Fiche méthodologique

Revue des habilitations
Chorus Cœur

1. Objectif du contrôle

Les habilitations et profils informatiques participent à la **sécurisation des accès aux systèmes d'information**. Leur bon usage conditionne la confidentialité et l'intégrité des données portées par ceux-ci, ainsi que la traçabilité des différents intervenants dans les applications. Il constitue ainsi un enjeu majeur de maîtrise des risques.

La thématique des accès à Chorus Cœur, particulièrement sensible, doit faire l'objet d'une attention particulière de la part des ministères. La nécessité de mettre en œuvre une **revue annuelle des habilitations à Chorus Cœur** est à cet égard rappelée.

La revue des habilitations est un contrôle de supervision *a posteriori* qui permet de s'assurer de la **concordance** entre les **habilitations et profils** informatiques, les **attributions** de chaque agent du service et, le cas échéant, les **délégations de signature** correspondantes.

2. Périmètre du contrôle

Par définition, ce contrôle est **exhaustif** :

- contrôle de **tous les comptes et habilitations à Chorus Cœur** ouverts au sein de chaque service ministériel (administration centrale et services déconcentrés) ;
- contrôle de **tous les agents du service**.

3. Acteurs chargés du contrôle

Ce contrôle doit être réalisé au niveau de chaque **responsable de service**.

4. Périodicité du contrôle

Ce contrôle doit être réalisé ***a minima*** **annuellement**.

Ce contrôle est idéalement réalisé au mois d'octobre, à l'appui de données extraites à la fin du mois de septembre. Ce calendrier permet de s'assurer de la prise en compte des mouvements de personnel souvent importants sur le mois de septembre.

Il est recommandé de procéder au contrôle au plus près de la date de l'extraction des données relatives aux utilisateurs.

5. Support de contrôle

La revue des habilitations est réalisée sur la base d'une **extraction de la liste des utilisateurs actifs Chorus Cœur** au sein du service.

L'Agence pour l'Informatique Financière de l'État (AIFE) procède à une extraction des données nationales le 30 septembre 2021 au soir afin qu'un contrôle des comptes et des habilitations Chorus Cœur puisse être mené au niveau de chaque périmètre ministériel.

Cette extraction est transmise par l'AIFE aux Correspondants Chorus Habilitations référents (CCH) dès le 1er octobre 2021 ainsi qu'aux supports de niveau 1 (SN1) de chaque ministère. Les référents ministériels « contrôle interne » en sont destinataires en copie, pour information.

Cette extraction prend la forme d'un tableur, comportant deux onglets (« Chorus Cœur » et « Suppléances »). Le contrôle portera sur la liste des habilitations à Chorus Cœur, ainsi que sur la liste des suppléances actives.

Le contrôle des suppléances (*cf.* point de contrôle n°5 ci-dessous), préconisé à titre facultatif en 2018, est depuis 2019 préconisé à titre obligatoire.

6. Points à contrôler

La revue des habilitations Chorus Cœur à mener à partir de l'extraction des utilisateurs actifs au sein du service consiste à **contrôler les six points suivants** :

Point 1. Onglet « Chorus Coeur » : Les agents disposant d'une habilitation sont-ils effectivement présents dans le service ?

Ce premier point de contrôle consiste à s'assurer que tous les utilisateurs actifs répertoriés dans l'extraction sont **toujours présents** au sein du service et **exercent toujours des fonctions** sous Chorus.

Il permet d'identifier les éventuelles habilitations non utilisées au sein du service et dont il convient de demander la suppression.

Réponse	Signification
OUI	L'agent est toujours présent dans le service et les fonctions qui lui sont attribuées nécessitent bien une habilitation à Chorus Cœur.
NON	L'agent a quitté le service. OU L'agent est toujours présent dans le service mais les fonctions qui lui sont attribuées ne nécessitent pas ou plus une habilitation à Chorus Cœur.

NB. La détection des habilitations non utilisées dans les services est facilitée par la réalisation par l'AIFE d'une campagne annuelle de désactivation.

Point 2. Onglet « Chorus Coeur » : Le groupe utilisateur Chorus auquel est rattaché l'utilisateur correspond-t-il au service d'affectation de l'agent ?

Ce deuxième point de contrôle consiste à s'assurer que les agents du service disposant d'une habilitation à Chorus Cœur sont **bien rattachés au groupe utilisateur** correspondant au service.

Réponse	Signification
OUI	Le groupe utilisateur Chorus auquel est rattaché l'utilisateur correspond au service d'affectation de l'agent.
NON	Le groupe utilisateur Chorus auquel est rattaché l'utilisateur ne correspond pas au service d'affectation de l'agent.

Point 3. Onglet « Chorus Coeur » : Les différentes informations liées à « l'utilisateur » sont-elles exactes ?

Ce troisième point de contrôle consiste à vérifier l'**exactitude des informations** attachés à chaque utilisateur : nom, prénom, adresse e-mail.

Réponse	Signification
OUI	Les nom, prénom et adresse e-mail de l'utilisateur sont corrects.
NON	Les nom, prénom et/ou adresse e-mail de l'utilisateur sont erronés. Préciser l'origine de l'anomalie (nom, prénom et/ou adresse e-mail).

Point 4. Onglet « Chorus Coeur » : Les rôles rattachés à chaque utilisateur correspondent-ils aux fonctions exercées par l'agent ? L'octroi de plusieurs rôles à un même agent respecte-t-il les préconisations d'incompatibilité proposées par la matrice des associations de rôles Chorus?

Ce quatrième point de contrôle consiste à vérifier :

• d'une part, la **concordance** entre les **rôles Chorus** rattachés à chaque utilisateur et ses **attributions** au sein du service.

Dans un service, l'encadrement doit attribuer les rôles Chorus de manière restrictive, en vertu du principe du « moindre privilège » qui veut qu'un utilisateur ne dispose que des droits nécessaires aux missions qui lui sont confiées (en tenant compte de la durée de ces missions). Il doit cependant disposer de l'ensemble des droits qui lui sont nécessaires, afin de garantir la continuité du service.

• d'autre part, l'**absence de cumul de rôles** considéré comme risqué par un même utilisateur.

Dans un service de taille conséquente, il est fortement recommandé de suivre ces préconisations d'incompatibilité. Dans un service de taille moindre, une approche plus pragmatique peut être appliquée par l'encadrement afin de prévenir d'éventuels blocages de la chaîne de travail. Si, au

regard de cette analyse, le responsable du service fait le choix de ne pas respecter une préconisation d'incompatibilité, les motivations de ce choix doivent être précisées et les mesures de sécurisation destinées à couvrir ce point de fragilité doivent être exposées (mise en place d'un contrôle de supervision par exemple).

• pour les **utilisateurs possédant un profil de validant** dans Chorus Cœur, ce point de contrôle inclut également le rapprochement avec la **délégation de signature** correspondante : existence de la délégation de signature, concordance des périmètres (ex : engagement / service fait, seuil financier, …).

La « matrice des associations » de rôles Chorus pour les gestionnaires, élaborée en 2020 dans le cadre d'un groupe de travail interministériel animé par la DGFiP et la Direction du Budget, est mise à la disposition des ministères et peut servir d'appui à la réalisation de ce point de contrôle. Ce support vient documenter, de manière indicative, le niveau de risque découlant du cumul par un même agent de différents rôles, et oriente donc la détection de potentielles incompatibilités. Il dresse en outre la liste des rôles Chorus nécessitant une délégation de signature.

Cette matrice est mise en ligne sur le serveur de la qualité comptable[1], accessible depuis tout poste informatique avec les identifiant et mot de passe suivants :

Identifiant : etat@cic.fr
Mot de passe : etat2020@cic

Réponse	Signification
OUI	L'utilisateur dispose de l'ensemble des rôles nécessaires à l'exercice de ses missions. ET L'utilisateur ne possède aucun rôle ne correspondant pas à ses missions. ET L'utilisateur ne possède pas plusieurs rôles incompatibles entre eux ; OU il existe un cumul de rôles incompatibles mais celui-ci est justifié au regard de la situation du service et contrebalancé par un renforcement des mesures de contrôle interne. ET Si l'utilisateur dispose d'un rôle de validation, il bénéficie bien d'une délégation de signature dont le périmètre concorde avec les droits de validant qui lui sont ouverts dans Chorus Cœur.
NON	Les rôles attribués à l'utilisateur ne couvrent pas l'ensemble de ses missions. ET/OU L'utilisateur possède un ou plusieurs rôles ne correspondant pas à ses missions. ET/OU L'utilisateur possède plusieurs rôles incompatibles entre eux ; ET ce cumul de rôles incompatibles n'est pas justifié au regard de la taille du service et n'est pas couvert par des mesures de sécurisation. ET/OU Si l'utilisateur dispose d'un rôle de validation, il ne bénéficie de la délégation de signature correspondante ou le périmètre de celle-ci ne concorde pas avec les droits de validant qui lui sont ouverts dans Chorus Cœur.

1 - SQC/Etat/00_Nouveautés
- SQC/Etat/03_Animation/03_Groupes de travail/2020_Rôles Chorus gestionnaires_Matrice des associations

Point 5. Onglet « Suppléances » : Les suppléances (délégation d'une habilitation donnée) attribuées par les agents du service sont-elles connues du chef de service et respectent-elles les préconisations d'incompatibilité ?

Les règles de suppléance actuellement en vigueur dans l'application Chorus permettent à un utilisateur de désigner un suppléant afin que celui-ci accède et traite les pièces présentes dans les bannettes du titulaire en son absence. Ces suppléances peuvent être réalisées sans validation de l'encadrement. Cette possibilité permet potentiellement au suppléant d'accéder à des tâches auxquelles il n'est normalement pas habilité. Par ailleurs, les suppléances restent actives même après le départ des utilisateurs « responsables de suppléance ». À ce titre, elles présentent un risque.

Ce point de contrôle consiste ainsi à vérifier que :

- les suppléances toujours actives émanent bien d'utilisateurs « responsables de suppléance », et donc de **titulaires, encore présents et habilités** dans le service ;
- les suppléances sont bien **attribuées à des agents du service** (le groupe utilisateur suppléant correspond au groupe utilisateur du titulaire et donc au service) :
Les groupes utilisateurs suppléants n'étant pas automatiquement supprimés lors des changements d'affectation des agents, des anomalies peuvent être constatées sur ce point.
- les suppléances attribuées par les agents du service sont **connues du chef de service** ;
- les suppléances respectent bien les **préconisations d'incompatibilité** des rôles[2].

Réponse	Signification
OUI	Le groupe utilisateur suppléant de l'agent correspond à son service d'affectation et au groupe utilisateur du titulaire. ET L'agent déléguant (ou titulaire « responsable de suppléance ») occupe toujours les mêmes fonctions. ET Le chef de service avait connaissance de l'ensemble des suppléances attribuées au sein du service, celles-ci correspondent à la répartition des tâches mise en œuvre entre les agents. ET L'agent déléguant et le suppléant ne disposent pas de rôles Chorus incompatibles entre eux.
NON	Le groupe utilisateur suppléant de l'agent ne correspond pas à son service d'affectation et au groupe utilisateur du titulaire. ET/OU L'agent déléguant a quitté le service ou a changé de fonctions. ET/OU Le chef de service n'avait pas connaissance de l'ensemble des suppléances attribuées au sein du service. ET/OU L'agent déléguant et le suppléant disposent de rôles Chorus incompatibles entre eux.

2 Se référer au besoin à la « matrice des associations » de rôles Chorus pour les gestionnaires pré-citée.

Point 6. Onglets « Chorus Cœur » et « Suppléances » : L'organigramme fonctionnel du service est-il à jour des habilitations et des suppléances ?

L'organigramme fonctionnel nominatif (OFN) d'un service doit retracer, pour chaque tâche mise en œuvre au sein du service, le nom des **titulaires**, les **habilitations et profils** informatiques dont ils disposent, et leurs éventuelles **délégations de signature**. Les noms, habilitations, profils informatiques et délégations de signature des **suppléants** désignés sur ces tâches doivent également être précisés.

L'OFN doit être tenu à jour par le chef de service.

Ce sixième point de contrôle consiste à vérifier la **concordance des informations retracées dans l'OFN avec les constats issus de la revue des habilitations**.

En cas de discordance, le chef de service procédera à l'actualisation de l'OFN.

7. Modalités de formalisation

La formalisation des constats et corrections opérés et leur archivage s'avèrent fondamentaux afin de **garantir la traçabilité** de la revue des habilitations menée et des pistes d'amélioration identifiées.

S'agissant d'une revue menée au niveau national et afin de favoriser l'homogénéisation des travaux menés par chaque entité, il vous est proposé de formaliser les résultats des six points de contrôle préconisés directement dans les colonnes prévues à cet effet dans le support de contrôle transmis par l'AIFE. La colonne « Observations » permettra de détailler les anomalies détectées et de préciser les actions correctrices opérées ou programmées.

Le fichier listant les utilisateurs, complété des constats issus de la revue ainsi que de tout document utile à la compréhension du contrôle, doivent être **conservés et archivés**. L'OFN actualisé doit notamment être joint au contrôle, ainsi que tout document attestant de suites données aux anomalies détectées (délégations de signature à jour par exemple).

Le responsable du contrôle certifiera, pour son service, les informations complétées dans le document formalisant le contrôle, datera ce dernier, et le transmettra au référent « contrôle interne » de l'entité et au correspondant Chorus local pour suppression des habilitations des agents n'exerçant plus de fonctions Chorus.