de traitement et la résolution des incidents sera traitée par une équipe de gestion des incidents spécialisée.

L'équipe de gestion des incidents est chargée des actions suivantes:

- effectuer une première analyse, catégoriser l'incident et évaluer sa gravité;
- coordonner les actions entre toutes les parties prenantes, y compris la documentation complète de l'analyse de l'incident, les décisions prises pour remédier à l'incident et les éventuelles faiblesses constatées;
- en fonction de la gravité de l'incident de sécurité, faire appel en temps utile au niveau de traitement approprié pour information et/ou décision.

Dans le processus de gestion de la sécurité de l'information, toutes les informations concernant les incidents sont classées au niveau le plus élevé de sensibilité de l'information et, en tout état de cause, jamais en dessous du niveau «SEQE SENSIBLE».

Dans le cas d'une enquête en cours et/ou d'une faiblesse susceptible d'être exploitée et jusqu'à la résolution du problème, les informations sont classées «SEQE CRITIQUE».

9.3. Caractérisation des incidents de sécurité

En fonction du type d'événement de sécurité, le responsable de la sécurité de l'information détermine les organismes appropriés à associer et à inclure dans l'équipe de gestion des incidents.

9.4. Analyse des incidents de sécurité

L'équipe de gestion des incidents prend contact avec toutes les organisations concernées et les membres compétents de leurs équipes, selon qu'il convient, pour examiner l'incident. L'analyse permet de déterminer l'ampleur de la perte de confidentialité, d'intégrité ou de disponibilité d'une ressource d'information et d'en évaluer les conséquences pour toutes les organisations concernées. Ensuite sont définies les mesures initiales et les mesures de suivi à

prendre pour remédier à l'incident et gérer son impact ainsi que l'impact de ces mesures sur les ressources.

9.5. Évaluation de la gravité de l'incident de sécurité, remontée de l'incident et établissement d'un rapport

L'équipe de gestion des incidents évalue la gravité de tout nouvel incident de sécurité après sa caractérisation et entreprend l'action immédiate requise en fonction du niveau de gravité.

9.6. Rapport de réaction à un incident de sécurité

L'équipe de gestion des incidents inclut les résultats de la maîtrise de l'incident et du rétablissement du service dans le rapport de réaction à un incident lié à la sécurité de l'information. Le rapport est remis au 3e niveau de traitement par courrier électronique sécurisé ou par d'autres moyens de communication sécurisée mutuellement acceptés.

La partie responsable examine les résultats de la maîtrise de l'incident et du rétablissement du service, et:

- reconnecte le registre en cas de déconnexion préalable;
- communique des informations relatives à l'incident aux équipes des registres;
- clôture l'incident.

L'équipe de gestion des incidents devrait inclure (de façon sécurisée) des détails importants dans le rapport relatif aux incidents liés à la sécurité de l'information, afin de garantir la cohérence de l'enregistrement et de la communication et de permettre une action rapide et appropriée pour maîtriser l'incident. L'équipe de gestion des incidents soumet le rapport final relatif à l'incident lié à la sécurité de l'information en temps utile après son achèvement.

9.7. Suivi, renforcement des capacités et amélioration continue

L'équipe de gestion des incidents soumettra les rapports relatifs à tous les incidents de sécurité au 3e niveau de traitement. Les rapports seront utilisés à ce niveau de traitement pour déterminer les éléments suivants:

- les points faibles dans les contrôles de sécurité et/ou l'exploitation qui doivent être renforcés;
- les besoins éventuels de renforcement de cette procédure afin d'améliorer l'efficacité de la réaction aux incidents;
- les possibilités de formation et de renforcement des capacités pour améliorer encore la résilience des systèmes de registres aux incidents liés à la sécurité de l'information, réduire le risque de futurs incidents et limiter leur impact.

10. GESTION DE LA SECURITE DE L'INFORMATION

La gestion de la sécurité de l'information vise à garantir la confidentialité, l'intégrité et la disponibilité des informations et données classifiées et des services informatiques sensibles d'une organisation. Outre les composants techniques, y compris leur conception et tests (voir NTC), les procédures opérationnelles communes suivantes sont nécessaires pour satisfaire aux exigences de sécurité requises pour la solution provisoire.

10.1. Caractérisation des informations sensibles

La sensibilité d'une information est évaluée en déterminant le niveau d'impact que pourrait avoir sur l'activité (par exemple, pertes financières, dégradation de l'image, violation de la loi, etc.) une atteinte à la sécurité en rapport avec cette information.

Les ressources d'information sensibles sont caractérisées d'après l'incidence qu'elles ont sur le couplage.

Le niveau de sensibilité de ces informations est évalué au moyen de l'échelle de sensibilité applicable à ce couplage, décrite en détail dans la section «Traitement des incidents liés à la sécurité de l'information» du présent document.

10.2. Niveaux de sensibilité des ressources d'information

Lors de sa caractérisation, la ressource d'information est classée en appliquant les règles suivantes:

- l'indication d'au moins un niveau ÉLEVÉ de confidentialité, d'intégrité ou de disponibilité entraîne le classement de la ressource en tant que SEQE CRITIQUE;
- l'indication d'au moins un niveau MOYEN de confidentialité, d'intégrité ou de disponibilité entraîne le classement de la ressource en tant que SEQE SENSIBLE;
- l'indication d'un simple FAIBLE niveau de confidentialité, d'intégrité ou de disponibilité entraîne le classement de la ressource en tant que SEQE LIMITÉ.

10.3. Désignation du propriétaire de la ressource d'information

Toutes les ressources d'information devraient avoir un propriétaire attitré. Les ressources d'information du SEQE qui font partie du couplage entre l'EUTL et le SSTL ou qui y sont associées devraient figurer sur une liste d'inventaire des ressources communes, tenue à jour par les deux parties. Les ressources d'information du SEQE qui sont étrangères au couplage entre le l'EUTL et le SSTL devraient figurer sur une liste d'inventaire des ressources tenue à jour par la partie concernée.

La propriété de chaque ressource d'information faisant partie du couplage entre l'EUTL et le SSTL ou qui y est associée doit être approuvée par les parties. Le propriétaire d'une ressource d'information est responsable de l'évaluation de la sensibilité de cette ressource.

Le propriétaire doit avoir le niveau de responsabilité approprié pour la valeur de la ou des ressources attribuées. La responsabilité du propriétaire concernant la ou les ressources et l'obligation lui incombant de maintenir le niveau requis de confidentialité, d'intégrité et de disponibilité devraient faire l'objet d'un accord et d'une formalisation.

10.4. Enregistrement des informations sensibles

Toutes les informations sensibles sont enregistrées sur la liste des informations sensibles (LIS).

Le cas échéant, le regroupement d'informations sensibles qui pourraient avoir un impact plus important que celui d'une seule information est pris en compte et est enregistré sur la LIS (par exemple, ensemble d'informations stockées dans la base de données du système).

La LIS n'est pas statique. Les menaces, les vulnérabilités, la probabilité ou les conséquences des incidents de sécurité liés aux ressources peuvent changer sans préavis, et de nouvelles ressources pourraient être introduites dans le fonctionnement des systèmes de registres.

Par conséquent, la LIS doit être réexaminée régulièrement, et toute nouvelle information jugée sensible doit être immédiatement enregistrée dans la LIS.

La LIS comprend au moins, pour chaque entrée, les informations suivantes:

- la description de l'information,
- le propriétaire de l'information,
- le niveau de sensibilité,
- une mention précisant si l'information contient des données à caractère personnel,
- des informations complémentaires si nécessaire.

10.5. Traitement des informations sensibles

Lorsqu'elles sont utilisées en dehors du couplage entre le registre de l'Union et le registre suisse, les informations sensibles sont traitées conformément aux instructions de traitement.

Les informations sensibles utilisées par le couplage entre le registre de l'Union et le registre suisse sont traitées conformément aux exigences de sécurité des parties.

10.6. Gestion des accès

L'objectif de la gestion des accès est d'accorder aux utilisateurs autorisés le droit d'utiliser un service, tout en empêchant l'accès des utilisateurs non autorisés. La gestion des accès est parfois également appelée «gestion des droits» ou «gestion de l'identité».

En ce qui concerne la solution provisoire et son fonctionnement, les deux parties ont besoin d'avoir accès aux éléments suivants:

- Wiki: environnement de collaboration pour l'échange d'informations communes telles que la planification des mises en production;
- outil de gestion des services informatiques (ITSM) pour la gestion des incidents et des problèmes (voir chapitre «Approche et normes»);
- systèmes d'échange de messages: chaque partie fournit un système sécurisé d'échange de messages pour la transmission des messages contenant les données de transaction.

L'administrateur du registre suisse et l'administrateur central de l'Union veillent à ce que les accès soient à jour, et font office de points de contact pour leurs parties en ce qui concerne les activités de gestion de l'accès. Les demandes d'accès sont traitées conformément aux procédures d'exécution des demandes.

10.7. Gestion des certificats/clés

Chaque partie est responsable de la gestion de ses propres certificats/clés (génération, enregistrement, stockage, installation, utilisation, renouvellement, révocation, sauvegarde et récupération des certificats/clés). Comme indiqué dans les normes techniques de couplage (NTC), seuls sont utilisés les certificats numériques délivrés par une autorité de certification qui bénéficie de la confiance des deux parties. Le traitement et le stockage des certificats/clés doivent respecter les dispositions prévues dans les instructions de traitement.

Toute révocation et/ou tout renouvellement de certificats et de clés est coordonné par les deux parties. Les demandes d'accès sont traitées conformément aux procédures d'exécution des demandes.

L'administrateur du registre suisse et l'administrateur central de l'Union échangeront les certificats/clés par des moyens de communication sécurisés conformément aux dispositions prévues dans les instructions de traitement.

Toute vérification des certificats/clés par tout moyen entre les parties est effectuée hors bande.