RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

FINANCES PUBLIQUES

La maîtrise des risques financiers et informatiques

La lutte contre la fraude aux faux ordres de virement

Les guides relatifs au système d'information

Guide méthodologique relatif au contrôle interne des systèmes d'information des collectivités locales

Recueil de recommandations relatives au système d'information financière de l'État

Direction générale des Finances publiques
Mission Responsabilité Doctrine et Contrôle Interne Comptables
Juillet 2022

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

La lutte contre l'escroquerie aux faux ordres de virements

Les guides relatifs au système d'information

Le guide méthodologique relatif au contrôle interne des systèmes d'information des collectivités locales

Le recueil de recommandations relatives au système d'information financière de l'État

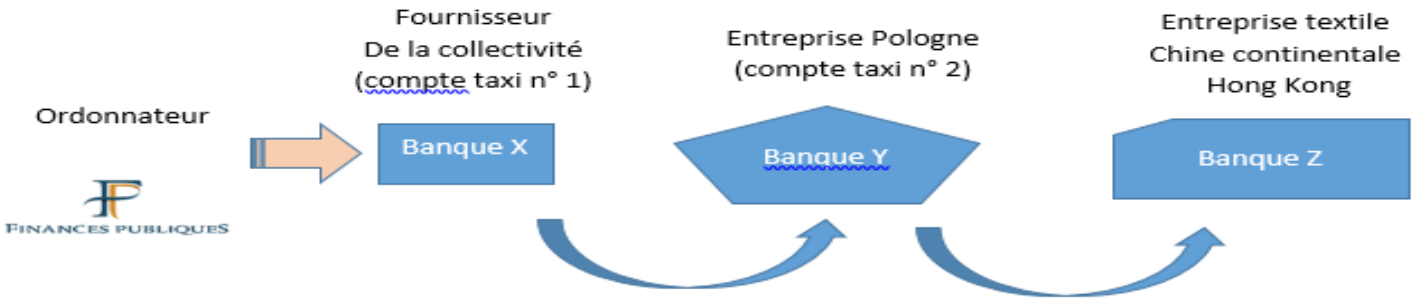
RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

Les modes opératoires des escroqueries aux faux ordres de virement (1/2)

Les escroqueries aux faux ordres de virement (FOVI) visent à pousser un salarié ou un agent public à effectuer un virement bancaire, **par usurpation d'identité du véritable créancier** ou d'un autre acteur habilité à intervenir dans la chaîne du règlement.

Ce type de manœuvres frauduleuses est identifié depuis 2010, et constitue une réalité pour l'ensemble des acteurs économiques, tant privés que publics.

Pour le secteur public (État, collectivités locales, établissements publics), les FOVI sont en forte recrudescence depuis la crise sanitaire.
Les victimes principales sont très majoritairement les communes.



RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

Les modes opératoires des escroqueries aux faux ordres de virement (2/2)

Les escrocs recourent principalement à trois techniques :

- **l'escroquerie au changement de coordonnées bancaires** : l'escroc peut se faire passer pour un fournisseur, un pensionné, un agent public souhaitant modifier ses coordonnées bancaires ou mettre en place un affacturage. Il s'agit de la fraude la plus commune dans le secteur public.

- la fraude au président : l'escroc usurpe l'identité du président, du DAF ou d'un ordonnateur, et demande à un collaborateur d'effectuer un virement de toute urgence à un tiers, au prétexte d'un dossier sensible et confidentiel

- l'escroquerie à l'informatique : l'escroc peut se faire passer pour un responsable informatique ou pour l'éditeur du logiciel de comptabilité utilisé, pour prendre le contrôle du poste informatique d'un agent en charge de la comptabilité

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

Les signaux d'alerte pour se prémunir des FOVI (1/2)

➢ **transmission de factures par messagerie électronique ou par courrier** (celles-ci pouvant avoir été falsifiées)

Depuis le 1er janvier 2020, toutes les entreprises sont tenues de transmettre leurs factures à destination de la sphère publique via le Portail Chorus Pro (https://chorus-pro.gouv.fr/cpp/utilisateur?execution=e1s1). Les fournisseurs y accèdent au suivi du traitement de la facture et notamment à sa date de paiement.

➢ **demandes de changement de coordonnées bancaires ou d'affacturage par messagerie électronique ou par courrier, en particulier au profit d'un compte de néobanque ou d'un compte étranger**, notamment lorsque le changement concerne :

→ une PME/TPE dont le compte bancaire initial était domicilié dans une banque traditionnelle

→ un nouveau compte bancaire dans un pays autre que celui où se trouve le bénéficiaire supposé du paiement

➢ **courriels d'interlocuteurs** utilisant des adresses électroniques de type contact.noreplyXXX@gmail.com ou des noms de domaine de type @dr.com, @mail.com, @protonmail.com, @servicecomptabilite.net, @financier.com

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

Les signaux d'alerte pour se prémunir des FOVI (2/2)

➢ Demandes de confirmation de virement/date de paiement accompagnant la demande de changement de coordonnées bancaires ou ultérieures, **laissant supposer que le demandeur n'a pas accès à Chorus Pro** ;

➢ Fautes d'orthographe, **logo et/ou adresse de messagerie légèrement modifiés**, préfixe téléphonique, etc.

➢ **Contrats d'adhésion** joints à une facture portant une mention d'**affacturage**.

→ les escrocs peuvent également se présenter en tant qu'**organisme financier bénéficiaire** d'un affacturage (affactureur ou factor).

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

Les consignes / conseils pour se prémunir des FOVI (1/3)

➢ effectuer un **contre-appel** au fournisseur à partir de **coordonnées fiabilisées** (internet ou pages jaunes)

➢prévoir les coordonnées bancaires du créancier sur les formulaires de demande de subvention et les reporter dans les décisions d'attribution. De manière plus générale, mentionner les coordonnées bancaires sur l'ensemble des documents contractuels.

➢**adopter les réflexes CHORUS PRO fournisseurs**

→ indiquer les coordonnées bancaires de paiement sur la facture ou renseigner le champs « références bancaires » sur son compte Chorus pro ;

→ déposer les nouveaux RIB en pièce jointe complémentaire d'une facture sur Chorus Pro.

➢**adopter les réflexes CHORUS PRO ordonnateurs**

→ communiquer aux fournisseurs les réflexes listés ci-dessus ;

→ prendre en compte uniquement les factures transmises par Chorus Pro afin de limiter le risque de falsification très présent lors des envois par messagerie ou par voie papier ;

→ en cas de réception d'une nouvelle coordonnée bancaire par mel, ne pas l'intégrer dans la base tiers en l'état et rappeler au fournisseur les réflexes Chorus Pro attendus ;

→ tenir compte uniquement des coordonnées bancaires ayant transitées par Chorus Pro (mention sur la facture PDF, saisie dans le champs "références bancaires du fournisseur" ou RIB en PJ d'une facture déposé sur Chorus) ;
→ utilisation de la fonction "suspension de la facture" afin de demander au fournisseur d'ajouter le RIB sur Chorus Pro dans l'intérêt de limiter le risque de fraude.

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

Les consignes / conseils pour se prémunir des FOVI (2/3)

➢ lors des demandes de changement de coordonnées bancaires ou d'affacturage, consulter :

→ le site IBANCALCULATOR (https://www.ibancalculator.com/), rechercher la banque associée à l'IBAN bénéficiaire du paiement ; si la banque est différente de celle indiquée sur le RIB, il y a risque de falsification

→ le site REGAFI (le registre des agents financiers de la Banque de France) dans le cadre d'un affacturage, pour s'assurer que l'organisme dispose bien d'un agrément de la Banque de France

➢ **ne pas divulguer** à l'extérieur, ou à un contact inconnu, des informations sur le fonctionnement de l'administration et sur ses fournisseurs (organigramme, contacts, documents comportant la signature d'acteurs-clés, procédures internes, etc.)

➢ accroître la vigilance pendant les **périodes de congés** et de **forte charge de travail**

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

Les consignes pour se prémunir des FOVI (3/3)

➢ être vigilant* sur les demandes de modification de coordonnées bancaires vers des **néobanques** et notamment en présence des données suivantes :

TYPE DE COMPTE	CODE BANQUE	CODE BIC
Compte Nickel « FINANCIERE DES PAIEMENTS ELECTRONIQUES »	16598	FPELFR21
Compte QONTO « OLINDA SAS »	16958	QNTOFRP1
Compte PREPAID / PAYTRIP / GLOBEX « PFS CARD SERVICES »	21833	PRNSFRP1
Compte MA FRENCH BANK « LA BANQUE POSTALE »	16908	LBDIFRP1
Compte ANYTIME « PPS EU SA » / « ORANGE BANK »	25733	PSSSFR22

Attention, le nom de la banque pouvant avoir été falsifié sur le RIB (mention d'une banque traditionnelle à la place de la néobanque), il convient de se fier plutôt au code BIC ou au code Banque pour identifier les néobanques.

* Cette vigilance ne doit en aucun cas aboutir à un blocage systématique des mandatements/paiements vers ce type de comptes au risque d'être en non-conformité avec la réglementation européenne, mais à un contrôle plus approfondi afin de s'assurer que les coordonnées bancaires appartiennent bien au véritable créancier.

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

Les actions de sensibilisation pour se prémunir des FOVI

➢ **Renforcer la sensibilisation** aux FOVI de l'ensemble des acteurs de la dépense, et notamment au sein des petites collectivités. S'assurer que chacun d'entre eux ait conscience des risques et connaisse les moyens de s'en prémunir.

➢ **Accroître la vigilance sur le risque de piratage des boîtes de messagerie :**

→ Changer de mot de passe de connexion en cas de doute et régulièrement ;

→ S'assurer de l'absence de paramétrages de transfert de message vers des adresses tierces ;

→ Ne jamais cliquer sur des liens ou prendre contact à partir de messages suspects ;

→ Ne jamais communiquer d'informations d'authentification de messagerie (y compris au fournisseur d'accès).

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

La conduite à tenir en cas d'escroquerie (1/2)

Dans le cas d'une escroquerie avérée (→ les sommes ont été payées sur un compte frauduleux)

➢ **Prévenir immédiatement le comptable** afin qu'en cas de paiement, il engage le plus rapidement possible les procédures bancaires de récupération des fonds. Si le paiement n'est pas encore intervenu, le comptable rejette la dépense afin de bloquer sa mise en paiement.

➢ **Transmettre au comptable** dans les meilleurs délais, les pièces liées à l'escroquerie (échanges de courriels avec l'escroc demandant le changement de RIB, etc.). Le comptable fera parvenir l'ensemble de ces pièces à l'administration centrale, afin de demander le blocage du compte bancaire dans certaines applications métiers de la DGFiP.

➢ **Invalider les coordonnées bancaires frauduleuses** dans la base tiers du logiciel financier.

➢ **Déposer plainte** en tant que victime directe d'escroquerie (prioritairement auprès du service régional de police judiciaire, ou bien auprès d'un service de police ou de gendarmerie de proximité, ou encore par courrier recommandé avec accusé de réception adressé au procureur de la république).

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

La conduite à tenir en cas d'escroquerie (2/2)

Dans le cas d'une tentative de fraude (→ aucun paiement n'a été réalisé)

- **Prévenir immédiatement le comptable et lui transmettre** dans les meilleurs délais, les pièces liées à l'escroquerie (échanges de courriels avec l'escroc demandant le changement de RIB, etc.). Le comptable fera parvenir l'ensemble de ces pièces à l'administration centrale, afin de demander le blocage du compte bancaire dans certaines applications métiers de la DGFiP.

- **Invalider les coordonnées bancaires frauduleuses** dans la base tiers du logiciel financier.

- **Déposer plainte en tant que victime directe d'escroquerie,** prioritairement auprès du service régional de police judiciaire, ou bien auprès d'un service de police ou de gendarmerie de proximité, ou encore par courrier recommandé avec accusé de réception adressé au procureur de la république.

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

Les conséquences du signalement de l'escroquerie (1/2)

Importance de signaler immédiatement tous les cas de fraudes de type FOVI, y compris les tentatives n'ayant pas donné lieu à paiement

- Un partage d'information auprès de la Banque de France.

- Un partage d'information auprès de l'OCRGDF (Office Central pour la Répression de la Grande Délinquance Financière) du ministère de l'Intérieur et auprès de TRACFIN, cellule de renseignement financier du ministère de l'Économie, des Finances et de la Relance pour enquête sur les auteurs des escroqueries.

Objectif : croiser les informations relatives aux comptes frauduleux pour appuyer les actions judiciaires, accroître les possibilités de retour des fonds virés à l'étranger via l'appui du réseau des Attachés de Sécurité Intérieure auprès des ambassades ou des cellules de renseignement financier étrangères.

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

Les conséquences du signalement de l'escroquerie (2/2)

Importance de signaler immédiatement tous les cas de fraudes de type FOVI, y compris les tentatives n'ayant pas donné lieu à paiement

- Un blocage automatique des coordonnées bancaires identifiées comme frauduleuses dans les applications métiers de la DGFIP (Chorus et Hélios).

- Un partage d'information des coordonnées bancaires identifiées comme frauduleuses avec les agents comptables publiées sur le site intranet de la DGFiP http://ulyssecontrib.dgfip/metier/la-documentation-0

Objectif : empêcher les nouvelles escroqueries sur les coordonnées bancaires identifiées comme frauduleuses.

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

La lutte contre l'escroquerie aux faux ordres de virements

Les guides relatifs au système d'information

Le guide méthodologique relatif au contrôle interne des systèmes d'information des collectivités locales

Le recueil de recommandations relatives au système d'information financière de l'État

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

Le guide méthodologique relatif aux contrôle interne des systèmes d'information des collectivités locales

La DGFiP a rédigé en 2020 un « **Guide méthodologique relatif au contrôle interne des systèmes d'information des collectivités locales** »

→ à la demande du **comité national de fiabilité des comptes locaux** dans le cadre de l'expérimentation de la certification des comptes

→ validé par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et par la Direction interministérielle du numérique (DINUM).

Publié sur le site Collectivités locales
https://www.collectivites-locales.gouv.fr/finances-locales/guide-methodologique-relatif-au-controle-interne-des-systemes-dinformation-des

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

Le guide méthodologique relatif aux contrôle interne des systèmes d'information des collectivités locales

- Le contrôle interne des systèmes d'informations des collectivités locales consiste à :

  → faire face aux risques numériques ;

  → couvrir tous les facteurs déclenchants : humain, technique, environnemental, juridique ;

  → élaborer une cartographie des risques (inhérents puis résiduels) annuellement mise à jour ;

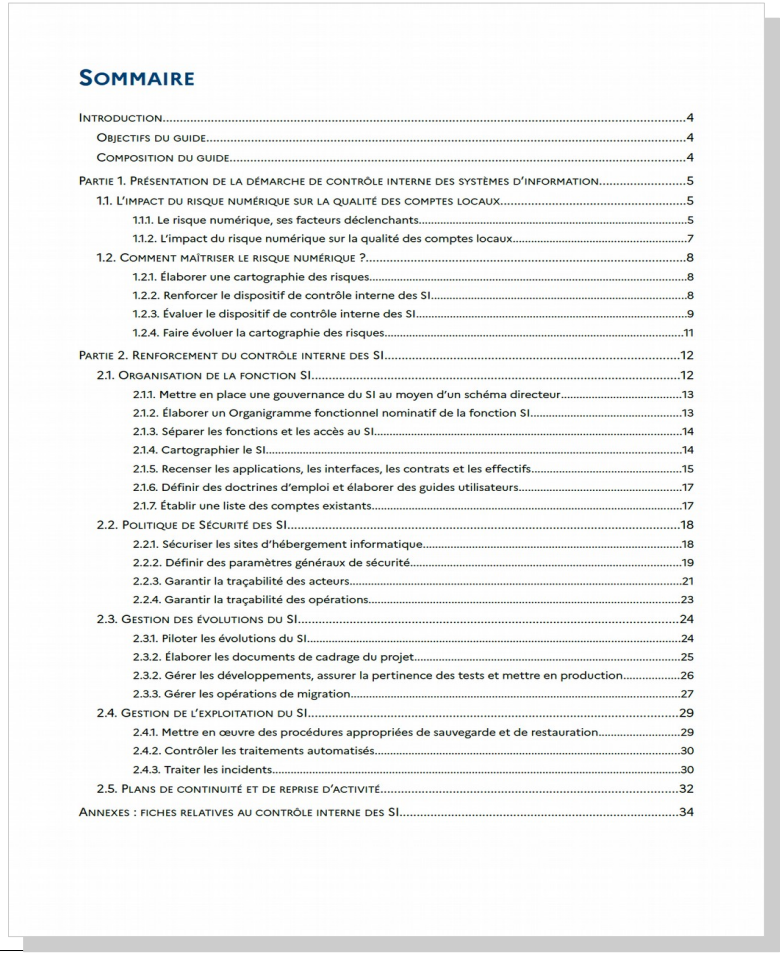
  → mettre en place ou renforcer un dispositif de contrôle interne (autour de trois piliers : la documentation, l'organisation et la traçabilité)

  → évaluer le dispositif (contrôle de supervision / audit interne ou externe, notamment dans le cadre de la certification)

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Le guide méthodologique relatif aux contrôle interne des systèmes d'information des collectivités locales

Le support se compose d'un premier volet littéral comprenant des explications sur le contexte, les définitions, les enjeux…

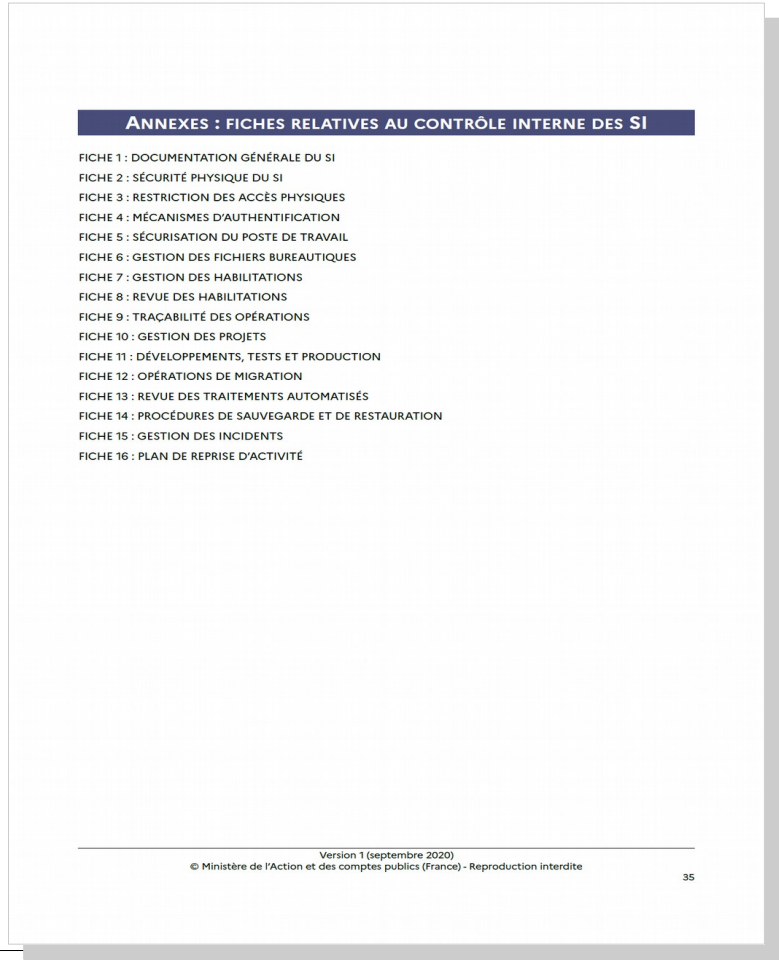


Sommaire

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Le guide méthodologique relatif aux contrôle interne des systèmes d'information des collectivités locales

… Et d'un second volet composé de fiches thématiques dédiées au contrôle interne des systèmes d'information.



ANNEXES : FICHES RELATIVES AU CONTRÔLE INTERNE DES SI

FICHE 1 : DOCUMENTATION GÉNÉRALE DU SI
FICHE 2 : SÉCURITÉ PHYSIQUE DU SI
FICHE 3 : RESTRICTION DES ACCÈS PHYSIQUES
FICHE 4 : MÉCANISMES D'AUTHENTIFICATION
FICHE 5 : SÉCURISATION DU POSTE DE TRAVAIL
FICHE 6 : GESTION DES FICHIERS BUREAUTIQUES
FICHE 7 : GESTION DES HABILITATIONS
FICHE 8 : REVUE DES HABILITATIONS
FICHE 9 : TRAÇABILITÉ DES OPÉRATIONS
FICHE 10 : GESTION DES PROJETS
FICHE 11 : DÉVELOPPEMENTS, TESTS ET PRODUCTION
FICHE 12 : OPÉRATIONS DE MIGRATION
FICHE 13 : REVUE DES TRAITEMENTS AUTOMATISÉS
FICHE 14 : PROCÉDURES DE SAUVEGARDE ET DE RESTAURATION
FICHE 15 : GESTION DES INCIDENTS
FICHE 16 : PLAN DE REPRISE D'ACTIVITÉ

Version 1 (septembre 2020)

35

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

Le guide méthodologique relatif aux contrôle interne des systèmes d'information des collectivités locales

Les points clés :

- assurer la continuité de l'activité :
  - → lutter contre les intrusions/prises de contrôle du SI ou des outils majeurs
  - → permettre l'accès à distance en toute sécurité des agents habilités

- assurer la sécurité des données :
  - → incompatibilité des rôles
  - → séparation des tâches (administrateur/opérationnel – saisisseur/valideur)
  - → revue des habilitations (pour la DGFiP : accès au PIGP permettant d'accéder aux applications DGFiP)
  - → détection des mails ou PJ de mails risqués

La protection et la sécurisation des messageries des collectivités doit constituer une préoccupation majeure. En effet, leur piratage (hameçonnage pour récupérer les codes d'accès à la messagerie puis paramétrage d'un transfert des messages vers une adresse mail tierce à l'insu du titulaire de la boîte) est constaté dans la grande majorité des FOVI.

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

Le guide méthodologique relatif aux contrôle interne des systèmes d'information des collectivités locales

Une **approche différenciée** en fonction des typologies de collectivités

- pour les collectivités sans service informatique spécialisé :

  → cibler les points majeurs : mécanismes d'authentification (fiche 4) et sécurisation du poste de travail (fiche 5)

  → sensibiliser aux risques de **piratages de messagerie** : cf. fiche CNIL

- pour les collectivités disposant d'un service informatique ou bien d'une structure de contrôle interne :

  → le guide est une base d'informations et d'auto-diagnostic

  → prioriser les actions pour sécuriser le SI, le cas échéant en lien avec les structures intercommunales ou des cabinets spécialisés

  → point d'appui à la mise en œuvre des normes spécialisées (ISO 27002, 27001)

→ accompagnement possible des collectivités par l'ANSSI et cybermalveillance.gouv.fr

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

La lutte contre l'escroquerie aux faux ordres de virements

Les guides relatifs au système d'information

Le guide méthodologique relatif au contrôle interne des systèmes d'information des collectivités locales

Le recueil de recommandations relatives au système d'information financière de l'État

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

Le recueil de recommandations relatives au système d'information financière de l'État (SIFE)

Diffusé à l'ensemble des référents ministériels du contrôle interne en 2020

Disponible à l'adresse suivante : https://chorus-diapason.finances.ader.gouv.fr/docs/dgfip-mission-rdcic-recueil-de-recommandations-relatives-au-systeme-dinformation-financiere-de-letat/

- Élaboré par la DGFiP en lien avec l'Agence pour informatique financière de l'État (AIFE)

- Couvre l'ensemble du SIFE : CHORUS, ainsi que les applications de gestion, interfacées ou non avec CHORUS, dès lors qu'elles **impactent *in fine* la comptabilité de l'État**

- À défaut d'unicité et d'homogénéité de l'environnement et des configurations informatiques de gestion, la définition et le déploiement de dispositifs de contrôle interne du SIFE nécessitent :
  - → une analyse fine des situations
  - → une adaptation des orientations proposées