

# CONTRÔLE DES ACCÈS

## En bref

Le contrôle des accès vise à garantir que seuls les utilisateurs autorisés disposent des droits nécessaires à l'exercice de leurs fonctions. La Séparation des Tâches (Segregation of duties - SoD) est un principe fondamental de maîtrise des risques opérationnels, notamment pour prévenir les fraudes ou les erreurs.

Les risques clés incluent notamment le cumul de droits sensibles intra-applicatifs (ex. : création/modification/paiement fournisseur) et inter-applicatifs (ex. accès trésorerie - accès comptabilité), l'absence de revue périodique des droits, la gestion inadéquate des départs temporaires ou définitifs d'utilisateurs internes et externes, la non-traçabilité de la demande et de la validation des attributions des accès, la gestion inadéquate des mobilités internes.

Le commissaire aux comptes doit vérifier l'existence d'une politique formalisée de gestion des accès et de SoD, un outil de gestion des identités, une matrice de séparation des tâches ainsi qu'un suivi régulier des dérogations au travers un contrôle récurrent du correct respect des règles de séparation des tâches.

Les ERP (type SAP, Oracle) doivent être paramétrés pour empêcher les cumuls de fonctions à risque dès la conception des profils et des habilitations.

En cas d'incompatibilités détectées, une analyse des dérogations et des contrôles compensatoires est attendue.

Enfin, l'implication du contrôle interne et de la DSI dans le pilotage est essentielle pour fiabiliser le dispositif de gestion des accès.

## Séquence 1

# Comprendre la thématique

## Contexte et enjeux

Le dispositif de gestion des accès constitue un maillon critique du contrôle interne, en lien direct avec la sécurité des traitements comptables et financiers. Le droit d'accès est, d'une façon générale, le droit nécessaire à un utilisateur pour accéder à des ressources : ordinateur, données, réseau etc.

La séparation des tâches (SoD) vise à prévenir les fraudes, erreurs et abus en interdisant l'accumulation de fonctions incompatibles intra-applicatifs (ex. : création + validation d'un paiement) et inter-applicatifs (ex. accès trésorerie - accès comptabilité).

Pour le commissaire aux comptes, ces éléments revêtent une importance stratégique, dans la mesure où des défaillances peuvent compromettre l'intégrité des opérations comptables et la fiabilité des états financiers. L'absence de revues périodiques des droits, la persistance de profils sensibles non justifiés, la coexistence de droits incompatibles (ex. : création et validation d'un paiement) exposent l'entité auditée à des risques accrus de fraude ou d'erreurs comptables.

Ces faiblesses peuvent remettre en cause la maîtrise des processus clés (achats, ventes, paie, trésorerie, comptabilité) et avoir un impact direct sur la certification des comptes.

Il est donc essentiel pour l'auditeur de s'assurer que l'entité dispose d'un dispositif robuste de gestion des accès, d'un processus défini de gestion et de contrôle des règles de SoD et de contrôles compensatoires documentés en cas de dérogation.

## Cycle des achats

		Création d'une fiche fournisseur	RIB fournisseur	Passation de commande	Réception	Contrôle facture fournisseur	Paiement fournisseur	État de rapprochement bancaire	Lettrage compte fournisseur	Rapprochement BA/BG
1	Création d'une fiche fournisseur									
2	RIB fournisseur									
3	Passation de commande									
4	Réception									
5	Contrôle facture fournisseur									
6	Paiement fournisseur									
7	État de rapprochement bancaire									
8	Lettrage compte fournisseur									
9	Rapprochement BA/BG									

## Cycle des ventes

		Création d'une fiche client	RIB client	Émission de commande	Suivi des encaissements	Lettrage compte client	Émission d'avoirs	Rapprochement BA/BG	Relance client
1	Création d'une fiche client								
2	RIB client								
3	Émission de commande								
4	Suivi des encaissements								
5	Lettrage compte client								
6	Émission d'avoirs								
7	Rapprochement BA/BG								
8	Relance client								

	Risque significatif
	Risque moyen
	Risque acceptable

Les enjeux et risques spécifiques liés au contrôle des accès et à la séparation des tâches à couvrir par les commissaires aux comptes afin d'évaluer leur impact potentiel sur les comptes annuels et la fiabilité des traitements comptables sont les suivants :

- Absence de procédure de gestion et de validation des accès qui couvre création, modification, suppression des droits avec une vérification des règles SoD avec une attention particulière,
- Le cas échéant, la formalisation des règles de SoD dans une matrice de séparation des tâches détaillant les combinaisons incompatibles des habilitations basées sur l'analyse des fonctions incompatibles sur les processus critiques (achats, paie, comptabilité générale),
- Persistance de profils sensibles non justifiés,
- Absence de piste d'audit pour les actions critiques,
- Absence de contrôles compensatoires en cas de dérogation aux règles SoD,
- Absence de revue périodique des accès.

Ces lacunes peuvent affecter la traçabilité, l'intégrité et la fiabilité des écritures comptables. Elles sont susceptibles d'entraîner des anomalies non détectées ou des erreurs significatives, avec incidence potentielle sur l'opinion d'audit.

Le droit d'accès à une ressource ou un système d'information doit être aligné au poste occupé par le collaborateur. Il doit par ailleurs prendre en compte l'aspect relatif à la séparation des tâches, pour éviter une situation d'auto-approbation, contraire aux principes élémentaires du contrôle interne quel que soit le niveau de droit d'accès autorisé. Les règles de séparation des tâches et le principe du moindre privilège doivent s'appliquer également aux accès en lecteur seule. Les avantages liés à la correcte séparation des tâches résident dans la facilitation de la détection des erreurs (involontaires ou frauduleuses). Les deux matrices ci-contre illustrent les tâches incompatibles entre elles pour le cycle des achats et le cycle des ventes. Elles sont un exemple concret des tâches qui ne doivent pas être réalisées par les mêmes personnes. Toutefois, l'organisation de l'entité et le jugement professionnel du commissaire aux comptes doit être pris en considération pour adapter ces matrices à l'environnement applicable (NEP 315).

## Conséquences pour le commissaire aux comptes

Les enjeux liés au contrôle des accès et à la séparation des tâches (SoD) influencent directement l'approche d'audit du commissaire aux comptes. En présence de faiblesses identifiées dans ces dispositifs, celui-ci devra adapter sa planification en intensifiant les tests sur les cycles sensibles (achats, paie, trésorerie), vérifier la traçabilité des opérations critiques, et étendre la portée de ses contrôles substantifs. L'absence de SoD effective ou de revue périodique des habilitations constitue un facteur de risque majeur qui peut conduire à une évaluation plus faible du contrôle interne et justifier une approche d'audit plus substantielle. Dans certains cas, ces constats peuvent également alimenter le jugement professionnel du CAC sur la fiabilité du dispositif global de gouvernance, voire impacter la formulation de son opinion.

En conséquence, les accès et leurs contrôles constituent un élément du dispositif de contrôle interne de l'entité. Le pilotage des accès au patrimoine applicatif de l'entité dépend à la fois du service des ressources humaines (connaissance du profil et du niveau de responsabilité) et de la DSI (connaissance des outils et de leurs fonctionnalités), ce qui suppose une communication permanente pour une mise à jour des profils utilisateurs et droits d'accès correspondant en fonction de l'évolution des effectifs (entrées / mouvements/sorties) au sein de l'entité.

## Séquence 2

# Mission du CAC : objectifs, bonnes pratiques et outils

### Thématique 1

## Gestion des accès

### Objectifs

Dans le cadre de sa mission et conformément à la NEP 315 (compréhension de l'entité et de son environnement), le commissaire aux comptes doit vérifier que l'entité dispose d'un dispositif formalisé de gestion des accès. Il s'attache à valider l'existence d'une politique d'attribution des droits fondée sur le principe du moindre privilège (accès juste nécessaire), la traçabilité et la validation des créations, modifications et suppressions de comptes utilisateurs, ainsi que la mise en œuvre de revues périodiques des accès. Il vérifie que les droits sont systématiquement révoqués en cas de départ, de changement de fonction ou d'inactivité prolongée.

Il est également essentiel de s'assurer que les contrôles soient effectués non seulement au niveau du réseau si existant, mais aussi au niveau applicatif. Les comptes à droits étendus, sont des comptes utilisateurs auxquels sont associés des droits ou permissions élargis, leur permettant d'accéder à des fonctionnalités, services ou ressources supplémentaires par rapport à des comptes standards. Ils doivent être restreints et justifiés. Ils doivent également faire l'objet d'un contrôle renforcé, notamment d'une revue périodique et d'une supervision d'activité. Ces travaux visent à garantir l'intégrité des données, la sécurité des systèmes et la fiabilité des traitements comptables et financiers.

## Bonnes pratiques

- Définir, formaliser et mettre en place processus formalisé de gestion des accès (entrée/mouvement/sortie) en lien avec les processus RH et en intégrant les principes de moindre privilège (accès juste nécessaire) et de SoD,
- Identifier, dans une cartographie fonctionnelle et applicative, les principaux systèmes d'information qui concourent à la construction des états financiers (logiciels comptables, logiciels de gestion, logiciels métier) et veiller à définir les profils et les droits associés aux différents cas d'usage, en respectant les principes du moindre privilège et les règles SoD,
- Mettre en place un processus de revue périodique des accès (de toute nature),
- Sécuriser les comptes à droits étendus (administrateurs) par une supervision renforcée, une journalisation des actions et, idéalement, l'usage de coffres-forts pour les mots de passe,
- Définir et mettre en place un contrôle permettant de désactiver les comptes inactifs automatiquement après un délai défini (ex. 90 jours).

## Outils & documentations mises à disposition

- Politique de gestion des accès et procédures et workflows associés en identifiant les outils, les acteurs, les rôles et responsabilités et les contrôles mis en place,
- Extractions détaillées des accès associés aux principaux systèmes d'information qui concourent à la construction des états financiers (logiciels comptables, logiciels de gestion, logiciels métier),
- Rapport ISAE 3402
- Registres des comptes utilisateurs (création, modification, suppression)
- Listes de mouvements RH (entrée, sortie, mobilité) et listes des effectifs RH (internes, externes, stagiaires, etc.),
- Compte-rendu des revues périodiques des droits incluant les extractions avant et après des utilisateurs et accompagnés de la liste des actions correctives,
- Cartographie des applications critiques qui concourent à la construction des états financiers et dictionnaires des profils associés en identifiant les accès à droits étendus,
- Plans d'actions issus d'audits internes ou de contrôles précédents

## Impact dans la stratégie du commissaire aux comptes

Ces éléments analysés permettent au CAC d'évaluer la robustesse du contrôle général sur l'intégrité des systèmes d'information. Une faiblesse dans la gestion des accès pourrait élever le niveau de risque d'audit, notamment sur la fiabilité des données comptables et financières. Cela peut justifier un élargissement du périmètre de contrôle IT, une intensification des tests substantifs, et la formulation de recommandations fermes dans la lettre d'observations. Une analyse d'impact doit être menée par les commissaires aux comptes afin d'identifier si des mesures compensatoires (procédures, contrôles etc.) permettent de mitiger le risque résiduel associé à des éventuelles faiblesses identifiées dans la gestion des accès. Par exemple un compte utilisateur appartenant à un ancien collaborateur n'a pas été désactivé plusieurs mois après son départ.

Le CAC devra analyser si une connexion post-départ est effectuée. Dans le cas ou, il n'y a pas de connexion post-départ.

Le risque résiduel est faible. Il doit également vérifier s'il existe un contrôle compensatoire, tel qu'un monitoring des connexions ou analyse des journaux d'accès sensible, permettant de réduire le risque d'utilisation frauduleuse. En l'absence de tels dispositifs, le risque résiduel est élevé et doit être considéré dans l'évaluation du risque d'audit global.

### Thématique 2

## SoD

### Objectifs

Le commissaire aux comptes, dans le cadre de l'évaluation du contrôle interne (NEP 265 et NEP 330), doit analyser l'existence d'une séparation effective des tâches dans les processus critiques (achats, ventes, paie, trésorerie, comptabilité). Il identifie les combinaisons de droits ou de rôles pouvant générer un risque de fraude ou d'anomalie (ex. : création et validation d'un paiement, saisie et approbation d'écritures).

Il vérifie l'existence d'une cartographie des risques SoD, de contrôles préventifs dans les outils (paramétrage), et, en cas d'exceptions, de contrôles compensatoires documentés et actifs. L'objectif est de s'assurer que les flux comptables ne peuvent être manipulés, que les anomalies soient détectées en amont, et que les processus soient suffisamment robustes pour garantir la régularité, la sincérité et la fidélité des comptes annuels.

### Bonnes pratiques

- Élaborer une matrice de séparation des tâches alignée sur les profils métiers pour les processus clés incluant les règles de SoD intra- applicatifs et inter-applicatifs pour tous les droits applicatifs y compris les droits en consultation, validée par la direction financière et la DSI,
- Mettre en place un contrôle de vérification de la correcte mise à jour des règles SoD suite aux évolutions applicatives impactant les profils utilisateurs et les fonctionnalités,
- Mettre en place un processus permettant d'identifier les règles de séparation des tâches dans la définition et l'implémentation des profils applicatifs,
- Intégrer des contrôles SoD dans les applications, via des profils types ou des alertes en cas de cumul de fonctions lors de la création ou modification d'accès.
- Mettre en place un contrôle de monitoring et d'analyse régulière des dérogations et des violations SoD en documentant systématiquement les justifications et contrôles compensatoires associés,
- Formaliser les justifications et plans de remédiation associés aux cas de non-respect des règles SoD,
- Sensibiliser les utilisateurs clés aux enjeux de la séparation des tâches à travers des sessions de formation ou des communications internes.

## Outils & documentations mises à disposition

- Matrice des fonctions incompatibles par processus (achats, paie, compta...)
- Fiches de poste et rôles dans les systèmes
- Paramétrages des droits dans l'ERP ou autres outils (profil utilisateur)
- Preuves des contrôles de monitoring des règles SoD,
- Relevés et justification des dérogations SoD,
- Relevés d'anomalies SoD issues d'audits internes ou outils GRC
- Justifications et plans de remédiation en cas de violation des règles SoD
- Description des contrôles compensateurs et preuves d'exécution

## Impact dans la stratégie du commissaire aux comptes

Une matrice SoD incomplète ou non suivie génère un risque de manipulation ou de fraude interne, avec une incidence directe sur les cycles sensibles.

Le CAC adaptera alors sa stratégie en renforçant les travaux sur les processus impactés, en approfondissant les tests sur les écritures comptables et en questionnant la gouvernance de contrôle interne. La lettre de recommandations pourra inclure une exigence de mise en conformité rapide.

Par ailleurs, dans les environnements traitant des données à caractère personnel, une mauvaise séparation des tâches peut entraîner des traitements inappropriés ou non conformes aux exigences du Règlement Général sur la Protection des Données (RGPD).

Le commissaire aux comptes, bien que n'étant pas chargé de certifier la conformité au RGPD, peut relever que l'absence de SoD effective compromet également la sécurité des données personnelles (ex. : accès non justifié à des données RH ou clients).

Ces constats peuvent justifier l'émission de recommandations visant la mise en œuvre rapide d'un référentiel de droits cohérent, la formalisation des contrôles compensatoires, et une meilleure articulation entre gestion des risques opérationnels et exigences de conformité réglementaire.

## Séquence 3

# Cas d'usage

### Usage 1

## SoD

### Contexte

Dans le cadre de notre mission légale de l'entité « Best in Class », nous avons pris connaissance de l'environnement informatique qui repose sur l'ERP SAP couvrant notamment les modules Finance (FI), Gestion des articles (MM), Vente & Distribution (SD) et Comptabilité des immobilisations (FI-AA).

Une procédure interne encadre la désactivation des comptes utilisateurs SAP. Elle prévoit :

- une clôture des comptes dans un délai de 31 jours suivant le départ d'un collaborateur,
- une obligation pour les managers de notifier par e-mail le service support le jour du départ.

### Travaux à réaliser

À la demande de la direction et en amont de nos propres investigations, un audit flash a été diligenté sur la thématique des accès SAP, avec un focus sur la désactivation systématique des comptes des collaborateurs sortants.

L'objectif de cette analyse est de vérifier le respect effectif de la procédure en place et de détecter d'éventuelles failles exposant l'entité à des risques de :

- Maintien d'accès pour des utilisateurs non autorisés,
- Usage inapproprié ou détourné des droits d'accès résiduels,
- Altération ou perte de confidentialité des données sensibles.

## Impact pour notre stratégie d'audit

Les constats issus de cette analyse influenceront directement :

- Notre évaluation du risque d'audit IT, notamment sur le cycle achats et finances,
- La détermination du périmètre des contrôles applicables à SAP et la fiabilité du paramétrage des autorisations,
- La nature et l'étendue des tests à mener sur les flux traités via les comptes SAP (journaux, écritures, affectations...).

En cas de lacunes constatées, des recommandations spécifiques seront émises à l'attention de la gouvernance, et nous pourrions être amenés à renforcer notre approche substantielle sur les zones exposées.

## Démarche

L'audit se déroule en deux étapes :

1. **Évaluation de la conception du contrôle** (*Design effectiveness*). L'objectif est d'évaluer si la procédure de désactivation des comptes couvre bien les risques identifiés et si elle est bien implémentée.

**Question clé :** La procédure existante garantit-elle un niveau de contrôle suffisant ?

2. **Évaluation de l'efficacité opérationnelle du contrôle** (*Operating effectiveness*). Il s'agit d'analyser si la procédure est effectivement appliquée.

**Méthodologie :** Comparaison entre les **utilisateurs SAP** actifs et les **collaborateurs présents sur la période auditée** :

**Données nécessaires :**

- Liste des utilisateurs SAP
- Liste des collaborateurs durant la période auditée (internes et externes).

## Séquences de tests détaillées

### Évaluation de la conception du contrôle :

- Analyse de la cohérence du délai de 31 jours : ce délai est-il justifié par des contraintes opérationnelles (délai RH, process IT) ou défini arbitrairement ?
- Vérification de l'absence de mécanisme d'alerte automatique à l'approche ou au dépassement du délai.
- Question à poser : un délai plus court ou un contrôle automatisé limiterait-il mieux l'exposition au risque ?
- Constat 1 : Si la justification du délai est faible ou si aucun contrôle de suivi n'existe, la conception du contrôle est perfectible.

### Identification des comptes utilisateurs SAP des collaborateurs sortants

- Clé de rapprochement :
  - Colonne « Utilisateur » dans la liste SAP.
  - Colonne « LOGIN USER » dans les données RH.
- Outil utilisé : Fonction Excel RECHERCHEV.
- Constat 2 : Si les comptes des collaborateurs sortants ne sont pas désactivés, la procédure n'est pas respectée

### Analyse du délai de désactivation

- Calcul du nombre de jours entre la date de sortie et la date de désactivation.
- Formule Excel : Soustraction simple.
- Constat 3 : Si l'écart dépasse 31 jours, la procédure n'a pas été respectée.

### Identification des connexions après départ

- Vérification des comptes non désactivés ayant une dernière connexion postérieure à la date de sortie.
- Formule Excel : Soustraction simple.
- Constat 4 : Si un nombre de jours positif est constaté, cela signifie qu'un accès a eu lieu après le départ.

## Observations attendues

### Sur la conception du contrôle :

- La procédure de désactivation est-elle claire, complète et réaliste ?
- Existe-t-il des écarts possibles non couverts par la procédure ?

### Sur l'application du contrôle :

- La désactivation est-elle effective ?
- Les délais de désactivation sont-ils respectés ?
- Y a-t-il des connexions suspectes après départ ?
- Des actions correctives sont-elles nécessaires pour renforcer la sécurité ?



## Conclusion

L'analyse de la procédure de désactivation des comptes utilisateurs SAP au sein de l'entité « Best in Class » met en évidence plusieurs points d'attention, tant sur la conception que sur l'application du contrôle.

La procédure actuelle couvre les risques majeurs liés à la gestion des accès, notamment via la définition d'un délai de désactivation et l'implication des managers.

Toutefois, elle présente certaines limites : elle repose sur une notification manuelle, sujette à des oublis ou retards, et aucun mécanisme de vérification a posteriori systématique n'est prévu pour s'assurer de la bonne exécution de la procédure.

Les tests réalisés ont permis de relever plusieurs cas de non-conformité, notamment des comptes non désactivés dans les délais impartis, voire toujours actifs après le départ de certains collaborateurs.

Dans certains cas, des connexions postérieures à la date de sortie ont été observées, ce qui constitue un risque pour la sécurité du système d'information.

Pour améliorer ce dispositif, il est recommandé de mettre en place un processus automatisé de désactivation basé sur les données RH, de réaliser des contrôles réguliers de cohérence entre les comptes SAP et les effectifs RH, d'archiver systématiquement les preuves de désactivation via un outil de ticketing, et de renforcer la sensibilisation des managers sur leurs responsabilités dans le processus de départ.

## Usage 2

## SoD

## Contexte

Dans le cadre de notre mission légale auprès de l'entité « Smart Supply », nous avons pris connaissance de l'environnement informatique structuré autour d'un ERP SAP, intégrant les modules Finance (FI), Gestion des approvisionnements (MM), Paie (PY) et Comptabilité fournisseurs (AP).

L'entité dispose d'une matrice de séparation des tâches validée par la DSI et la direction financière.

Cette matrice recense les combinaisons de rôles incompatibles au sein de SAP (ex. : saisie + validation de factures, gestion fournisseurs + paiement), et un outil a été récemment implémenté pour détecter les violations de SoD.

## Travaux à réaliser

À la suite d'une demande de la gouvernance, nous avons intégré à notre programme d'audit un volet dédié à l'évaluation de la mise en œuvre effective des règles de séparation des tâches.

L'objectif est de :

- Vérifier la couverture et la mise à jour de la matrice SoD,
- Identifier les violations de SoD actives dans les systèmes,
- Évaluer les contrôles compensatoires et les plans de remédiation éventuels.

Ce contrôle vise à prévenir :

- Les risques de fraude interne (ex. : auto-validation de paiements),
- Les erreurs comptables non détectées,
- Une gouvernance inefficace des accès critiques.

## Démarche

L'audit se déroule en deux étapes :

### 1. Évaluation de la conception du contrôle (*Design Effectiveness*) :

**Objectif** : évaluer si la matrice SoD est exhaustive, validée et bien alignée avec les processus métiers.

**Question clé** : Le dispositif en place permet-il de prévenir efficacement les conflits de fonctions ?



## 2. Évaluation de l'efficacité opérationnelle du contrôle (*Operating Effectiveness*) :

**Objectif :** tester si les règles SoD sont bien respectées dans les systèmes en production.

**Méthodologie :**

- Obtenir les rapports d'analyse GRC identifiant les conflits de fonctions utilisateurs,
- Comparer les profils attribués à chaque utilisateur avec les fonctions listées comme incompatibles,
- Évaluer la criticité des conflits et la présence de contrôles compensatoires actifs.

## Séquences de tests détaillées

### Revue de la matrice des tâches incompatibles

- Vérifier qu'elle couvre les principaux processus métiers (achats, paie, compta...).
- Identifier les combinaisons à haut risque (ex. : création + validation des fournisseurs).

### Analyse des violations SoD détectées par l'outil GRC

- Exporter le rapport des utilisateurs ayant des profils conflictuels.
- Évaluer le nombre et la nature des conflits (mineur, majeur, critique).
- Vérifier si des dérogations documentées existent.

### Évaluation des contrôles compensatoires

- Pour les utilisateurs avec droits conflictuels : vérifier l'existence d'un journal d'activité, d'une supervision managériale, ou d'un double contrôle opérationnel.
- Examiner les preuves d'exécution de ces contrôles (ex. : signature, log, rapprochement périodique).

## Observations attendues

### Sur la conception du contrôle :

- La matrice SoD est-elle formalisée, validée et alignée avec les risques métiers ?
- Les rôles SAP sont-ils conçus sur un modèle RBAC (contrôle d'accès basé sur le rôle) cohérent ?
- Un contrôle de monitoring des règles SoD est-il défini et mis en place ?

### Sur l'application du contrôle :

- Les dérogations des règles SoD sont-elles documentées et monitorées ?
- Des conflits de fonctions existent-ils sans justification ?
- Les alertes remontées sont-elles traitées efficacement ?
- Les contrôles compensatoires sont-ils actifs et documentés ?

## Conclusion

L'analyse du dispositif de séparation des tâches chez « Smart Supply » met en lumière une démarche structurée, appuyée par une matrice formalisée et l'usage d'un outil GRC.

La conception du contrôle est globalement cohérente, bien qu'une mise à jour plus régulière de la matrice et un alignement renforcé avec les processus métiers soient nécessaires.

L'exploitation des rapports GRC a révélé plusieurs violations actives, dont certaines sans justification formelle ni contrôle compensatoire documenté. Cette situation accroît les risques de fraude interne ou d'erreurs non détectées.

Il est donc recommandé de renforcer la revue périodique des conflits identifiés, de formaliser systématiquement les dérogations accordées, et de garantir l'effectivité des contrôles compensatoires pour les profils à risque.

### Impact pour notre stratégie d'audit

Les résultats de cette analyse auront un impact direct sur :

- Notre évaluation du contrôle interne général et IT, notamment sur les cycles achats, trésorerie et paie,
- La confiance que nous pouvons accorder au paramétrage applicatif et à la fiabilité des données issues de SAP,
- La nature des tests à réaliser sur les écritures sensibles : il pourra être nécessaire de renforcer les travaux substantifs si des conflits SoD critiques sont identifiés sans mesures de contrôle compensatoires adéquates.

En cas de faiblesses constatées, nous pourrions recommander une mise à jour de la matrice SoD, une meilleure formalisation des rôles dans SAP et/ou une automatisation renforcée des alertes de conflits via les outils GRC.

## Séquence 4

# Allez plus loin

### Missions SACC

- donner un avis quant au processus d'attribution des droits d'accès aux applications et infrastructures sous-jacentes
- revoir la politique des mots de passe et son application ainsi que les règles d'authentification
- revoir la conception des rôles et profils mis en œuvre dans les applications pour s'assurer notamment de leur conformité en termes de séparation de fonctions
- revoir l'attribution de ces rôles et profils aux utilisateurs afin de s'assurer qu'ils ne cumulent pas des droits incompatibles
- s'assurer qu'un processus est en place de revue périodique des utilisateurs et des rôles et profils et le tester

### Ressources pratiques

- NEP 240 : Prise en considération de la possibilité de fraudes lors de l'audit des comptes
- NEP 250 : Prise en compte du risque d'anomalies significatives dans les comptes résultant du non-respect des textes légaux et réglementaires
- NEP 265 : Communication des faiblesses du contrôle
- NEP 315 : Connaissance de l'entité et de son environnement et évaluation du risque d'anomalies significatives
- NEP 330 : Procédures d'audit mises en œuvre par le commissaire aux comptes à l'issue de son évaluation des risques
- Norme ISO CEI 27001 : Gestion de la Sécurité des Systèmes d'Information
- Guide ANSSI
- COBIT : Control Objectives for IT (référentiel de gouvernance des Systèmes d'Information)

### Formations recommandées

Formation dispensée par la CRCC et l'Université Paris-Dauphine