Fiche de méthodologie et de formalisation des contrôles « AGIR »

Chorus Formulaires _ Revue des habilitations à Chorus Formulaires

Thème de contrôle national ☑ **Thème de contrôle local** ☐

Historique du document

Version	Date	Réalisé par	Changement sur le document	Statut
1.0	16/10/2023	DCISIF		Création

Niveau de rattachement à la cartographie des processus

Cycle d'activité	**(G) SYSTÈME D'INFORMATION**
Sous Cycle d'activité	**(GA) EXPLOITATION ET SUPPORT**
Processus	**(GAA) FONCTION SUPPORT**
Procédure	**(GAA2) GESTION DES HABILITATIONS – Chorus Formulaires**
Tâche	
Opération	

Caractéristiques du thème de contrôle

Unité(s) de travail chargée(s) de réaliser le contrôle :	- Chefs de service, Correspondants Chorus Formulaires de proximité CCFp et référents CIF

Périodicité du contrôle :	☑ Annuelle ☐ Trimestrielle ☐ Semestrielle ☐ Mensuelle

Mois de réalisation du contrôle	J	F	M	A	M	J	J	A	S	O	N	D	J	F
				X										

Informations générales	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. Le contrôle de supervision *a posteriori* offre une garantie quant à la **concordance** entre les habilitations et profils informatiques, les attributions de chaque agent du service et, le cas échéant, les délégations de signature correspondantes.

Question 1	**Q1 - Les agents disposant d'un compte Chorus Formulaires depuis plus de 9 mois et n'ayant pas réalisés de connexion depuis 9 mois sont-ils à désactiver ?**
Question 2	**Q2 - Les rôles rattachés à chaque utilisateur correspondent-ils effectivement à leurs fonctions et les préconisations présentées dans la matrice des associations de rôles, en cas de cumul, sont-elles respectées ?**
Question 3	**Q3 - Le groupe utilisateur Chorus Formulaires auquel est rattaché l'utilisateur correspond-il au service d'affectation de l'agent ?**
Question 4	**Q4 - Le principe d'application de l'authentification forte à Chorus formulaire est-il respecté ?**

Modalités de contrôle

Question 1	**Q1 - Les agents disposant d'un compte Chorus Formulaires depuis plus de 9 mois et n'ayant pas réalisés de connexion depuis 9 mois sont-ils à désactiver ?**	**Type de grille AGIR :** ☐ Analyse de comptes (AC) ☑ Analyse d'opérations (AO) ☐ Diagnostic de process (DP)

Critères de qualité / Risque(s)	**Objectifs** : Présentation et bonne information / Probité **Risques :** 02.01.06.01_Absence d'organigramme fonctionnel 06.02.01.04 _ Absence de demande de suppression ou de modification d'habilitations 06.02.02.01 _ Manque de coordination entre service informatique (technique) / plateforme (métier) pour la gestion des habilitations 06.02.02.03 _ Erreur dans le traitement de la demande d'habilitation 12.02.04.01_ Fraude due à l'accès aux systèmes d'information

1. Objectif et méthode du contrôle	Ce point de contrôle consiste à s'assurer que tous les utilisateurs répertoriés dans l'extraction sont toujours présents au sein du service et exercent toujours des fonctions sous Chorus Formulaires. <u>Modalité de réalisation :</u> Le contrôle est réalisé sur la base du fichier des comptes inactifs extrait pas l'AIFE et communiqué par la Mission Ministérielle Chorus à ses correspondants. Il s'agit de renseigner la dernière colonne dédiée au résultat du contrôle sur le bienfondé ou non du maintien du compte. Cette colonne permettra de renseigner les résultats dans AGIR.
2. Documentation utile	Matrice des associations de rôles

Constitution de l'échantillon à contrôler

3. Nature des opérations à contrôler et seuil éventuel	Liste des comptes inactifs Chorus Formulaires fournie par l'AIFE.
4. Périmètre temporel des opérations à contrôler	Situations extraites à la date du 01/04/N (photographie à date)
5. Nombre d'opérations à contrôler	☑ Exhaustif ☐ Échantillon de XX opérations ☐ Sans objet. Le contrôle est un diagnostic de process.

Analyse des résultats du contrôle

6. Décompte des anomalies	Décompter une anomalie dès lors que les agents ne sont plus présents dans le service (habilitation « obsolète ») **ou** que l'agent est toujours présent dans le service mais que les fonctions qui lui sont attribuées ne nécessitent pas ou plus une habilitation à Chorus Formulaires. **Toute anomalie détectée doit être décomptée, y compris si la correction est effectuée immédiatement**.
7. Préconisations en cas d'anomalies	Propositions d'actions d'amélioration du dispositif de contrôle interne : - Si un agent dispose d'un compte encore actif alors qu'il n'est plus présent dans le service identifié, il convient de procéder à la suppression du compte. Il est rappelé qu'à chaque mouvement de personnel, les chefs de services doivent s'assurer que les comptes utilisateurs correspondent à la situation de leurs agents (création pour les entrants, suppression ou mise à jour pour les sortants…). - Une check-list des vérifications à mener lors d'un mouvement de personnel pourra être utilement mise en place par le responsable de service. En cas d'anomalie, l'encadrement veillera à demander la correction nécessaire, notamment en supprimant l'habilitation obsolète ou dormante.

Précisions sur la formalisation du contrôle dans AGIR	
8. Montant des opérations contrôlées	☐ À préciser ☑ Sans objet
9. Montant des anomalies constatées	☐ À préciser ☑ Sans objet
10. Pièces justificatives / Consignes d'archivage	Il convient de joindre *a minima* dans la grille de restitution AGIR, le(s) pièce(s) justificative(s) suivante(s) : • Fichier des utilisateurs **annoté** des constats ainsi que tout document utile à la compréhension du contrôle et notamment des anomalies.
11. Autres	Les précisions suivantes sont attendues dans le champ « Commentaires » : • Préciser les motifs principaux d'anomalies.

Question 2	**Q2 - Les rôles rattachés à chaque utilisateur correspondent-ils effectivement à leurs fonctions et les préconisations présentées dans la matrice des associations de rôles, en cas de cumul, sont-elles respectées ?**	**Type de grille AGIR :** ☐ Analyse de comptes (AC) ☑ Analyse d'opérations (AO) ☐ Diagnostic de process (DP)

Critères de qualité / Risque(s)	**Objectifs** : Justification / Gestion des compétences / Régularité / Probité **Risques** 01.02.01.09 _ Non-conformité de la demande d'habilitation aux délégations de signature 02.01.06.01_Absence d'organigramme fonctionnel 02.01.06.02 _ Absence de séparation des tâches (incompatibilité des rôles) 06.02.01.04_ Absence de demande de suppression ou de modification d'habilitations 06.02.02.03 _ Erreur dans le traitement de la demande d'habilitation 06.04.02.02_Absence de traçabilité des demandes de paramétrage 12.02.04.01_ Fraude due à l'accès aux systèmes d'information
1. Objectif et méthode du contrôle	Ce deuxième point de contrôle vise à s'assurer que les rôles rattachés à chaque utilisateur correspondent aux fonctions réellement exercées par les agents et que l'octroi de plusieurs rôles sous Chorus Formulaires (voire cumulés avec des rôles sous Chorus cœur) à un même agent respecte les préconisations présentées dans la matrice des associations de rôles. Il consiste à vérifier : • d'une part la concordance entre les rôles ou habilitations sous Chorus formulaires CFO rattachés à chaque utilisateur et ses attributions au sein du service. • d'autre part, l'absence de cumul de rôles considéré comme risqué pour 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). <u>Modalité de réalisation :</u> Le contrôle est réalisé à partir de l'extraction des utilisateurs précisant les groupes utilisateurs (GU) de rattachement réalisée et transmise par la Mission Chorus ministérielle préalablement à la date de réalisation du contrôle. Ce fichier est complété de colonnes dédiées à l'information en cas de non-conformité des points de contrôles liés aux fonctions et cumuls de rôles présentant un risque. Il s'agit de répondre par « oui » ou par « non » selon la situation constatée. S'agissant du second point, dans le cas où les préconisations d'incompatibilités ne peuvent pas être mises en œuvre comme précité, le responsable du contrôle devra mentionner dans la colonne « observations » la justification et les mesures de contrôles propres mises en place pour garantir la couverture du risque représenté. Par ailleurs, il s'agit de détecter si un même utilisateur ne bénéficie pas de plusieurs comptes, ce qui constitue nécessairement une anomalie.

2. Documentation utile	- **matrice des associations de rôles Chorus**

Constitution de l'échantillon à contrôler	
3. Nature des opérations à contrôler et seuil éventuel	Liste des utilisateurs Chorus formulaires.
4. Périmètre temporel des opérations à contrôler	Situations extraites à la date du 01/04/N (photographie à date)
5. Nombre d'opérations à contrôler	☑ Exhaustif (**après exclusion des habilitations obsolètes**) ☐ Échantillon de ☐ Sans objet. Le contrôle est un diagnostic de process.

Analyse des résultats du contrôle	
6. Décompte des anomalies	Une anomalie sera décomptée dans le(s) cas suivant(s) : 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 pas de la délégation de signature correspondante ou le périmètre de celle-ci ne concorde pas avec les droits de valideur qui lui sont ouverts dans Chorus Formulaires. En cas de cumul de rôles identifié comme risqué, dès lors que le responsable peut justifier des mesures et/ou contrôles couvrant ce risque, il convient de considérer qu'il ne s'agit pas d'une anomalie. En revanche, si aucune mesure spécifique de contrôle n'accompagne ce procédé, il s'agit d'une anomalie.
7. Préconisations en cas d'anomalies	Propositions d'actions d'amélioration du dispositif de contrôle interne : • Si lors du contrôle, il a été constaté que l'habilitation n'est pas conforme aux fonctions de l'utilisateur, il convient de le signaler et demander la correction des habilitations de l'agent. Il est rappelé qu'à chaque mouvement de personnel, *les chefs de services doivent s'assurer que les habilitations correspondent à la situation de leurs agents* (création pour les entrants, suppression ou mise à jour pour les sortants, etc.) • Une check-list des vérifications à mener lors d'un mouvement de personnel pourra être utilement mise en place par le responsable de service. • Si des habilitations présentent des rôles cumulés identifiés risqués sont décomptées en anomalies faute de mesure de sécurisation associée, il convient de mettre en place une procédure de contrôle des opérations (mutuel ou *a posteriori* sur échantillon).

Précisions sur la formalisation du contrôle dans AGIR	
8. Montant des opérations contrôlées	☐ À préciser ☑ Sans objet
9. Montant des anomalies constatées	☐ À préciser ☑ Sans objet
10. Pièces justificatives / Consignes d'archivage	Il convient de joindre *a minima* dans la grille de restitution AGIR, le(s) pièce(s) justificative(s) suivante(s) : • Joindre le fichier des utilisateurs **annoté** des constats ainsi que tout document utile à la compréhension du contrôle et notamment des anomalies
11. Autres	Les précisions suivantes sont attendues dans le champ « Commentaires » : • Préciser les motifs principaux d'anomalies

Question 3	**Q3 - Le groupe utilisateur Chorus Formulaires auquel est rattaché l'utilisateur correspond-il au service d'affectation de l'agent ?**	**Type de grille AGIR :** ☐ Analyse de comptes (AC) ☑ Analyse d'opérations (AO) ☐ Diagnostic de process (DP)

Critères de qualité / Risque(s)	**Objectifs** : Gestion des compétences / Régularité / Probité **Risques** 02.01.06.01_Absence d'organigramme fonctionnel 06.02.01.04 _ Absence de demande de suppression ou de modification d'habilitations 06.02.02.01 _ Manque de coordination entre service informatique (technique) / plateforme (métier) pour la gestion des habilitations 06.02.02.03 _ Erreur dans le traitement de la demande d'habilitation 06.04.02.02_Absence de traçabilité des demandes de paramétrage 12.01.10.02_Absence de délégation 12.02.04.01_ Fraude due à l'accès aux systèmes d'information 12.02.03_Non respect volontaire des droits d'accès au système d'information

1. Objectif et méthode du contrôle	Ce troisième point de contrôle consiste à s'assurer que les agents du service disposant d'une habilitation à Chorus Formulaires sont bien rattachés au groupe utilisateur correspondant au service. Modalité de réalisation : Le contrôle est réalisé à partir de l'extraction des utilisateurs précisant les groupes utilisateurs (GU) de rattachement utilisé pour la question 2. Il s'agit de répondre par « oui » ou par « non » dans la colonne dédiée à ce point de contrôle. Pour les **utilisateurs possédant un profil de valideur dans Chorus formulaires**, ce point de contrôle inclut également le rapprochement avec la **délégation de signature** correspondante : existence de la délégation de signature, concordance des périmètres.
2. Documentation utile	- Organigramme fonctionnel du service des personnels concernés

Constitution de l'échantillon à contrôler

3. Nature des opérations à contrôler et seuil éventuel	Liste des utilisateurs Chorus formulaires.
4. Périmètre temporel des opérations à contrôler	Situations extraites à la date du 01/04/N (photographie à date)
5. Nombre d'opérations à contrôler	☑ Exhaustif (**après exclusion des habilitations obsolètes**) ☐ Échantillon de ☐ Sans objet. Le contrôle est un diagnostic de process.

Analyse des résultats du contrôle

6. Décompte des anomalies	Une anomalie sera décomptée dans le(s) cas suivant(s) : • Décompter une anomalie pour chaque agent dont le groupe utilisateur de rattachement ne correspond pas au service d'affectation de l'agent
7. Préconisations en cas d'anomalies	Propositions d'actions d'amélioration du dispositif de contrôle interne : • Si lors du contrôle, il a été constaté que l'habilitation n'est pas conforme aux fonctions de l'utilisateur, il convient de le signaler et demander la correction des habilitations de l'agent. Il est rappelé qu'à chaque mouvement de personnel, les chefs de services doivent s'assurer que les habilitations correspondent à la situation de leurs agents (création pour les entrants, suppression ou mise à jour pour les sortants, etc.) • Une check-list des vérifications à mener lors d'un mouvement de personnel pourra être utilement mise en place par le responsable de service.

Précisions sur la formalisation du contrôle dans AGIR

8. Montant des opérations contrôlées	☐ À préciser ☑ Sans objet
9. Montant des anomalies constatées	☐ À préciser ☑ Sans objet
10. Pièces justificatives / Consignes d'archivage	Il convient de joindre *a minima* dans la grille de restitution AGIR, le(s) pièce(s) justificative(s) suivante(s) : • Joindre le fichier des utilisateurs **annoté** des constats ainsi que tout document utile à la compréhension du contrôle et notamment des anomalies
11. Autres	Les précisions suivantes sont attendues dans le champ « Commentaires » : • Le type d'anomalies rencontré (motif) est à inscrire

Question 4	**Q4 - Le principe d'application de l'authentification forte à Chorus formulaire est-il respecté ?**	**Type de grille AGIR :** ☐ Analyse de comptes (AC) ☑ Analyse d'opérations (AO) ☐ Diagnostic de process (DP)

Critères de qualité / Risque(s)	**Objectifs** : Gestion des compétences / Régularité / Probité **Risques** 02.01.06.01_Absence d'organigramme fonctionnel 06.02.01.01_ Absence de suivi et de traçabilité des habilitations au SI 06.02.01.04 _ Absence de demande de suppression ou de modification d'habilitations 06.02.02_ Erreur dans le traitement de la demande d'habilitation 06.04.02.02_Absence de traçabilité des demandes de paramétrage 12.01.10.02_Absence de délégation 12.02.04.01_ Fraude due à l'accès aux systèmes d'information
1. Objectif et méthode du contrôle	Par ce point de contrôle, il s'agit de s'assurer que la solution d'authentification forte est mise en œuvre pour les utilisateurs désignés dans la note du 27 juillet 2022. Conformément aux instructions relatives au renforcement de la sécurité des systèmes d'information financière et au positionnement de notre ministère en la matière, les utilisateurs ayant un rôle de « valideur » dans Chorus formulaire et ceux qui, en complément d'un rôle dans Chorus formulaire, détiennent un clé Token pour l'accès à Chorus cœur doivent utiliser l'authentification forte. Modalité de réalisation : En s'appuyant sur l'export des utilisateurs transmis par la mission Chorus dans lequel le mode d'authentification est indiqué : forte (F) ou simple (S), le contrôle consiste 1. à vérifier que, si l'agent est habilité sur un **GU de validation**, son mode d'authentification est correct, à savoir une authentification forte → concordance entre les colonnes « AUTH » et « GU » ; 2. à rapprocher les données relatives au mode d'authentification de la liste des comptes Chorus cœur, chaque détenteur d'un compte chorus cœur doit être en authentification forte.
2. Documentation utile	- note-DAF-DNE-2022-006941 relative au renforcement de la sécurité des systèmes d'information financière du 27 juillet 2022, - Mode opératoire _ paramétrage pour un accès à Chorus formulaire en authentification forte, - Recueil ou arrêtés de délégations de signature, - Organigramme fonctionnel du service des personnels concernés.

Constitution de l'échantillon à contrôler	
3. Nature des opérations à contrôler et seuil éventuel	Liste des utilisateurs Chorus formulaires.
4. Périmètre temporel des opérations à contrôler	Situations extraites à la date du 01/04/N (photographie à date)

5. Nombre d'opérations à contrôler	☑ Exhaustif (**après exclusion des habilitations obsolètes**) ☐ Échantillon de ☐ Sans objet. Le contrôle est un diagnostic de process.

Analyse des résultats du contrôle	
6. Décompte des anomalies	Une anomalie sera décomptée dans le(s) cas suivant(s) : • Décompter une anomalie pour chaque agent identifié en authentification simple qui relève qui a un compte Chorus cœur ou qui détient un rôle de valideur dans Chorus formulaire.
7. Préconisations en cas d'anomalies	Propositions d'actions d'amélioration du dispositif de contrôle interne : • Si lors du contrôle, il a été constaté que le mode d'authentification n'est pas cohérent avec les accès de l'utilisateur, il convient de corriger la situation. • Une check-list des vérifications à mener, et ajustements à réaliser le cas échéant, lors d'un mouvement de personnel pourra être utilement mise en place par le responsable de service.

Précisions sur la formalisation du contrôle dans AGIR	
8. Montant des opérations contrôlées	☐ À préciser ☑ Sans objet
9. Montant des anomalies constatées	☐ À préciser ☑ Sans objet
10. Pièces justificatives / Consignes d'archivage	Il convient de joindre *a minima* dans la grille de restitution AGIR, le(s) pièce(s) justificative(s) suivante(s) : • Joindre le fichier des utilisateurs **annoté** des constats ainsi que tout document utile à la compréhension du contrôle et notamment des anomalies
11. Autres	Les précisions suivantes sont attendues dans le champ « Commentaires » : • Le type d'anomalies rencontré (motif) est à inscrire