CNIEG

Votre retraite, notre métier

Rapport relatif au dispositif de Contrôle Interne

2021

Nicolas MITJAVILE
Directeur de la CNIEG

Hervé DUCHAIGNE
Directeur comptable et financier

Caisse Nationale des Industries Électriques et Gazières
20, rue des Français Libres
BP 60415
44 204 NANTES Cedex 2

Table des matières

INTRODUCTION 04

CONFORMITÉ AUX LOIS ET RÈGLEMENTS 05
- Le Code de la sécurité sociale (CSS) 06
- Les tutelles 07
- L'Inspection générale des affaires sociales (IGAS) 08
- L'Inspection générale des finances (IGF) 08
- La Cour des comptes 08
- Les Commissaires aux Comptes 08

ORGANISATION DU CONTRÔLE INTERNE À LA CNIEG 09
- Structure dédiée 10
- Le comité des risques 10
- La direction 10
- Le comité d'Audit 11
- Plan de contrôle interne (PCI) 11
- Méthodologie de contrôle 11
- Méthode d'échantillonnage 12
- Compléments de contrôle du flux 13
- Contrôles sur stock 13
- Plan de contrôle du DCF 13

PILOTAGE PAR LES RISQUES 14
- Définition du risque 15
- Méthodologie de gestion et de maîtrise des risques 15
- Modalités d'analyse des risques 18
- Modalités de suivi des risques 20
- Cartographie des risques 20

LES FAITS MARQUANTS DE 2021 21
- Synthèse des résultats PCI 2021 22
- Transfert d'activités métiers 24
- Priorités 2021 24
- Les indicateurs de suivi du contrôle interne 25
- Optimisation des enjeux 26
- Réorganisation des activités 26

RÉSULTATS DÉTAILLÉS DU PCI 2021 27
- Indicateurs 28
- Analyse des résultats 29
- Zoom sur les compléments de contrôle 31
- Zoom sur les contrôles sur stock 31
- Évolution des taux d'anomalies 32
- Évolution de la détection des anomalies 32
- Impacts financiers 33
- Répartition de l'impact financier 34
- Recouvrement & contrôle 2021 35

CONTRÔLE DU SYSTÈME D'INFORMATION 36
- Impact Financier 37
- Exécution des traitements 37
- Projets informatiques 38
- Modification de traitements (maintenance) 38
- Synthèse des contrôles 2021 39
- Incidents informatiques 39
- Sécurité du SI 40
- Règlement général de protection des données 42

DISPOSITIF DE LUTTE CONTRE LA FRAUDE 44
- Groupe d'analyse du risque de fraude (GARF) 45
- Travaux 2021 45
- Méthodes de lutte contre la fraude transfrontalière ou internationale 45
- Résultats 2021 46

RÉSULTATS DU PLAN DE CONTRÔLE DU DIRECTEUR COMPTABLE ET FINANCIER 2021 48
- Immobilisations 49
- Frais de personnel 49
- Gestion des tiers 50
- Gestion technique (comptabilité du Régime IEG) 50
- Trésorerie 51
- Obligations 52
- Réglementation 52

AXES D'AMÉLIORATION POUR 2022 53
- Poursuite de la transformation du Pôle Maîtrise des Risques 54
- Pilotage par les risques 55
- Maitrise des risques 55
- Gestion des incidents informatiques 55

GLOSSAIRE 56

Introduction

La Caisse nationale des industries électriques et gazières (CNIEG) est un organisme de sécurité sociale de droit privé sous la tutelle de l'État.

Elle a été créée le 1er janvier 2005 par la loi n° 2004-803 du 9 août 2004. Elle assure la gestion du régime spécial d'assurance vieillesse, invalidité, décès, accidents du travail et maladies professionnelles des industries électriques et gazières (IEG).

La gouvernance de la CNIEG est assurée par :

- un conseil d'administration composé de 16 membres dont la durée du mandat est de 5 ans et répartis en deux collèges :
  - 8 représentants des salariés désignés par les organisations syndicales représentatives au sein de la branche des IEG ;
  - 8 représentants des employeurs désignés par les fédérations représentatives des employeurs de la branche des IEG.
- un directeur et un directeur comptable et financier (DCF) nommés par le conseil d'administration aux séances duquel ils participent avec voix consultative.

Depuis le 1er janvier 2005, le régime de retraite des IEG est un régime « adossé » financièrement : son financement est en partie assuré par des prestations d'adossement versées par les régimes de droit commun CNAV et AGIRC-ARRCO en contrepartie du reversement par la CNIEG des cotisations de retraite équivalent régimes de droit commun, patronales et salariales, reçues des employeurs des IEG et calculées dans le strict respect des règles des régimes de droit commun. Ce dispositif permet de sécuriser le financement du régime, dans le respect d'une stricte neutralité financière tant pour le régime des IEG que pour les régimes de droit commun.

Conformément à l'article D. 114-4-16 du Code de la sécurité sociale, la CNIEG produit annuellement un rapport présentant le bilan de son dispositif de contrôle interne et intégrant les conclusions des audits.

Conformité aux lois et règlements

Conformité aux lois et règlements

LE CODE DE LA SÉCURITÉ SOCIALE (CSS)

En tant qu'organisme de sécurité sociale, la CNIEG se conforme aux dispositions du Code de la sécurité sociale qui lui sont applicables.

Au titre du contrôle interne, la CNIEG répond aux articles D. 114-4-6 à D. 114-4-18 du CSS.

L'article D. 114-4-6 du Code de la sécurité sociale prévoit que : « Le directeur et [le directeur comptable et financier] de l'organisme national conçoivent et mettent en place conjointement un dispositif national de contrôle interne dont l'objet est d'assurer la maîtrise des risques de toute nature, notamment financiers, inhérents aux missions confiées à cet organisme ».

Un protocole d'accord du contrôle interne à la CNIEG, en date du 1er juin 2005 et toujours en vigueur, définit « les modalités de l'association entre le directeur et [le directeur comptable et financier] lors des différentes phases de contrôle interne et dans les domaines suivants :

- définition du champ d'application ;
- définition des orientations et des objectifs généraux ou particuliers ;
- conception du dispositif général de contrôle interne ;
- élaboration du plan détaillé de contrôle interne ;
- définition de méthodes de travail et de moyens humains et matériels ;
- réalisation des actions ;
- examen des résultats d'activités et mesures correctives ;
- suivi des décisions et supervision du dispositif de contrôle interne. »

Toute évolution relative au contrôle interne fait l'objet d'un avenant au protocole initial.

À minima, un avenant est signé chaque année afin de valider le plan de contrôle interne.

À compter de 2014, le dispositif de contrôle interne répond aux exigences du décret n° 2013-917 relatif au contrôle interne des régimes obligatoires de base de sécurité sociale et des organismes concourant à leur financement, et participe à apporter une assurance raisonnable quant au respect des objectifs suivants :

- maîtrise des risques financiers, directs et indirects, inhérents aux missions confiées à la CNIEG ;
- conformité aux lois, règlements et conventions ;
- exactitude des montants de cotisations, des contributions sociales, des autres prélèvements à recouvrer et des prestations liquidées ;
- prévention des indus et recouvrement des créances ;
- utilisation efficiente des fonds publics et des moyens de toute nature mis en œuvre, dans le respect des autorisations budgétaires annuelles et pluriannuelles ;
- protection des personnes et du patrimoine de l'organisme ;
- prévention et détection des fraudes internes et externes ;
- intégrité, fiabilité et caractère exhaustif des informations financières, comptables, budgétaires et de gestion.

Conformité aux lois et règlements

Pour ce faire, le contrôle interne s'applique à l'ensemble des activités et opérations effectuées au sein de la CNIEG et susceptibles d'induire un risque financier direct ou indirect, à effet immédiat ou différé dans le temps.

Il s'exerce également sur les flux d'informations transmis à la CNIEG par des entités extérieures et, par voie de conséquence, peut s'appliquer à ces entités dans le respect des compétences respectives des uns et des autres, dans le cadre des conventions existantes ou à venir.

Conformément à l'article D. 114-4-16 du code de la sécurité sociale, la CNIEG présente au conseil d'administration et à ses autorités de tutelle avant le 30 juin 2022, le bilan 2021 de son dispositif de contrôle interne et plus particulièrement :

- la description des principales caractéristiques du dispositif de maîtrise des risques et du plan de contrôle interne ;
- les résultats des activités de contrôle et des indicateurs de maîtrise des risques ;
- l'analyse des principaux motifs d'anomalies détectées et la description des actions de correction mises en œuvre ou prévues ;
- les conclusions des audits de contrôle interne.

LES TUTELLES

La CNIEG est placée sous la tutelle conjointe du ministre chargé de la sécurité sociale et du ministre chargé du budget.

Une convention d'objectifs et de gestion (COG) a été contractualisée entre les ministères de tutelle et la CNIEG pour la période 2020-2024. Elle poursuit le renforcement du dispositif de contrôle interne avec la mise en place de 5 indicateurs de performance sur l'activité du contrôle interne :

- efficacité de la détection des anomalies par le dispositif de contrôle interne ;
- qualité des résultats du dispositif du contrôle interne ;
- qualité des dossiers avant et après paiement (IQV et IQL) ;
- taux d'incidence financière des erreurs (régime) (TIF) ;
- efficacité du dispositif de lutte contre la fraude.

Deux commissaires du Gouvernement, mandatés par chacun des ministères de tutelle, et un contrôleur général assistent aux séances du conseil d'administration avec voix consultative.

L'INSPECTION GÉNÉRALE DES AFFAIRES SOCIALES (IGAS)

L'IGAS est un service d'inspection commun aux ministères chargés de la sécurité sociale, de la santé et du travail.

Dans le cadre de leur mission, les membres de l'IGAS :

- « exercent le contrôle supérieur de tous les [...] organismes [...] qui participent à l'application des législations de sécurité sociale » (CSS art. D 113-1) ;
- « sont chargés d'effectuer les missions et enquêtes d'ensemble sur l'application des législations de sécurité sociale, sur la coordination des différents régimes obligatoires, spéciaux et complémentaires » (CSS art. D 113-2).

En tant qu'organisme de sécurité sociale, la CNIEG peut être contrôlée par l'IGAS.

L'Inspection Générale des Affaires Sociales n'est pas intervenue à la CNIEG en 2021.

L'INSPECTION GÉNÉRALE DES FINANCES (IGF)

L'État exerce sur les organismes de sécurité sociale les contrôles financiers spécialisés du ministère chargé de l'économie et des finances.

C'est ainsi que les organismes de sécurité sociale, dont la CNIEG, sont soumis au contrôle (CSS art. R. 153-9) de l'Inspection générale des finances. Celle-ci intervient dans les mêmes conditions que l'Inspection générale des affaires sociales et, de plus en plus, conjointement avec elle.

L'Inspection générale des finances n'est pas intervenue à la CNIEG en 2021.

LA COUR DES COMPTES

La Cour des comptes contrôle « tous les organismes de droit privé jouissant de la personnalité civile ou de l'autonomie financière et assurant en tout ou en partie la gestion d'un régime légalement obligatoire » d'assurance sociale ou de prestations familiales.

À la suite d'un contrôle, la Cour des comptes communique ses observations tant à l'autorité de tutelle qu'au Président du conseil d'administration de l'organisme contrôlé.

En 2021 la Cour des comptes a interrogé la CNIEG dans le cadre d'une enquête sur les droits familiaux de retraite.

La Cour des comptes a également ouvert une enquête flash portant sur le rapprochement automatisé avec le fichier des comptes bancaires (Ficoba) des identités bancaires utilisées par les organismes de protection sociale. La Cour conforte, dans son relevé d'observations provisoires, la politique de lutte contre la fraude menée par la CNIEG sur ces sujets.

LES COMMISSAIRES AUX COMPTES

Conformément au Code de la sécurité sociale, les comptes de la CNIEG sont certifiés annuellement par un commissaire aux comptes.

Pour l'exercice 2021, les comptes de la CNIEG ont été certifiés « réguliers et sincères » par le cabinet KPMG.

Organisation du Contrôle interne à la CNIEG

Organisation du Contrôle interne à la CNIEG

STRUCTURE DÉDIÉE

Le dispositif de maîtrise des risques est animé par un collectif composé de quatre emplois placés sous l'autorité du DCF et du directeur auxquels il rend compte :

- un emploi de délégué à la gestion des risques en charge de la politique de pilotage par les risques et la valeur ajoutée ;
- trois emplois d'auditeurs en charge de l'audit et du contrôle interne dont **les missions principales sont les suivantes** :
  - l'assistance et/ou le conseil auprès de l'ensemble des acteurs de la démarche de maîtrise des risques ;
  - l'assistance et/ou le conseil auprès de l'ensemble des équipes de travail internes pour l'actualisation du dispositif de contrôle interne en fonction des évolutions législatives, organisationnelles et informatiques ;
  - l'expertise en matière d'organisation du contrôle ;
  - le suivi de l'ensemble des actions relatives au contrôle interne et l'examen des résultats et des actions correctives ;
  - le pilotage de la mise en œuvre et du suivi du plan de contrôle interne, en particulier, dans le domaine de la supervision et de l'analyse des risques ;
  - l'examen des plans de contrôle des différentes équipes de travail afin de garantir leur cohérence et leur complémentarité ;
  - la présentation de propositions destinées à la gouvernance de la caisse et concernant les évolutions à apporter au contrôle interne ;
  - la réalisation des contrôles sur stock ;
  - la validation des évolutions des applications informatiques ayant une incidence financière.

LE COMITÉ DES RISQUES

Mise en place en 2020, cette instance animée par la déléguée à la gestion des risques a pour objectif d'effectuer une revue trimestrielle de l'ensemble des risques en fonction des évènements de la période. Cette instance permet de mettre en place les actions de maîtrise nécessaires à la couverture des nouveaux scénarios de risque. Elle se déroule avant les comités d'audit de mars, juin, septembre et décembre.

Cette instance permet d'alimenter le cinquième comité d'audit du conseil d'administration, programmé en octobre, dédié à la revue des risques stratégiques et au cours duquel est réalisé un zoom sur la sécurité SI et un point d'avancement du plan d'action de prévention des risques.

LA DIRECTION

Depuis 2020, le comité de direction a été remplacé par :

- une équipe de quart chargée d'appuyer le directeur et d'assurer la continuité de service de la direction ;
- un comité stratégique chargé d'assurer une revue stratégique régulière et d'effectuer le suivi de la mise en œuvre de la COG.

La direction examine annuellement la cartographie des risques, et notamment les risques stratégiques dont elle assure un suivi spécifique. Elle fixe les priorités d'actions et les moyens affectés au dispositif de contrôle interne et valide les mesures susceptibles d'améliorer le dispositif.

LE COMITÉ D'AUDIT

Le comité d'audit est l'organe du conseil d'administration qui a pour objet de préparer les travaux du CA relatifs, notamment, aux sujets d'ordre financier.

Il donne son avis sur :

- les budgets ;
- les prévisions de trésorerie ;
- la situation financière, la sécurité financière et les comptes de la caisse ;
- les rapports à caractère économique et financier établis par la caisse ;
- le suivi financier de l'adossement avec les régimes de droit commun ;
- les travaux des Commissaires aux comptes ;
- le contrôle interne et les risques.

Sur ce dernier point, le comité d'audit :

- s'assure de l'existence d'une procédure d'identification et de suivi des risques ;
- examine et valide la cartographie des risques et les plans d'actions ;
- examine les incidences potentielles des risques significatifs, notamment les risques majeurs ;
- s'assure de l'existence de procédures de conformité aux obligations légales et réglementaires ;
- donne son avis sur le rapport de contrôle interne.

En 2021, les 5 séances tenues ont abordé des sujets relatifs au contrôle interne et/ou à la maitrise des risques.

PLAN DE CONTRÔLE INTERNE (PCI)

En fonction de l'évaluation des niveaux de risques potentiels déterminés par les services, en collaboration avec le collectif maîtrise des risques et en s'appuyant éventuellement sur les expertises externes, la CNIEG prépare chaque année un plan de contrôle interne. Ce plan porte sur les contrôles des dossiers mouvementés sur l'exercice (appelés flux), mais aussi sur l'examen de certains dossiers non mouvementés dans l'année ou nécessitant une surveillance particulière (appelés stock).

Le plan de contrôle interne précise :

- les actions de contrôle prévues, avec leurs modalités, à exécuter par les services ;
- les actions de supervision et de vérification, avec leurs modalités, exécutées par le pôle maîtrise des risques ;
- la qualité et l'identité des responsables de chaque action de contrôle.

Après consultation du comité d'audit, le plan est proposé au directeur et au DCF qui le rendent exécutoire en le contresignant.

Indépendamment des contrôles de premier et de deuxième niveau, le pôle maîtrise des risques s'assure également de la mise en œuvre et du suivi des actions correctives et/ou préventives (boucle de régulation).

MÉTHODOLOGIE DE CONTRÔLE

Le système est fondé sur deux niveaux de contrôle.

Un premier niveau correspond aux contrôles effectués par les services sur leurs activités propres.

Un second niveau concerne la supervision des contrôles de premier niveau. Cette supervision est réalisée par les équipes du pôle maîtrise des risques.

Le second niveau n'a pas pour vocation de rechercher des dossiers en anomalie. Son objectif est de s'assurer de la réalisation des contrôles de premier niveau et de donner une assurance raisonnable quant à leur fiabilité.

Afin de ne pas avoir à contrôler de façon exhaustive l'ensemble des dossiers lors des contrôles de premier niveau, le principe retenu est de s'appuyer sur une démarche statistique d'échantillonnage, construite sur la base des préconisations de PricewaterhouseCoopers (PwC - cf. infra).

MÉTHODE D'ÉCHANTILLONNAGE

Le cabinet PWC a préconisé, dans son rapport commandé par la CNIEG en 2007, quatre méthodes d'échantillonnage possibles : méthode exhaustive, méthode d'échantillonnage non statistique, méthode d'échantillonnage statistique, méthode de test des contrôles.

Deux méthodes adaptées à la CNIEG ont été retenues depuis 2008 pour les contrôles sur populations :

- la méthode exhaustive ;
- la méthode d'échantillonnage statistique « SAS » : sondage aléatoire simple (loi normale). Cette méthode est utilisée avec les paramètres suivants : niveau de confiance = 95 %, erreur tolérable = 5 %.

La CNIEG utilise aussi la méthode d'échantillonnage non statistique pour certains cas particuliers de contrôle.

La méthode de sondage aléatoire simple est fondée sur les principes suivants :

- elle détermine la taille de l'échantillon à contrôler pour que celui-ci soit représentatif de la population totale ;
- elle utilise la loi normale en tenant compte d'un niveau de confiance de 95 %.

Tout résultat d'un sondage fait l'objet d'une marge d'erreur. Ainsi, un intervalle de confiance à 95 % donnera un encadrement correct de la valeur dans 95 % des cas.

Par ailleurs, le taux d'anomalie mis en évidence par les contrôles doit, pour être juste, tenir compte d'un intervalle de confiance correspondant à la valeur du quantile 2,5 % de la loi normale.

Dans le cas du contrôle interne de la CNIEG, tout résultat de contrôle devrait donc s'exprimer sous la forme suivante :

- Taux d'anomalie estimé sur l'ensemble de la population = valeur issue des contrôles + ou – l'intervalle de confiance.

Pour des raisons de facilité de lecture, seule la valeur issue des contrôles est le plus souvent affichée.

Exemple : le taux d'anomalie avec incidence financière constaté sur l'échantillon représentatif des liquidations vieillesse (attribution et révision de droits) pour 2021 est de 1,05 %.

L'application de la méthode permet de déduire que :

1. la probabilité que l'échantillon soit représentatif de l'ensemble de la population est de 95 % ;
2. le taux d'anomalie ramené à l'ensemble des liquidations est compris entre 0,52 % et 1,58 %.

Le nombre de liquidations et révisions vieillesse étant de 7 712, on peut affirmer avec 95 % de confiance, que le nombre de dossiers comportant une erreur à incidence financière est compris entre 40 et 122.

COMPLÉMENTS DE CONTRÔLE DU FLUX

À l'examen des résultats de contrôle d'un échantillon représentatif, des compléments de contrôle peuvent s'avérer nécessaires et sont déterminés selon des modalités préalablement définies dans un mode opératoire.

Ils permettent de mettre en œuvre des actions correctives adaptées, en fonction de la typologie des anomalies et des résultats de l'échantillon représentatif (garant de l'évaluation du risque).

CONTRÔLES SUR STOCK

Pour être exhaustif, le PCI doit s'assurer que les dossiers en stock (non mouvementés en gestion au cours de l'exercice) ne comportent pas d'anomalie.

Ce contrôle est réalisé par le pôle maîtrise des risques, par interrogation des bases de données.

Lorsqu'un dossier présente un écart par rapport à un résultat attendu, il est systématiquement vérifié.

Le programme de contrôle sur stock peut être amendé en tant que de besoin en cours d'année. Ce programme participe notamment au dispositif de détection des fraudes et des risques majeurs liés au traitement automatique des informations.

PLAN DE CONTRÔLE DU DCF

Conformément à l'article D. 122-8 du CSS, le DCF de la CNIEG établit un plan de contrôle, inséré dans le dispositif de contrôle interne et basé sur la cartographie des risques.

Les actions de contrôle prévues dans ce plan, à fréquence trimestrielle ou mensuelle, portent sur :

- la qualification des dépenses et des recettes ;
- l'exhaustivité et les délais d'enregistrement des opérations dans les comptes ;
- l'appréciation des risques, charges potentielles et provisions ;
- la séparation des périodes et exercices ;
- la réalisation des inventaires ;
- la gestion et la protection du patrimoine ;
- la justification des comptes ;
- le suivi de la production comptable ;
- la tenue de la documentation obligatoire.

Les résultats du plan de contrôle du DCF sont présentés dans le chapitre "Contrôle du système d'information" de ce document.

Pilotage par les risques

Pilotage par les risques

Le dispositif de contrôle interne a pour vocation de couvrir les risques, notamment financiers, encourus par la caisse. Celle-ci conduit une démarche de maîtrise transverse qui cartographie les risques, évalue leur criticité et définit les actions à mettre en œuvre pour les ramener à un niveau acceptable. Ces risques sont revus, a minima, tous les ans avec leurs pilotes.

Cette action majeure s'exerce dans le cadre réglementaire et normatif défini par :

- le Code de la sécurité sociale qui impose aux organismes de sécurité sociale de « concevoir et mettre en place un dispositif de contrôle interne lui permettant de maîtriser les risques [...] » (Article D. 114-4-6 du CSS) ;
- la norme ISO 9001 – V2008 : la CNIEG ayant été certifiée pendant plus de 10 ans, continue à s'inspirer de cette norme ;
- le modèle EFQM 2013 : la CNIEG a fait le choix de s'inscrire dans cette démarche d'excellence dont elle a obtenu le prix national en 2018.

DÉFINITION DU RISQUE

L'Autorité des marchés financiers (AMF) donne une définition du risque dans « cadre de référence des dispositifs de gestion des risques et de contrôle interne – version 2010 ». Sur cette base et compte-tenu des spécificités de la CNIEG (missions définies par la loi du 9 août 2004), la Caisse a retenu la définition adaptée suivante :

« Le risque représente la possibilité qu'un évènement survienne et dont les conséquences pourraient avoir une influence négative sur les personnes, les actifs, l'environnement, les objectifs de la CNIEG, la réalisation de ses missions définies par la loi, sa réputation. »

MÉTHODOLOGIE DE GESTION ET DE MAÎTRISE DES RISQUES

En 2017, la CNIEG a décidé de créer une mission de « chargée de la mise en œuvre de la stratégie transverse de maîtrise des risques » confiée à la responsable du Pôle Maîtrise des Risques. Cette mission a été transformée en poste de « Déléguée à la Gestion des risques » en 2021 sous la responsabilité conjointe du directeur et du DCF de la CNIEG.

Son rôle est de développer la méthode spécifique basée sur l'analyse des risques et des moyens de maîtrise de tout évènement ou incident ayant un impact sur tout ou partie des activités de la CNIEG avec le souci de garantir la qualité de services auprès des affiliés, des pensionnés et des partenaires de la Caisse.

La CNIEG assure la couverture de l'ensemble des risques identifiés en formalisant et en mettant en œuvre pour chaque risque :

- des actions spécifiques de couverture ;
- des contrôles PCI ;
- des « bonnes pratiques ».

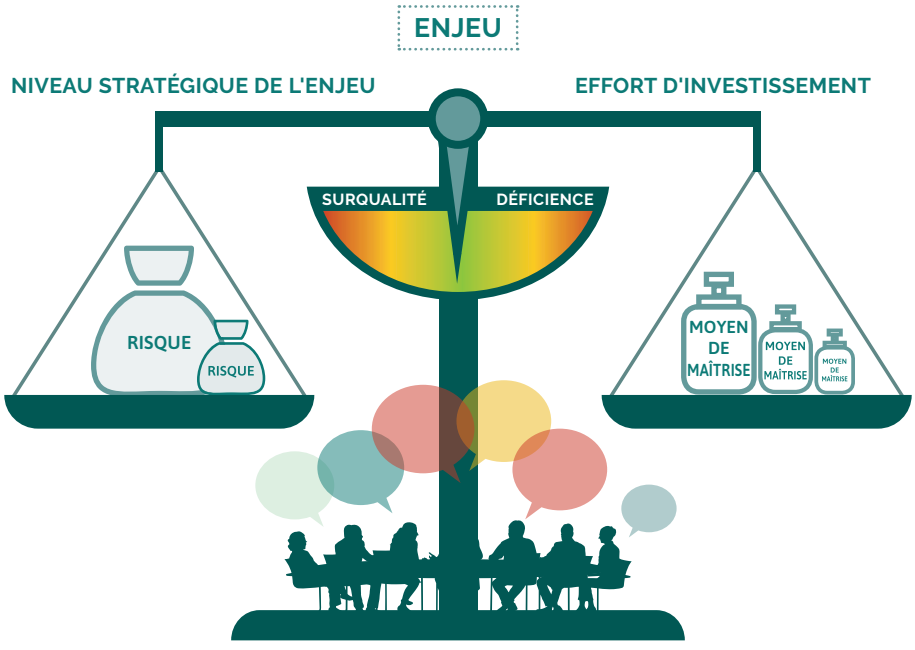
L'outil informatique de maîtrise des risques (GEDYS) permet d'enregistrer l'ensemble des risques identifiés et leurs caractéristiques ainsi que les contrôles, bonnes pratiques et actions de couverture associés.

Depuis 2020, GEDYS gère les évolutions inscrites dans l'optimisation du processus de maîtrise des risques : cotation brute, création et gestion d'enjeux, liens entre risques et enjeux, liens entre risques. Cet outil évoluera en même temps que la méthode.

L'objectif est d'optimiser les moyens de maîtrise pour garantir l'assurance raisonnable de couverture des risques.

ELLE OFFRE AUX PORTEURS D'ENJEUX DES ÉLÉMENTS PERMETTANT D'EFFECTUER DES ARBITRAGES :

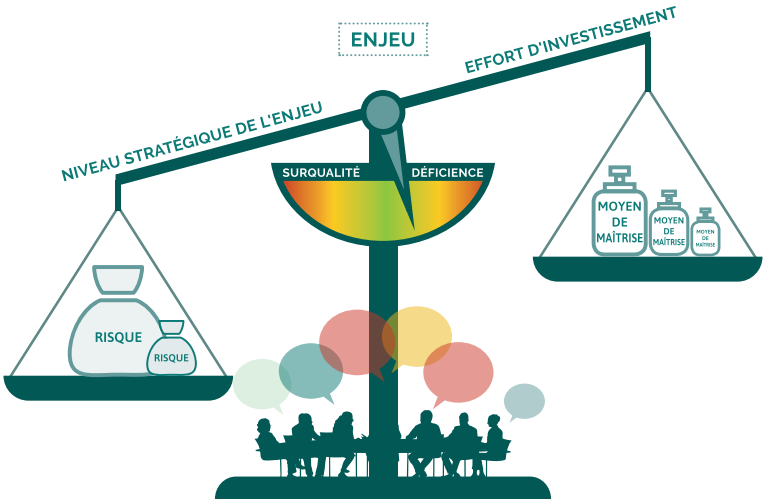
1. Équilibre entre risques et moyens de maîtrise



Les actions de maîtrise sont nécessaires et suffisantes pour couvrir les risques.
Les risques sont maîtrisés, l'enjeu est stabilisé.

Un gain en capacité à faire est possible pour sécuriser un autre enjeu ou la réalisation du plan de marche de la CNIEG. La décision de réduire les moyens de maîtrise (cf. point suivant) doit être prise par le porteur d'enjeu après avoir consulté ses pairs.

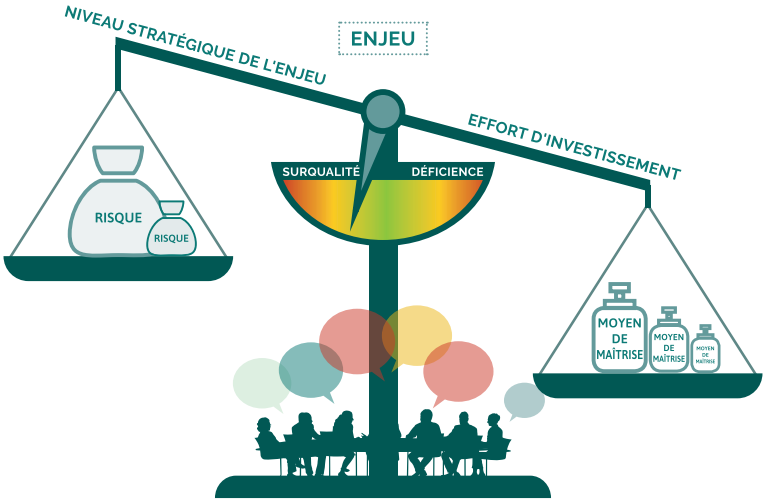
2. Déficience dans la couverture des risques



Il manque des actions de maîtrise pour couvrir les risques et sécuriser l'enjeu.
Deux choix sont possibles :

- accepter la situation car le niveau de maîtrise des risques est jugé acceptable (cotation résiduelle comprise entre 5 et 10) ;
- mettre en place des moyens supplémentaires car le niveau de maîtrise des risques est jugé insuffisant (cotation résiduelle supérieure à 10).

3. Surqualité



Les moyens de maîtrise mis en œuvre sont trop importants (surcoût) par rapport à la criticité des risques. Il faut supprimer les moyens de maîtrise à faible valeur ajoutée.

MODALITÉS D'ANALYSE DES RISQUES

Chaque risque est réévalué à chaque nouvel évènement (réglementation nouvelle, déficience des compétences, incident, …) impactant. Le pilote réévalue si nécessaire :

- la pertinence ;
- le périmètre ;
- la criticité brute ;
- les actions de couverture ;
- la criticité résiduelle.

La CNIEG a défini des critères communs utilisés pour calculer la criticité d'un risque (criticité = probabilité X gravité).

1 - PROBABILITÉ

Survenance de l'évènement redouté	Critères
1 - Extrêmement rare	Risque très improbable
2 - Rare	L'évènement redouté peut se produire mais c'est peu vraisemblable
3 - Possible	Il existe une chance réelle que l'évènement redouté se produise
4 - Fréquent	Il est fort probable que l'évènement redouté se produise

Ces critères sont valables quel que soit l'enjeu.

2 - GRAVITÉ

	Assurer les missions de la Caisse	Préserver l'image et la réputation de la Caisse	Garantir la Sécurité et la qualité de vie au travail	Maitriser le financement du Régime et la performance économique de la Caisse
1 - Mineure	**Organisation :** Nécessité d'adaptation négligeable du mode de fonctionnement habituel **Planning :** Décalage (hors chemin critique du PDM de la Caisse) **RGPD :** anomalie mineure sur traitement de données personnelles non sensibles **Périmètre :** Abandon d'une fonctionnalité mineure	Plaintes ou doléances limitées d'utilisateurs ou de partenaires : - de 5 réclamations par mois sur le sujet étudié Sanction interne	Inconfort minime des collaborateurs ou des personnes extérieures à la Caisse Alerte sans arrêt de travail	Impact financier (*) < ou = 50 euros (Mise en débet DCF) < ou = 5 000 euros (GA) < ou 100 000 euros (GT) Mobilisation de moyens supplémentaires < 10j.h
2 - Notable	**Organisation :** Perturbation importante d'une mission non critique **Planning :** Décalage (chemin critique) nécessitant un ajustement du PDM de la Caisse **RGPD :** diffusion de données non sensibles à un autre client **Périmètre :** Abandon d'une fonctionnalité (visible interne ou externe),	Plaintes importantes d'utilisateurs ou partenaires : entre 5 et 10 réclamations par mois sur le sujet étudié Détérioration de l'image de la caisse auprès de la gouvernance (CA, Tutelles) Mentions limitées dans la presse Condamnation civile d'un agent Mention de la caisse dans une affaire civile ou pénale	Inconfort des collaborateurs ou des personnes extérieures à la Caisse Manque d'implication et/ou démotivation Blessure légère de collaborateurs ou de personnes extérieures à la Caisse Arrêt de travail de courte durée < 1 semaine	Impact financier > 50 et < ou = 500 euros (Mise en débet DCF) > 5 000 et < ou = 50 000 euros (GA) > 100 000 et < ou = < 1 000 000 euros (GT) Mobilisation de moyens supplémentaires >10j.h et <100j.h
3 - Critique	**Organisation :** Perturbation importante d'une mission critique **Planning :** Décalage entrainant un impact important sur le PDM de la Caisse *(ex : descopage de certains sujets, décalage de jalons...)* **RGPD :** diffusion, perte, vol de données non sensibles **Périmètre :** Abandon d'une fonctionnalité importante, dégradant le niveau de service **Nombre d'appels téléphoniques :** > 500 par jour	Campagnes dans des médias locaux Mouvements de protestation limités entre 10 et 15 réclamations par mois sur le sujet étudié Perte limitée de pouvoir de négociation vis-à-vis de la gouvernance (CA, Tutelles) Condamnation prononcée à l'encontre de la Caisse Démission d'une haute autorité de la Caisse	Malaise important des collaborateurs ou des personnes extérieures à la Caisse Désengagement, départ de compétences clés Manque de salariés en capacité de produire. Blessure lourde de collaborateurs ou de personnes extérieures à la Caisse Arrêt de travail > 1 semaine	Impact financier > 500 et < ou = 5 000 euros (Mise en débet DCF) > 50 000 et < ou = 500 000 euros (GA) > 1 000 000 et < ou = < 10 000 000 euros (GT) Mobilisation de moyens supplémentaires >100j.h et <1000j.h
5 - Majeure	**Organisation :** ARRÊT ou Perturbation importante des missions critiques **RGPD :** diffusion, perte, vol de données sensibles (données médicales...) **Planning :** Décalage entrainant un non-respect des obligations réglementaires et contractuelles (ex: COG) **Périmètre :** Non tenue des objectifs initiaux	Campagnes dans des médias nationaux Mouvements de protestation importants + de 15 réclamations par mois sur le sujet étudié Perte importante de pouvoir de négociation vis-à-vis de la gouvernance (CA, Tutelles) Condamnation pénale d'un dirigeant	Malveillance de la part d'un ou de plusieurs salariés Arrêt de travail avec IPP Décès	Impact financier > 5 000 euros (Mise en débet DCF) > 500 000 euros (GA) > 10 000 000 euros (GT) Mobilisation de moyens supplémentaires >1000j.h

(*) Mise en débet : responsabilité financière du Directeur Comptable et Financier.
GA : Gestion Administrative : Budget Fonctionnement de la caisse (charges d'investissement et charges d'exploitation).
GT : Gestion Technique : Flux financiers liés au Régime.

***Important :** si le risque impacte une population sensible, passer la gravité au niveau supérieur (décision des risques du 5 mars 2020).*

Pilotage par les risques

Pour chaque risque étudié, il faut évaluer la gravité pour chaque enjeu.
La gravité retenue pour la cotation du risque est la gravité la plus haute parmi les 4 enjeux.

La grille suivante est utilisée pour définir la criticité :

Criticité d'un risque = Probabilité X Gravité

Grille de cotation des risques en vigueur à la CNIEG (AP-CONT-01)

Gravité	1 - Extrêmement rare	2 - Rare	3 - Possible	4 - Fréquent
5 - Majeure	5	10	15	20
3 - Critique	3	6	9	12
2 - Notable	2	4	6	8
1 - Mineure	1	2	3	4

Probabilité

MAÎTRISE

Criticité de 1 à 4 :
pas d'action de maîtrise.

ACCEPTABLE

Criticité > 4 et < 12 :
l'opportunité de mesures de couverture doit être envisagée.

INSUFFISANT

Criticité > ou = 12 :
des mesures de couverture doivent **obligatoirement** être mises en œuvre.

À noter : la gravité majeure est majorée (5 au lieu de 4) afin de mieux prendre en compte le résultat du produit : probabilité extrêmement rare x gravité Majeure. En utilisant la valeur 4, ce produit donnerait une criticité à 4 qui est considérée comme ne nécessitant pas d'action de maîtrise.

Pour mieux évaluer visuellement les effets des moyens de maîtrise sur le risque, les cotations brutes et résiduelles sont rappelées dans la représentation suivante (exemple réel) :

Gravité	1 - Extrêmement rare	2 - Rare	3 - Possible	4 - Fréquent
5 - Majeure	5	10	15 (Risque brut)	20
3 - Critique	3	6	9 (Risque résiduel)	12
2 - Notable	2	4	6	8
1 - Mineure	1	2	3	4

Probabilité

Dans cet exemple, le niveau de maîtrise est jugé acceptable, des moyens de maîtrise supplémentaires peuvent être envisagés.

MODALITÉS DE SUIVI DES RISQUES

Le comité des risques réunit les pilotes tous les trimestres afin de partager toute information pouvant amener à une réévaluation de la criticité des risques et, par voie de conséquences, à un ajustement des moyens de maîtrise assurant la couverture des risques.

L'ensemble des analyses de risques effectuées constitue un entrant pour les travaux annuels (octobre/novembre) d'élaboration de la cartographie et du plan de contrôle interne de l'année suivante.

Les risques stratégiques sont suivis plus spécifiquement lors d'une revue annuelle : ils sont surveillés, analysés et si nécessaire redéfinis au regard des différents éléments variables impactant la CNIEG (contexte économique, évolutions technologiques, évolutions réglementaires, modifications organisationnelles…).

Le comité d'audit examine et émet un avis chaque année sur la cartographie des risques. Une séance est spécifiquement dédiée à l'examen des risques stratégiques.

CARTOGRAPHIE DES RISQUES

La cartographie des risques est établie à partir de chaque activité des processus en vigueur à la CNIEG.

En 2019, quatre enjeux ont été définis pour la caisse :

- assurer les missions de la caisse ;
- préserver l'image et la réputation de la caisse ;
- garantir la sécurité et la qualité de vie au travail (QVT) ;
- maitriser le financement du régime et la performance économique de la caisse.

Chaque risque est suivi par un pilote ou deux pilotes en fonction du périmètre de l'activité couverte.

On distingue 2 types de risques :

- **les risques opérationnels :** risques résultant d'une inadaptation ou d'une défaillance imputable à des procédures, personnels et systèmes internes ou évènements extérieurs ;
- **les risques stratégiques :** risques portant sur les objectifs stratégiques de la caisse. Ils sont pilotés spécifiquement par le COSTRAT et les porteurs d'enjeu.

En 2021, la cartographie des risques recense 40 risques dont 9 considérés comme risques stratégiques :

- défaillance dans le financement du Régime ;
- défaillance grave d'un service et/ou d'un processus client ;
- incapacité de la CNIEG à mettre en œuvre une évolution réglementaire ;
- fraude interne ou externe ;
- déficience de compétences clés ;
- sécurité du SI non adaptée aux services déployés et aux données gérées ;
- gouvernance défaillante d'un projet (y compris SI) ;
- catastrophe naturelle ou accident majeur ;
- défaillance grave dans l'accompagnement au changement.

La cartographie des risques 2021 a fait l'objet d'un avis du comité d'audit du 6 décembre 2020. Elle est la base de l'élaboration du plan de contrôle interne (PCI) 2021.

Les Faits Marquants de 2021

SYNTHÈSE DES RÉSULTATS PCI 2021

Ce chapitre présente une synthèse des principaux résultats liés à la maîtrise des risques et des coûts de gestion administrative.

INDICATEURS DE PERFORMANCE ET DE SUIVI DU CONTRÔLE INTERNE

Dans le cadre de la nouvelle COG (2020-2024), de nouveaux indicateurs ont été mis en place dans un souci d'harmonisation avec les autres organismes de sécurité sociale.

Les indicateurs de la nouvelle COG sont en ligne avec les objectifs fixés sauf l'indicateur sur la fraude avec un résultat à 82 pour un objectif fixé à 87 pour 2021. Ce résultat est lié à la non-réalisation de certaines actions prévues en raison de la crise sanitaire.

Le pôle maîtrise des risques a souhaité garder l'indicateur de performance utilisé pour les COG précédentes comme indicateur de suivi de l'activité. Cela permet de voir l'évolution de l'activité par rapport aux années précédentes. Cet indicateur pourrait disparaître lorsque les nouveaux indicateurs auront un historique suffisant.

Pour 2021, l'indicateur de suivi du contrôle interne est en baisse avec un résultat de 84 (sur 100) pour un résultat de 90 en 2020. Celui-ci reste toutefois à un niveau de performance élevé et plus conforme aux années antérieures à 2020.

INCIDENCE FINANCIÈRE

Le montant de l'incidence financière est en baisse par rapport à 2020 (1 178 445 € contre 1 727 652 € en 2020).

Les résultats des contrôles de second niveau (supervision) présentent un taux d'anomalie de 0,21 % contre 0,08 % en 2020, soit 2 anomalies détectées sans incidence financière (1 anomalie sans incidence financière en 2020).

Les résultats des contrôles de niveau 1 réalisés par les services présentent un taux d'anomalie de 1,19 % contre 1,35 % en 2020. 162 anomalies ont été détectées par le niveau 1 pour un montant total de l'incidence financière de 946 361 € (contre 848 776 € en 2020).

Le reste des anomalies a été détecté par des contrôles hors PCI et par les contrôles sur stock.

Le nouvel indicateur COG sur l'efficacité de détection des anomalies par le contrôle interne permet de confirmer la qualité de ce dispositif avec un résultat de 81 conforme à l'objectif fixé pour l'année 2021.

CHARGE FINANCIÈRE

Le montant de la charge financière est en hausse à 31 047 € (contre 1 681 € en 2020). Cette somme est composée en partie par des remises de dettes accordées par la Commission de Recours Amiable (suite à des erreurs de gestion) et par des remises amiables accordées par le Directeur Comptable et Financier.

RISQUE FINANCIER

On note une baisse du risque financier (839 956 € contre 1 211 522 € en 2020). Pour rappel, le risque financier est l'extrapolation du montant total de l'incidence financière détectée en défaveur de la caisse.

RÉSULTATS LIÉS À LA MAÎTRISE DES COÛTS DE GESTION ADMINISTRATIVE

Les autorisations budgétaires, telles que validées par le Conseil d'Administration du 15 décembre 2020 ont été respectées.

Le ratio « frais de gestion », qui consiste à mesurer la maîtrise de la trajectoire budgétaire de la CNIEG et sa pertinence, est conforme à l'objectif visé dans la COG : il s'élève à 69,4 pour un objectif maximum fixé à 79,1.

TRANSFERT D'ACTIVITÉS MÉTIERS

L'année 2021 a été marquée par les projets de transfert des activités de gestion des prestations Accidents du Travail & Maladies professionnelles (AT/MP) vers la MSA Auvergne et de transfert du recouvrement social vers le régime général (UCn) et le régime agricole (pour les seules SICAE).

Ces transferts seront effectifs en 2022 avec un impact sur le contrôle et l'audit interne.

PRIORITÉS 2021

Les axes de contrôles prioritaires et les objectifs de maîtrise des risques pour 2021 ont été portés dans l'avenant N° 18 au protocole d'accord du contrôle interne après l'avis du comité d'audit du 6 décembre 2020.

Les axes prioritaires concernent :

- la garantie des opérations de gestion concourant à la liquidation des prestations et à la révision des droits ;
- la sécurisation des équilibres financiers du régime ;
- la régularité des informations financières publiées ;
- la lutte contre la fraude ;
- la sécurité du système d'information (accès au bâtiment, procédure incendie, habilitations, traitements, redressements, incidents…).

Après analyse des résultats du plan de contrôle 2020 et révision de la cartographie des risques de la CNIEG en prenant compte des évolutions contextuelles (légales et réglementaires, technologiques, organisationnelles, liées à l'émergence de nouveaux projets…), **le plan de contrôle interne intègre, en 2021 :**

- **122 actions de contrôle sur flux** (dont 39 relevant du PCDCF) qui couvrent l'ensemble des activités de la caisse. Les principales évolutions par rapport au périmètre du PCI 2020 sont :
  - La création de 2 nouvelles actions de contrôle :
    - > contrôle des Relevés d'Identité Bancaire (RIB) papier ;
    - > contrôle de l'attribution des CESU normaux et DOMISERVE.
  - La modification de 7 actions de contrôle (fréquence, mode opératoire, périmètre, responsabilité du contrôle) :
    - > montants forcés ;
    - > redressements manuels des écarts FICOBA ;
    - > revalorisation des montants forcés ;
    - > présence des pièces justificatives des flux financiers RDC ;
    - > contrôle des délégations de pouvoirs du Directeur Comptable et Financier ;
    - > vérifier la lisibilité des bandes légales et test de remontée sur les sauvegardes ;
    - > incidents informatiques.
  - La suppression de 2 actions de contrôle (obsolescence, fusion, transformation en activités, transformation en contrôles sur stock ou audit) :
    - > plan de reprise d'activité
    - > saisie et validation des absences.

5 actions de contrôle sur stock. Les principales évolutions par rapport au périmètre du PCI 2020 sont :

- La suppression de 2 contrôles :
  - > cotisation CAMIEG : le risque est couvert par une évolution de la démarche de demande de retraite ;
  - > cohérence entre les devis de rachats d'études et les montants saisis : le contrôle est réalisé une fois en 2020 pour traiter le stock, le risque sur le flux est couvert par le contrôle C017.
- La modification d'1 contrôle :
  - > SSF : le contrôle de non-cumul SSF/Allocation Logement est étendu à la population des agents de la CNIEG.

Dans le cadre des évolutions de ses activités, le Pôle Maîtrise des Risques a inscrit 3 audits internes dans son plan de contrôle interne 2021 :

- audit sur la sécurisation des modes de paiement ;
- audit sur le plan de reprise d'activités ;
- audit sur le suivi des réserves liées aux mises en production informatique.

La crise sanitaire qui s'est poursuivie en 2021 n'a pas permis de réaliser ces 3 audits. Seul l'audit sur la sécurisation des modes de paiements a été réalisé.

LES INDICATEURS DE SUIVI DU CONTRÔLE INTERNE

Dans le cadre de la COG 2020-2024, la CNIEG a défini 2 nouveaux indicateurs de suivi :

L'efficacité de la détection des anomalies par le dispositif de contrôle interne est mesurée au travers d'un indicateur composite pondéré permettant d'évaluer :

- la qualité de l'échantillon (pond. 2) ;
- la qualité de la couverture des risques (pond. 3) ;
- la qualité du contrôle (pond. 5).

La qualité des résultats du dispositif de contrôle interne est mesurée au travers d'un indicateur composite pondéré permettant d'évaluer :

- le taux de réalisation du plan de contrôle (pond. 2) ;
- le taux d'incidences financières des erreurs (régime - TIF) (pond. 1) ;
- le taux de détection avant paiement (régime) (pond. 2) ;
- le taux de recouvrement des indus fautifs (pond. 3) ;
- le montant total de la charge financière (pond. 2).

En outre, 3 indicateurs de benchmark DSS sont définis sur la branche "Régime" :

- le taux de qualité des dossiers après paiement (IQV) :
  Nombre de contrôles réalisés a posteriori et sans anomalie / Nombre total de contrôles réalisés a posteriori ;
- le taux de qualité des dossiers avant paiement (IQL) :
  Nombre de contrôles réalisés a priori et sans anomalie / Nombre total de contrôles réalisés a priori ;
- le taux d'incidences financières des erreurs (TIF) :
  Montant des erreurs financières de l'échantillon en valeur absolue / Montant total de l'échantillon.

Un indicateur spécifique de lutte contre la fraude est également défini. Il s'agit un indicateur composite pondéré permettant d'évaluer :

- le taux de couverture de la population ciblée dans le plan annuel de lutte contre la fraude (pond. 5) ;
- le taux de recouvrement des indus frauduleux (pond. 2) ;
- le taux de réalisation du plan d'action annuel contre la fraude interne (pond. 3).

OPTIMISATION DES ENJEUX

En 2021, un travail d'optimisation a été effectué entre les 4 enjeux définis pour la gestion des risques et les 5 enjeux stratégiques définis par le comité stratégique en 2020 :

- Services et relations clients ;
- Performance du SI ;
- La CNIEG et son environnement ;
- Organisation et richesse humaine de la Caisse ;
- Performance financière.

Les critères de gravités ont été définis pour chaque enjeu :

	Services et relations clients	Performance du SI	La CNIEG et son environnement	Organisation et richesse humaine de la Caisse	Performance financière
1 - Mineure	**Campagne de communication et/ou accompagnement (Population inférieure ou égale à 1 000)** Erreur sans impact sur le droit Retard de com sans impact sur le droit Cible erronée **Traitement des dossiers et services en ligne :** Erreur avec impact sur le droit ou le paiement sur population minime (< 50 personnes) Retard (- d'un mois TJ) **Déficit de la qualité et de la satisfaction client sur les offres de services Clients :** <5 % par rapport de l'indicateur de référence	**Niveaux de service :** disponibilité du Portail, SI métiers, SI support, SI Partenaires : Indisponibilité inférieure à 0,5 jour en période sensible ou inférieure à 1 jour hors période sensible **Tenue des engagements (jalons, valeurs métiers) :** Livraison d'un service partiel ou décalé sans impact direct sur nos clients / partenaires ou nos processus internes **RGPD :** anomalie mineure sur traitement de données personnelles non sensibles	**Continuité de service et engagements** Nécessité d'adaptation négligeable du mode de fonctionnement habituel **Planning :** Décalage (hors chemin critique du PDM de la Caisse) **Sanction interne**	**Disponibilité des compétences :** insuffisance avec impact mineur sur la continuité de service et les engagements de la caisse **Charge de travail** Surcroit d'activités mineur (à dire d'expert) **QVT (condition et environnement de travail) :** Désagrément mineur exprimé dans le baromètre social **Motivation et engagement :** Désengagement mineur exprimé dans le baromètre social **Alerte sans arrêt de travail ou blessure légère**	Impact financier (*) < ou = 50 euros (Mise en débet DCF) < ou = 5 000 euros (GA) < ou 100 000 euros (GT) Mobilisation de moyens supplémentaires < 10j.h
2 - Notable	**Campagne de communication et/ou accompagnement (Population comprise entre 1 000 et 5 000)** Erreur sans impact sur le droit ou avec impact pour population moyenne Retard sans impact sur le droit Cible erronée **Traitement des dossiers et services en ligne :** Erreur avec impact sur le droit ou le paiement sur population notable (de 50 à 499 personnes) Retard (1 mois) **Déficit de la qualité et de la satisfaction client sur les offres de services Clients :** de 5 à 10 % par rapport de l'indicateur de référence	**Niveaux de service :** disponibilité du Portail, SI métiers, SI support, SI Partenaires : Indisponibilité de 0,5 à 1 jour en période sensible ou de 1 à 2 jours hors période sensible **Tenue des engagements (jalons, valeurs métiers) :** Livraison d'un service partiel ou décalé sans impact direct sur nos clients / partenaires avec un impact potentiel sur nos processus internes **RGPD :** diffusion de données non sensibles à un autre client	**Continuité de service et engagements** Perturbation importante d'une mission non critique **Planning :** Décalage (chemin critique) nécessitant un ajustement du PDM de la Caisse **Détérioration de l'image de la caisse** auprès de la gouvernance (CA, Tutelles), Mentions limitées dans la presse **Condamnation civile** d'un agent, Mention de la caisse dans une affaire civile ou pénale	**Disponibilité des compétences :** insuffisance avec impact notable sur la continuité de service et les engagements de la caisse. **Charge de travail** Surcroit d'activités notable (à dire d'expert) **QVT (condition et environnement de travail) :** Désagrément notable exprimé dans le baromètre social **Motivation et engagement :** Désengagement notable exprimé dans le baromètre social **Arrêt de travail** de courte durée < 1 semaine **ou blessure**	Impact financier > 50 et < ou = 500 euros (Mise en débet DCF) > 5 000 et < ou = 50 000 euros (GA) > 100 000 et < ou = < 1 000 000 euros (GT) Mobilisation de moyens supplémentaires > 10j.h et < 100j.h
3 - Critique	**Campagne de communication et/ou accompagnement (Population comprise entre 5 000 et 10 000)** Erreur avec impact sur le droit/paiement Retard sans impact sur le droit/paiement Cible erronée **Traitement des dossiers et services en ligne :** Erreur avec impact sur le droit ou le paiement sur population critique (entre 500 et 1 000 personnes) Retard de 2 à 3 mois **Déficit de la qualité et de la satisfaction client sur les offres de services Clients :** de 11 à 15 % par rapport de l'indicateur de référence	**Niveaux de service :** disponibilité du Portail, SI métiers, SI support, SI Partenaires : Indisponibilité de 1 à 2 jours en période sensible ou de 2 à 4 jours hors période sensible **Tenue des engagements (jalons, valeurs métiers) :** Absence d'un nouveau service mais compensé par une mesure de contournement (dégradation des processus internes) **RGPD :** diffusion, perte, vol de données non sensibles **Sécurité :** Niveau de sécurité non conforme au RGS	**Déficit de pilotage interne** **Continuité de service et engagements** Perturbation importante d'une mission critique **Planning :** Décalage entrainant un impact important sur le PDM de la Caisse (ex : descopage de certains sujets, décalage de jalons…) **Perte limitée de pouvoir de négociation** vis-à-vis de la gouvernance (CA, Tutelles), Campagnes dans des médias locaux **Condamnation prononcée à l'encontre de la Caisse ; Démission** d'une haute autorité de la Caisse	**Disponibilité des compétences :** insuffisance avec impact critique sur la continuité de service et les engagements de la caisse. **Charge de travail** Surcroit d'activités critique (à dire d'expert) **QVT (condition et environnement de travail) :** Désagrément critique exprimé dans le baromètre social **Motivation et engagement :** Désengagement critique exprimé dans le baromètre social susceptible d'impacter la continuité de service et les engagements de la caisse. **Arrêt de travail** > 1 semaine ou **blessure lourde**	Impact financier > 500 et < ou = 5 000 euros (Mise en débet DCF) > 50 000 et < ou = 500 000 euros (GA) > 1 000 000 et < ou = < 10 000 000 euros (GT) Mobilisation de moyens supplémentaires > 100j.h et < 1 000j.h
5 - Majeure	**Campagne de communication et/ou accompagnement (Population supérieure 10 000)** Erreur avec impact sur le droit Retard de com sans impact sur le droit Cible erronée **Traitement des dossiers et services en ligne :** Erreur avec impact sur le droit pour plus de 1000 personnes Retard supérieur à 3 mois **Déficit de la qualité et de la satisfaction client sur les offres de services Clients :** >15 % par rapport de l'indicateur de référence	**Niveaux de service :** disponibilité du Portail, SI métiers, SI support, SI Partenaires : Indisponibilité au-delà de 2 jours en période sensible ou au-delà de 4 jours hors période sensible **Tenue des engagements (jalons, valeurs métiers) :** Absence d'un nouveau service sans mesure de contournement (dégradation du service client/partenaire) **RGPD :** diffusion, perte, vol de données sensibles (données médicales…) **Sécurité :** absence de couverture ou introduction d'une faille de sécurité	**Déficit grave de pilotage interne** **Continuité de service et engagements** ARRET ou Perturbation importante des missions critiques **Planning :** Décalage entrainant un non-respect des obligations réglementaires et contractuelles (ex: COG) **Campagnes dans des médias nationaux, réseaux sociaux,** Mouvements de protestation importants **Perte importante** de pouvoir de négociation vis-à-vis de la gouvernance (CA, Tutelles), **Condamnation pénale d'un dirigeant**	**Disponibilité des compétences :** insuffisance avec impact majeure sur la continuité de service et les engagements de la caisse. **Charge de travail** Surcroit d'activités majeur (à dire d'expert) **QVT (condition et environnement de travail) :** Désagrément majeur exprimé dans le baromètre social **Motivation et engagement :** Désengagement majeur exprimé dans le baromètre social et/ou détection de comportement malveillant **Burn-out** **Arrêt de travail avec IPP** **Accident mortel du travail**	Impact financier > 5 000 euros (Mise en débet DCF) > 500 000 euros (GA) > 10 000 000 euros (GT) Mobilisation de moyens supplémentaires > 1000j.h

(*) Mise en débet : responsabilité financière du Directeur Comptable et Financier.
GA : Gestion Administrative : Budget Fonctionnement de la caisse (charges d'investissement et charges d'exploitation).
GT : Gestion Technique : Flux financiers liés au Régime.

***Important :** si le risque impacte une population sensible, passer la gravité au niveau supérieur (décision des risques du 5 mars 2020).*

Dans le cadre de la revue des risques 2021 en vue de la cartographie et du PCI 2022, tous les risques ont été révisés afin d'être cotés sur les 5 enjeux suivis par les porteurs d'enjeu du comité stratégique.

RÉORGANISATION DES ACTIVITÉS

En 2021, le pôle maîtrise des risques a poursuivi sa professionnalisation vers le métier d'auditeur interne, tous les contrôles de niveau 1 du PCI ayant été transférés aux services.

La nouvelle organisation des activités de maîtrise des risques, présentée au Comité Social et Économique de la CNIEG le 15 décembre 2020, est entrée en vigueur le 1er avril 2021.

Résultats détaillés du PCI 2021

Résultats détaillés du PCI 2021

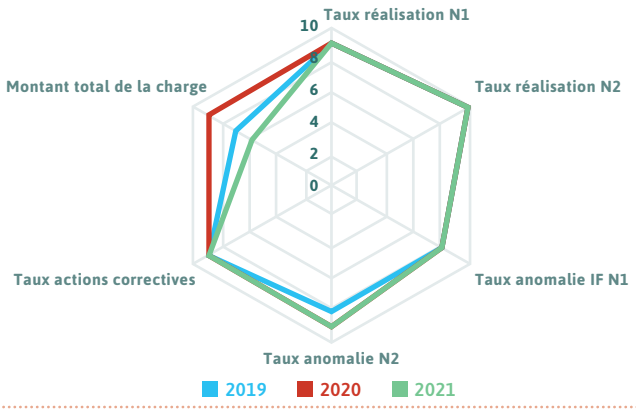
INDICATEURS

INDICATEUR DE SUIVI DU CONTRÔLE INTERNE

Critères (coef.)	2021		2020		2019	
	résultat	points	résultat	points	résultat	points
Taux de réalisation des contrôles de 1er niveau (2)	99,0 %	9	97,2 %	9	98,5 %	9
Taux de réalisation des contrôles de 2nd niveau (1)	100 %	10	100 %	10	100 %	10
Taux d'anomalie avec incidence financière (1)	0,37 %	8	0,63 %	8	0,58 %	8
Taux d'anomalie du contrôle de 2nd niveau (3)	0,21 %	9	0,08 %	9	1,06 %	8
Taux d'action corrective (1)	99,8 %	9	97 %	9	99 %	9
Montant de la charge financière totale (2)	31 047 €	6	1 681 €	9	28 590 €	7
Indicateur de performance	**84**		**90**		**83**	

L'augmentation de la charge financière fait perdre 6 points à l'indicateur de performance. Celui-ci reste toutefois à un niveau élevé et plus conforme aux années antérieures à 2020.

Notation des critères



Critère	Coef	Note										
		0	1	2	3	4	5	6	7	8	9	10
Taux de réalisation des contrôles de 2nd niveau (%)	2	0	30	45	60	75	80	86	88	90	95	100
Taux de réalisation des contrôles de 1er niveau (%)	1	0	30	45	60	75	80	86	88	90	95	100
Taux d'anomalie avec IF (%)	1	> 4	4	3	2	1,3	1	0,71	0,68	0,65	0,32	0
Taux d'anomalie détécté en 2nd niveau (%)	3	> 5	5	4,5	4	3,5	3	2,5	2	1,5	0,75	0
Taux d'action corrective (%)	1	0	10	20	30	40	50	60	70	80	90	100
Montant de la charge financière (k€)	2	> 225	225	180	140	105	75	50	30	15	5	0

INDICATEURS DE PERFORMANCE COG 2020-2024

Suivi des indicateurs annuels de la COG sur le périmètre du contrôle interne :

	Indicateur (1)	Objectif 2021	Résultat	2020
COG 9a	Efficacité de la détection des anomalies par le dispositif de contrôle interne	81	81	84
COG 9b	Qualité des résultats du dispositif de contrôle interne	77	82	81
COG 9c1	Taux de qualité des dossiers après paiement (régime) (IQV)	-	99,2 %	98,6 %
COG 9c2	Taux de qualité des dossiers avant paiement (régime) (IQL)	-	97,8 %	97,5 %
COG 9d	Taux d'incidences financières des erreurs (régime) (TIF)	-	2,3 %	2,06 %
COG 10	Efficacité du dispositif de lutte contre la fraude	87	82 (2)	80

(1) Cf. définition des indicateurs en page 25

(2) Toutes les actions de benchmark et de communication interne n'ont pu être menées à terme

ANALYSE DES RÉSULTATS

LES CONTRÔLES DE NIVEAU 1 (FLUX) ET ZOOM SUR LE RISQUE VIEILLESSE

	2021	2020
nombre actions réalisées	892	871
nombre de contrôles	43 988	44 877
taux de réalisation	99,0 %	97,2 %
nombre d'anomalies détectées	523	605
taux d'anomalie	1,19 %	1,35 %
nombre d'anomalies avec incidence financière	162	283
taux d'anomalies avec incidence financière	0,37 %	0,63 %
intervalle de confiance (borne basse / borne haute) (1)	0,31 % / 0,42 %	0,56 % / 0,70 %
taux d'action corrective	99,4 %	96,7 %
montant de l'incidence financière	946 361 €	848 776 €

(1) niveau de confiance à 95 %

zoom sur le risque vieillesse
(attributions et révisions des droits)

	2021	2020
taux d'anomalie	3,71%	2,71%
taux d'anomalies avec IF	1,05%	0,96%
intervalle de confiance	*0,52% / 1,58%*	*0,52% / 1,39%*
montant de l'IF	6 885 €	10 481 €

Les résultats ci-dessus présentent une synthèse des contrôles de premier niveau. Les résultats des contrôles de second niveau ont permis de valider ces éléments.

Sur le périmètre vieillesse, le taux d'anomalies est en hausse mais le taux d'anomalies à incidence financière reste stable. Le montant quant à lui est en baisse.

TYPOLOGIE DES PRINCIPALES ANOMALIES PCI DE NIVEAU 1 À INCIDENCE FINANCIÈRE

Contrôle	Nb. Ano.	Somme IF	Typologie des principales anomalies
VALIDATION DU TJ	51	275 596 €	Signalétique du bénéficiaire, absence de justificatif
TEM	33	525 548 €	Anomalie informatique, gestion rappel et trop-perçu, cotisations
FACTURES SANS COMMANDE	20	82 007 €	Achat/réception d'une facture sans commande préalable
DEMANDES LIQUIDATION (+15 ANS)	6	3 591 €	Absence de justificatif, erreur de calcul
CAPITAL DÉCÈS PENSIONNÉ	5	21 741 €	Absence de justificatif, erreur de calcul

Le montant de l'incidence financière des anomalies TEM constitue 55 % du montant de l'incidence financière globale détectée en 2021.

La baisse observée en 2020, liée aux différents correctifs apportés sur le système d'information, est confirmée sur cet exercice (665 775 € en 2020).

Les anomalies résiduelles du TEM sont maîtrisées par des requêtes automatiques. Elles n'entraînent pas de charges financières.

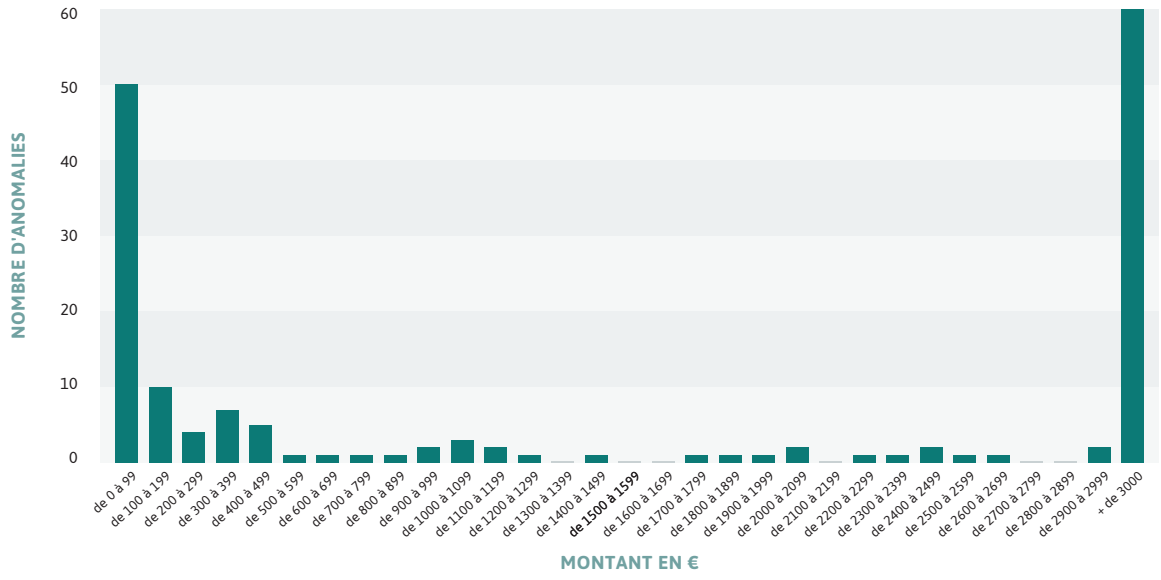
CRITICITÉ DES ANOMALIES PCI DE NIVEAU 1 À INCIDENCE FINANCIÈRE

	Nbre ano	taux ano	Mtt IF	Répart IF	Mtt Charge	Répart Charge	Mtt Risque	Répart Risque
Ano < 24 €	28	0,06 %	223 €	0,02 %	- €	0,00 %	788 €	0,21 %
24 < = Ano < 80	16	0,04 %	899 €	0,09 %	- €	0,00 %	22 947 €	6,07 %
Ano > = 80 €	118	0,27 %	945 240 €	99,88 %	93 €	100,00 %	354 181 €	93,72 %
	162	**0,37 %**	**946 361 €**	**100 %**	**93 €**	**100 %**	**377 916 €**	100 %

Nbre total de contrôles : 43 988

RÉPARTITION DES ANOMALIES PCI DE NIVEAU 1 PAR MONTANT

De nombreuses anomalies détectées via le contrôle des TJ (traitements journaliers) fait augmenter le nombre d'anomalies avec un montant supérieur à 3000 €. Il s'agit pour la plupart d'erreurs de calcul ou de l'absence de justificatif lors de l'attribution de capitaux décès. Toutes ces anomalies sont détectées et régularisées avant paiement.



ZOOM SUR LES COMPLÉMENTS DE CONTRÔLE

Suite à l'analyse des résultats des actions du PCI, des besoins en compléments de contrôle ont été identifiés. Un échantillon de 20 matricules complémentaires a été contrôlé, sans révéler d'anomalie.

Période analysée	Intitulé	Décision suite à l'analyse des résultats		Résultats		
		Proposition	Détail	nb ctrl	nb ano IF	mt IF
1er trimestre et avril	Prestations familiales	Complément de contrôles	Contrôler 20 % des dossiers traités par le gestionnaire à l'origine des écarts	14	0	- €
mai - juin - juillet	Indemnisation AT / MP	Contrôle exhaustif	Contrôler le dernier dossier restant sur la population	1	0	- €
août - septembre - octobre	Indemnisation AT / MP	Contrôle exhaustif	Contrôler les dossiers restant sur la population	1	0	- €
novembre - décembre	Indemnisation ATMP	Contrôle exhaustif	Contrôler les dossiers restant sur la population	1	0	- €
	Indemnisation AT / MP	Contrôle exhaustif	Contrôler les dossiers restant sur la population	3	0	- €

ZOOM SUR LES CONTRÔLES SUR STOCK

4 contrôles sur stock ont été réalisés au titre de l'exercice 2021.

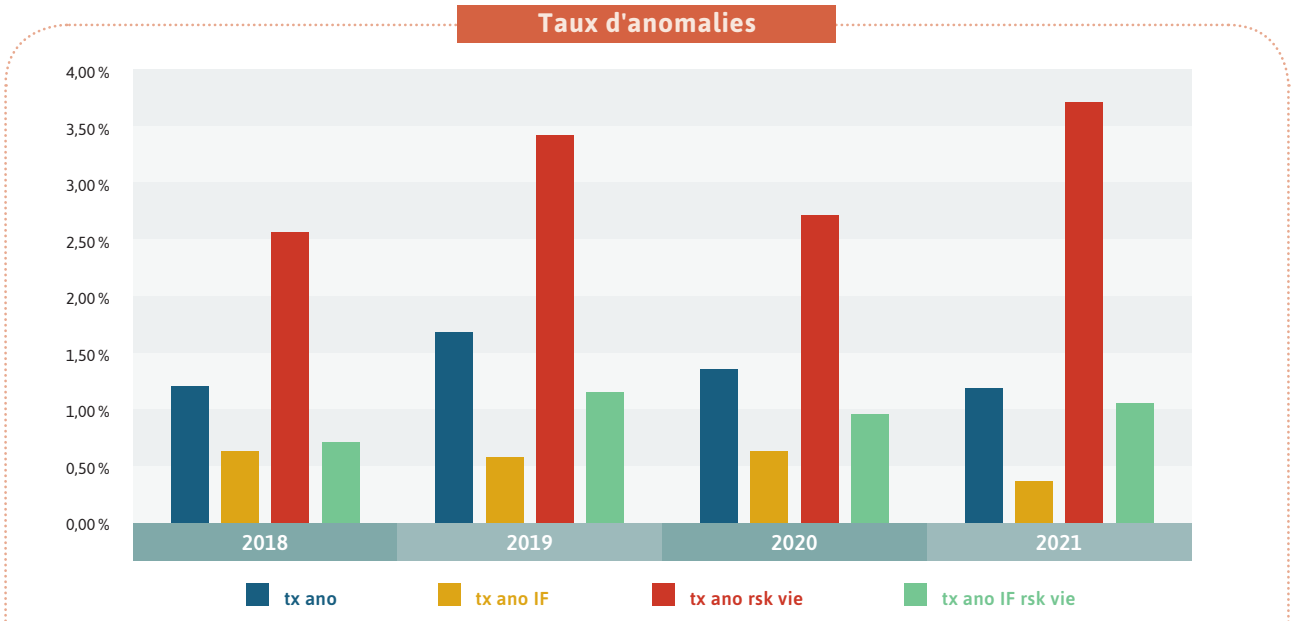
Du fait des nouvelles procédures de validation des modes de paiement à chaque échéance, le contrôle sur les changements de coordonnées bancaires est devenu obsolète.

	Nb contrôles	Résultats		Anomalies		Montant de l'IF
		OK	KO	Sans IF	Avec IF	
SSF	788	777	11	0	11	14 776,75 €
Evolutions annuelles atypiques	20	20	0	0	0	0,0 €
Changement de coordonnées bancaires successives autour d'un traitement de paie	Contrôle annulé (1)					
Modification nom et / ou prénom	397	390	7	7	0	0,0 €
Agents en formation	65	65	0	0	0	0,0 €

(1) Contrôle devenu obsolète du fait de la mise en œuvre de la nouvelle procédure de validation des modes de paiement

ÉVOLUTION DES TAUX D'ANOMALIES

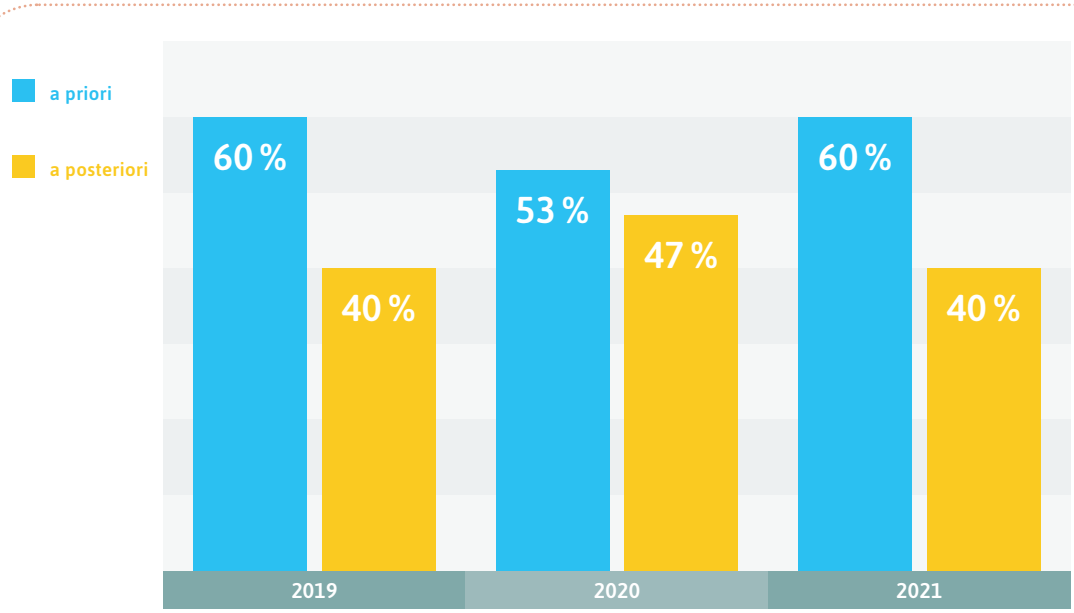
La baisse observée depuis 2018, liée à la sécurisation des procédures de gestion grâce au pilotage d'activités dans l'outil SIRIUS, est confirmée sur 2021.



ÉVOLUTION DE LA DÉTECTION DES ANOMALIES

Les anomalies détectées a priori sont celles qui sont décelées et corrigées avant le paiement.

La hausse de la détection a priori s'explique par le choix de la CNIEG de faire un traitement de paie Test complet avant le traitement de paie de production. Cela laisse plus de temps aux contrôleurs « métier » pour détecter et corriger les anomalies avant le paiement effectif de l'échéance.



IMPACTS FINANCIERS

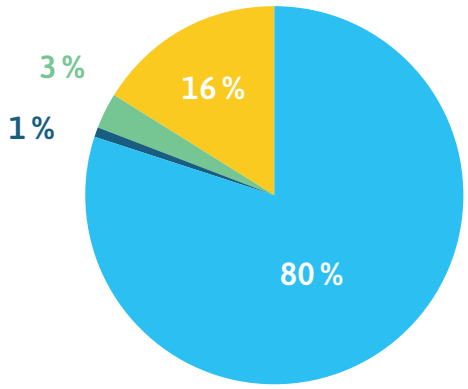
Le montant total de l'incidence financière détecté est de 1 178 445 € (différentiel entre ce qui est payé ou aurait pu être payé et ce qui est réellement dû).

La charge financière est de 31 047 € (elle correspond aux charges non recouvrables du fait de l'insolvabilité du débiteur, des remises de dettes, du dépassement des dates de prescription, de l'intangibilité des prestations…).

Le risque financier sur les dossiers contrôlés est de 839 956 €. Il représente le montant de l'incidence financière valorisée au regard de l'espérance de vie du débiteur ou de la fin de droit de la prestation, soit le coût de l'anomalie si le dossier n'avait pas été contrôlé).

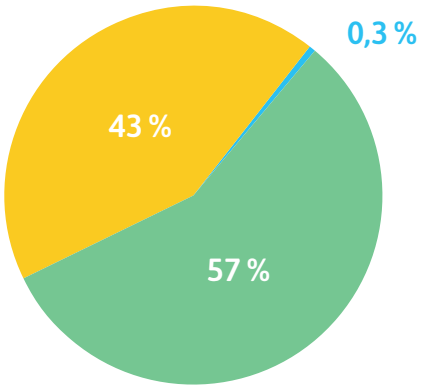
RÉPARTITION DE L'IMPACT FINANCIER

RÉPARTITION DE L'INCIDENCE FINANCIÈRE



84 % de l'incidence financière est détectée par les contrôles inscrits au PCI.

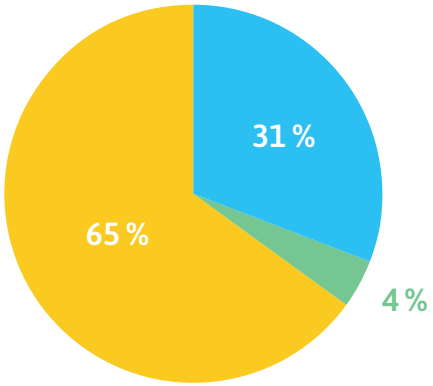
RÉPARTITION DE LA CHARGE FINANCIÈRE



57 % de la charge financière est issue des dossiers CRA. Elle correspond aux remises de dettes accordées pour des dossiers ayant pour origine une erreur de gestion de la CNIEG.

La part hors PCI est liée à des remises amiables accordées par le Directeur Comptable et Financier.

RÉPARTITION DU RISQUE FINANCIER



Le risque financier est projeté sur l'espérance de vie.

La part importante (65 %) du risque financier détecté hors PCI (avant paiement) s'explique principalement par deux anomalies qui dégagent un montant de 505 k€ (sur un total de 824 k€ de risque financier au titre de 2021).

Ce montant se décompose entre :

- Une prestation de réversion attribuée malgré l'absence de justificatif (pour 475 k€) ;
- Un rappel de rente accident de travail erroné (pour 30 k€).

PCI contrôles sur flux | PCI contrôles sur stock | dossiers CRA | hors PCI

RECOUVREMENT & CONTRÔLE 2021

RÉSULTATS DU RECOUVREMENT DE LA CNIEG

Le tableau ci-dessous présente l'état du recouvrement des cotisations et contribution dus à la CNIEG au titre de l'exercice 2021.

	Nbre de règlement en retard	Montant en retard	% règlement en retard	Montant en retard	Non recouvré au 01/03/2022	Taux de non recouvrement
RDC-RS	41	3 453 839,20 €	0,52 %	0,06 %	0,00 €	0,00 %
Petit-Pool	25	646 322,80 €	0,32 %	0,01 %	0,00 €	0,00 %
DSP	7	428 277,80 €	0,09 %	0,01 %	0,00 €	0,00 %
CTA	58	3 342 369,33 €	0,74 %	0,06 %	1 941 422,00 €	0,11 %
Total	**131**	**7 870 809,13 €**	**1,67 %**	**0,15 %**	**1 941 422,00 €**	**0,04 %**

Concernant le recouvrement social, la CNIEG présente au 1er mars 2022 un taux de recouvrement de 100 %.

La contribution tarifaire, qui relève de la sphère fiscale et concerne des entreprises également en dehors du périmètre de la branche professionnelle des IEG, présente un taux de recouvrement de 99,89 %.

Entreprises défaillantes :

Les montants non recouvrés en matière de contribution tarifaire correspondent à des entreprises mises en difficulté par la crise énergétique qui s'est déclarée à l'automne 2021. La situation des entreprises défaillantes est ainsi passée de 1 cas recensé en juin 2021 pour un total de 77 566,00 € à 5 cas recensés en juin 2022 pour un total de 2 708 084,09 € (y compris la société recensée déjà en 2021). Les cinq entreprises sont placées en liquidation judiciaire.

CONTRÔLE DE LA CONTRIBUTION TARIFAIRE

Du fait des contraintes liées au contexte sanitaire, les inspecteurs du recouvrement ont dû en 2021 adapter leur méthode de contrôle, organisant des réunions en distanciel avec leurs interlocuteurs au détriment des visites sur site.

Malgré cela, 7 contrôles ont été menés à leur terme au cours de l'année pour un redressement cumulé de plus de 5 M€ en faveur des entreprises.

3 contrôles à la fin de l'année restent à finaliser sur 2022 dont celui du plus gros collecteur, EDF.

2 faits marquants également ont nécessité une campagne d'information auprès des entreprises et une adaptation des outils de contrôle de la CTA :

- Nouvelle modalité de calcul de la quote-part CTA transport gaz des clients distribution au 1er juillet 2021 ;
- Évolution des taux CTA distribution et transport électricité à compter du 1er août 2021.

Avec l'arrivée programmée d'un nouvel inspecteur en 2022, l'objectif fixé sera d'augmenter le nombre de contrôles.

Contrôle du système d'information

Contrôle du système d'information

Conformément aux articles D.122-9 et D.114-4-10 à D.114-4-15 du Code de la sécurité sociale, le dispositif de contrôle mis en œuvre à la CNIEG comprend une part importante dédiée au contrôle des traitements informatiques :

- lors de leur conception, dans le cadre des projets informatiques ;
- lors de leur exécution ;
- lors de modifications apportées, dans le cadre de la maintenance courante ;
- dès lors que ces traitements ont un impact financier.

IMPACT FINANCIER

Toute application qui :

- traite des données financières (comptabilité, interface de paiement, gestion de comptes individuels…) ;
- génère des événements économiques (rubriques de paie, rubriques de cotisations…) ;
- attribue des droits à prestations (moteur de règles, moteur de liquidation…) ;
- impacte les calculs ou les répartitions de prestations dans le cadre de l'adossement ;

Est considérée comme ayant un impact financier.

Les redressements de données ayant une incidence sur le montant des prestations et les mises à jour de barèmes sont également considérés comme ayant un impact financier.

EXÉCUTION DES TRAITEMENTS

Tous les traitements informatiques font l'objet de contrôles automatiques qui restituent au moyen de listes d'erreurs toute anomalie rencontrée au cours de leur exécution. La « conduite d'applications », cellule dédiée au sein de la CNIEG, a pour mission de relever, traiter ou faire traiter ces anomalies.

De plus, chaque service effectue des contrôles supplémentaires sur certains traitements particuliers ayant un impact financier à l'aide de restitutions, d'éditions de cohérence…

PROJETS INFORMATIQUES

Durant les projets informatiques qui conduisent la CNIEG à mettre en œuvre de nouveaux traitements ou applications informatiques, le collectif maîtrise des risques intervient à différents niveaux dès lors que ces traitements ont un impact financier :

- participation à la phase de cadrage afin de définir les livrables indispensables à l'évaluation des risques de mises en service avec les pilotes des projets en fonction de leur nature.
- vérification de la présence d'études d'impacts ou d'analyses de risques ;
- validation de la stratégie et protocole de recette ;
- vérification de la couverture des tests et du respect de la stratégie de recette ;
- vérification de la bonne exécution de la recette ;
- vérification du plan de démarrage ;
- validation avant mise en production ;
- validation avant mise en service dans le respect des choix effectués dans la phase de cadrage.

Un représentant du DCF ou de la maîtrise des risques participe aux différents comités de pilotage des projets afin de suivre toutes les décisions opérationnelles et stratégiques.

L'ensemble de ces éléments permet de déterminer la couverture des risques avant toute mise en production.

MODIFICATION DE TRAITEMENTS (MAINTENANCE)

Toute évolution du système d'information à la CNIEG fait l'objet d'une demande formalisée, enregistrée et gérée informatiquement.

Toutes les demandes avec impact financier qui concernent des redressements de données sont validées par le collectif maitrise des risques dès émission de la demande.

Elles font l'objet :

- d'une autorisation de réalisation du redressement (phase de validation) ;
- d'un suivi et d'une vérification des recettes (fonctionnelles et utilisateurs) ;
- d'un contrôle de traçabilité ;
- d'une vérification de conformité préalable en environnement de recette.

Pour les cas particuliers où le redressement devient récurrent, le contrôle repose sur la réutilisabilité du script (paramètres) afin de limiter les contrôles décrits ci-dessus à la 1ère itération.

Toute demande avec impact financier impliquant une mise en production fait l'objet :

- d'une vérification de la couverture des tests par rapport aux spécifications ;
- d'un suivi et d'une vérification des recettes (fonctionnelles et utilisateurs) ;
- d'un contrôle de la recette de non-régression ;
- de contrôles complémentaires si nécessaire.

Les demandes sans impact financier font l'objet d'une vérification de l'absence réelle de cet impact.

Contrôle du système d'information

SYNTHÈSE DES CONTRÔLES 2021

127 (108 en 2020) demandes d'évolution du SI ont été émises par les différents services de la CNIEG dont 120 (105 en 2020) avec impact financier contrôlés par les auditeurs.

Ces demandes ont abouti à des redressements de données ou à des mises en production (MEP).

37 MEP (27 en 2020) dont 18 (13 en 2020) dites « Exceptionnelles » liées à des correctifs urgents.

351 redressements de données (297 en 2020) contrôlés par les auditeurs avec le soutien d'un renfort détaché du Département des Systèmes d'information.

Aucune demande de mise en production n'a été reportée à la demande du pôle maîtrise des risques.

Aucune demande de redressement de données n'a été reportée par celui-ci.

INCIDENTS INFORMATIQUES

Un incident informatique correspond à tout évènement ne faisant pas partie du fonctionnement d'un service attendu en production entraînant une interruption ou une réduction de la qualité du service et/ou une incidence financière.

Tous les incidents informatiques liés à l'exploitation du SI sont tracés par les équipes informatiques.

Deux types d'incidents techniques sont recensés : ceux correspondant à des attaques externes (voir Incidents liés à la sécurité) ayant des impacts sur le fonctionnement du site internet CNIEG et ceux liés à l'exploitation du SI.

En 2021, 41 incidents techniques se sont produits contre 31 en 2020.

La fréquence du contrôle des incidents informatiques a augmenté en 2021 : de semestrielle, elle est passée à trimestrielle. Le lien avec les risques de la cartographie CNIEG a été ajouté afin de faciliter la maîtrise du risque : ajout de scénario et/ou ajout de moyens de maîtrise complémentaires.

Pour prioriser la réalisation des nouvelles actions de maîtrise, en plus de la criticité de l'incident, un niveau d'effort de correction est évalué pour définir la valeur ajoutée de cette action.

En synthèse, voici l'historique des incidents :

Historique des incidents SI (COG)	2020		2021			
PCI-C220	**S1 2020**	**S2 2020**	**T1 2021**	**T2 2021**	**T3 2021**	**T4 2021**
Nombre d'incidents	24	7	5	8	18	10
Nombre incidents avec criticité >=8	0	2	0	0	1	0
Criticité maxi	6	20	4	5	9	3

Sur les 41 incidents, seul 1 incident a été évalué avec une criticité supérieure à 8. Il s'agit de l'inaccessibilité du portail pendant quelques minutes. Cet incident a eu lieu 3 fois en septembre 2021. Il a été évalué à 9 (possible et critique).

Cet incident a été rattaché au risque RSK-062 - NON-RESPECT DES NIVEAUX DE SERVICES DU SI.

L'effort de retour à la normale estimé par le service informatique est faible (1 sur une échelle de 1 à 4) puisqu'il consiste à relancer un service. La suppression du composant obsolète, générateur de l'incident, doit être réalisée.

SÉCURITÉ DU SI

Afin de sécuriser les données du SI, les machines de production sont redondées et sous contrat de maintenance. Les environnements de recette sont séparés de l'environnement de production.

Les bases de données de production, la gestion électronique de documents, les espaces collaboratifs et les serveurs de travail sont sauvegardés quotidiennement en mode incrémental, et en mode intégral hebdomadairement. Les politiques de rétention, mensuelle, annuelle ou pluriannuelle et de stockage des sauvegardes sont adaptées au besoin de conservation des données. Un exemplaire de toute sauvegarde est externalisé chez un prestataire dans un cadre contractualisé. Des tests réguliers de restauration sont effectués.

En cas de sinistre majeur, 25 positions de travail sont mises à la disposition de la CNIEG par la société SIGMA sur le site de repli de la Chapelle-Sur-Erdre (44). Celui-ci est en relié au Datacenter SIGMA de Carquefou (44) qui héberge les serveurs CNIEG sur lesquels sont répliqués quotidiennement une partie du SI. Les autres services hébergés chez SIGMA sont redondés sur au moins 2 datacenters. Le plan de reprise d'activité SI (PRA SI) décrit les actions mises en œuvre pour permettre le démarrage des moyens informatiques nécessaires à un retour de l'activité post-sinistre sur un périmètre d'activité défini et dans un court délai.

L'accès aux salles serveurs est sécurisé par un lecteur de cartes. Ces salles sont équipées de détecteurs incendie avec un système d'extinction automatique et de double climatisation sous contrat de maintenance. Les transferts de données vers des partenaires externes sont sécurisés et chiffrés.

Les postes utilisateurs sont chiffrés, protégés par un anti-virus et continuellement mis à jour des failles de sécurité. Conformément à la note d'application AP-DSI-00 relative aux contrôles sur les habilitations informatiques, tous les administrateurs des applications sont approuvés et vérifiés par une revue complète des habilitations. Grâce à ce contrôle les droits d'accès des agents ont été justifiés, modifiés ou clôturés.

Le trafic réseau est analysé par un prestataire externe. Le suivi fait l'objet d'un reporting mensuel mis à disposition de l'équipe exploitation. Les éventuelles tentatives d'intrusion sont étudiées par un SOC et escaladées vers le RSSI. Des tests et audits de sécurité sont menés régulièrement sur différents périmètres du SI.

BILAN 2021

La sécurité du SI fait l'objet, dans le dispositif de contrôle interne, d'un risque majeur identifié spécifiquement, couvert par 7 contrôles différents. Ceux-ci n'ont révélé aucune anomalie en 2021.

Cette année aura été marquée par un contexte cybersécurité mondial impliquant un niveau de risque sans précédent pour les entreprises et les administrations. Notamment, le risque lié au rançongiciel[1] a été pointé par tous les spécialistes comme étant le risque majeur présentant un fort niveau de criticité.

La CNIEG a pris en compte cette élévation exogène du niveau de risque et mis en œuvre un plan d'action spécifique de mesures de couverture, en lien avec son conseil d'administration et en s'appuyant sur son partenaire spécialisé en charge de l'hébergement de certains équipements réseau & informatiques ainsi que de la surveillance de la sécurité SI.

[1] *Un, rançongiciel ou logiciel de rançon est un logiciel malveillant qui prend en otage des données personnelles. Pour ce faire, il chiffre des données personnelles puis demande à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.*

Contrôle du système d'information

… SUITE BILAN 2021

En interne CNIEG :

Au premier trimestre 2021, la CNIEG a procédé au renouvellement de l'ensemble des postes de travail de ses collaborateurs afin de les doter d'équipements :

- Munis des outils leur conférant un niveau de sécurité optimal,
- Adaptés au contexte de télétravail massif.

En cours d'année, le système de sauvegarde du Système d'Information a été renouvelé vers une version intégrée plus sécurisée et embarquant le périmètre Office 365.

Plusieurs campagnes de sensibilisation des utilisateurs ont été menées en cours d'année, appuyées par la création d'un espace intranet dédié à la Sécurité SI et au RGPD, à destination de tous les collaborateurs, prestataires et intérimaires.

Portail web :

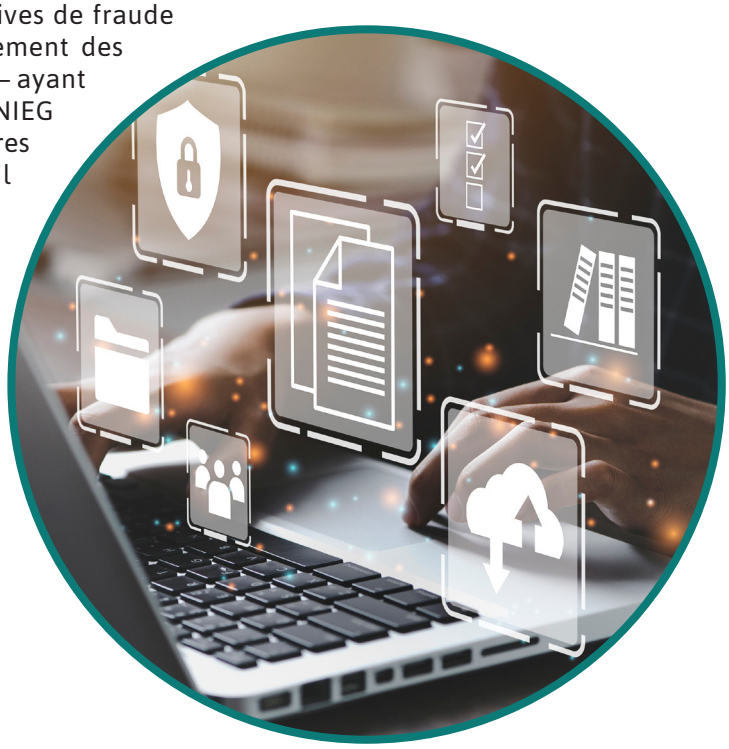
Le niveau de sécurité du portail de services web de la CNIEG a été renforcé en rendant obligatoire, pour certaines démarches critiques, l'authentification de l'utilisateur internaute par un deuxième facteur (code PIN de validation : procédé « MFA » : MultiFactor Authentification).

En octobre, l'homologation RGS (Référentiel Général de Sécurité) du portail web de la CNIEG, qui atteignait sa date d'expiration normale au bout de 3 ans, a été renouvelée par le Directeur et le Directeur Comptable et financier.

INCIDENTS LIÉS À LA SÉCURITÉ

Il n'y a eu aucun d'incident de sécurité détecté nécessitant l'organisation d'une cellule de crise en 2021.

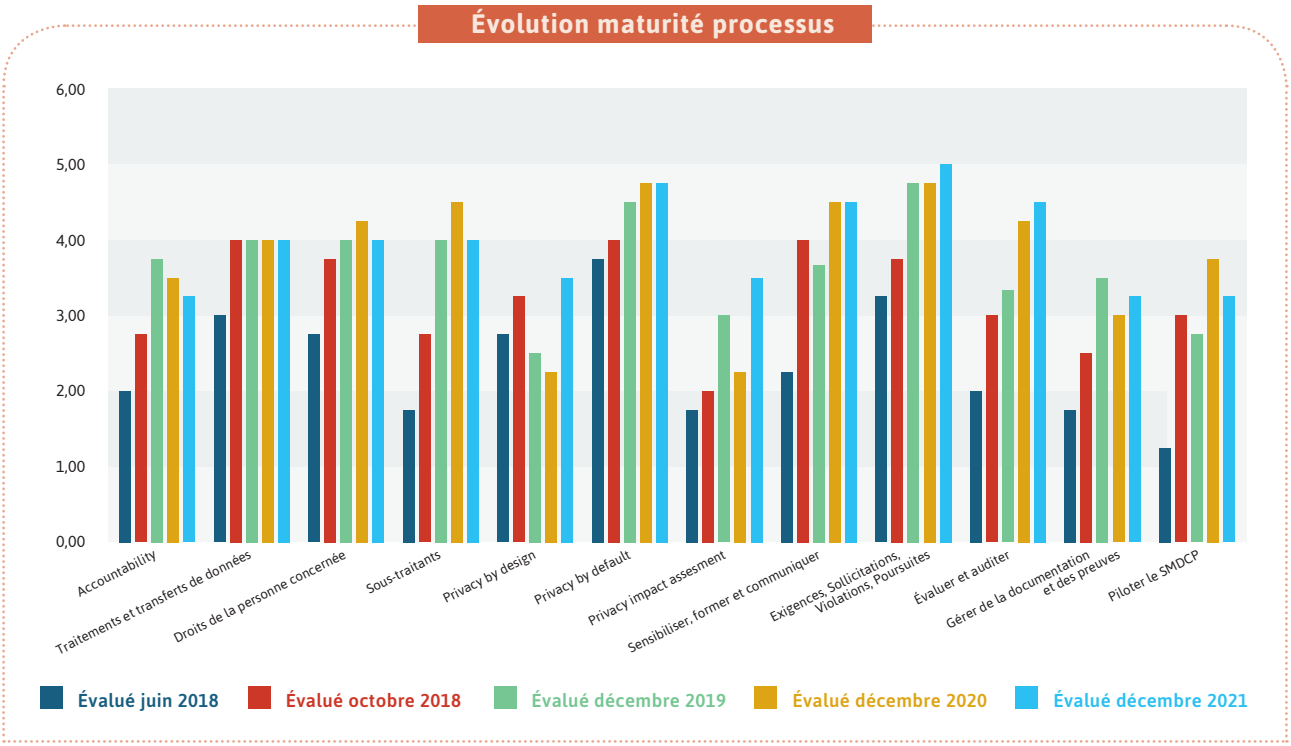
Toutefois, la détection début 2021 de tentatives de fraude aux coordonnées bancaires par le détournement des boites aux lettres numériques de pensionnés – ayant dans quelques cas, abouti – a conduit la CNIEG à mettre en place des mesures complémentaires de sécurisation des démarches sur son portail web, à l'aide de codes PIN de validation (cf. ci-dessus). Ces mesures ont été mises en place pour partie en 2021 (la suite étant prévue au premier semestre 2022) conformément aux recommandations du prestataire Orange Cyber Défense, que la CNIEG a consulté spécifiquement sur cette problématique.



RÈGLEMENT GÉNÉRAL DE PROTECTION DES DONNÉES

Évolution de 2018 à 2021 de l'évaluation de maturité :

Un dispositif de conformité sous contrôle et des fluctuations symboles des axes de développement priorisés durant l'année en cours.



Eléments d'analyse, quelques enseignements :

Rubrique « Management » *(de responsabilisation à sous-traitants)* :

Vecteurs de ce domaine globalement satisfaisants, reste à appuyer en 2022 sur la formalisation des politiques

Rubrique « opérationnel » *(de protection des données dès la conception à sensibiliser)* : le meilleur score global.

Pour « protection des données dès la conception » la note reste relativement faible mais on constate néanmoins une amélioration : 3,50 » vs 2,50 en A-1. En effet, « la protection des données » est mieux identifiée comme devant être une préoccupation dès le début d'un projet, d'une création ou d'une mise en place. Concernant la prise en compte de la gestion des droits de la personne et la sécurité des données dès la phase de conception du projet et durant son cycle de vie il n'y a pas de points de vigilance spécifiques actuellement. La sécurité mise en œuvre « couvre tout ». Dans le process de recettage et livraison, la sollicitation du DPD reste à mettre en place comme l'an passé mais lors de la phase de réflexion pré-mise en place le message semble passé.

Le « Protection des données par défaut » présente un score stabilisé par rapport à 2020 car c'est toujours à l'occasion d'une alerte, d'une anomalie ou d'un réexamen de procédure que l'existant est corrigé/réinterrogé et donc mis en conformité.

À noter : il y a toujours plus de flux existants à revisiter que de nouveaux flux en création ce qui minimise le risque de non-conformité.

Pour le PIA lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des clients ou lorsqu'une partie intéressée demande une preuve de conformité nous serions en mesure de produire l'analyse attendue car le travail effectué avec le GT réseau OSS nous a permis de mieux appréhender le périmètre et la méthodologie à mettre en œuvre concourant ainsi à l'atteinte de notre objectif 2021 dans ce domaine. Ce point « PIA » apparait toujours comme une contrainte supplémentaire pour les responsables de projet déjà très sollicités, un travail de sensibilisation sur ce point devra être mené en 2022.

Rubrique « support » *(de exigences à piloter)* :

Les notes des vecteurs 9 et 10 démontrent notre réactivité et notre implication sur le sujet protection des données : dossiers traités dans les délais, souci du respect de la réglementation. Reste à développer pour l'Item « support » les vecteurs 11 et 12 => à étudier dans le cadre d'une action de benchmark (réseau OSS) et le conseil d'un éventuel auditeur externe qui n'a pu être mobilisé sur 2021.

En résumé :

Les scores progressent pour les items : « protection des données dès la conception », « analyse d'impact relatives à la protection des données (AIPD) », « exigences - sollicitations - violation de données », « évaluer et auditer » du fait des efforts portés sur ces points à risque et essentiels ou non priorisés jusqu'alors (confidentialité). C'est le signe d'une montée en compétence et d'une volonté de systématiser la recherche de conformité (maturité du process) par toutes les parties prenantes.

Parmi les points à améliorer reste encore cette année « responsabilisation ». Cet item concerne la formalisation de la politique générale relative aux données de l'entreprise (processus, ressources, mesures) : chantier « projet » d'envergure qui ne peut pas prendre néanmoins le pas sur le « fonctionnement » = sollicitations clients et internes mais qui devra être mené (cf plan de marche 2022)

Concernant la gestion de la documentation (liste de documents à valeur de preuves…) et le pilotage l'amélioration viendra avec l'expérience et le benchmark : l'apport du réseau OSS, AFCDP, IEG,

Enfin un audit spécifique externe de la conformité RGPD serait souhaitable et de nature à valider cette évaluation qui reste somme toute subjective.

Dispositif de lutte contre la fraude

Dispositif de lutte contre la fraude

GROUPE D'ANALYSE DU RISQUE DE FRAUDE (GARF)

Le GARF est un groupe de travail multi¬disciplinaire, créé à la suite d'une décision du comité de direction du 8 septembre 2009.

Cette décision répond à la volonté du législateur de lutter contre la fraude (article L. 114-9 du Code de la sécurité sociale et les suivants) :

- obligation de faire procéder à des enquêtes et contrôles en présence de faits susceptibles de constituer une fraude ;
- élargissement du champ d'application de la sanction pénale applicable aux fraudes à la sécurité sociale et accroissement de son montant ;
- obligations concernant la coopération inter-organismes.

La mission du GARF s'articule autour de 4 axes principaux :

- proposer à la direction une politique de lutte contre les fraudes et à ce titre déterminer les priorités de l'année ;
- centraliser et analyser l'ensemble des informations relatives aux fraudes, abus et fautes afin d'avoir une vue globale de la situation de la CNIEG ;
- proposer des actions de prévention par le biais de « blocages » sur les chaînes de production, création de requêtes informatiques, mise en place de circuits de détection ;
- organiser le déploiement opérationnel du dispositif (plan d'actions, méthodologie, communication...).

TRAVAUX 2021

Au titre de la lutte contre la fraude, le GARF a travaillé sur les sujets suivants :

- développement du réseau local en matière de lutte contre la fraude ;
- professionnalisation des équipes dans la lutte contre la fraude ;
- renforcement de la communication interne et externe.
- renforcement de la sécurisation des coordonnées bancaires.

MÉTHODES DE LUTTE CONTRE LA FRAUDE TRANSFRONTALIÈRE OU INTERNATIONALE

La CNIEG demande, pour permettre le paiement d'une pension vieillesse sans interruption, que le pensionné résidant à l'étranger justifie de son existence et adresse à la CNIEG le formulaire « attestation d'existence pour le paiement des retraites » certifié par les autorités locales du pays de résidence, avant le 1er mars à valoir pour l'échéance du 1er avril de chaque année (sauf pour les résidents à Monaco et dans les collectivités territoriales où seule une attestation sur l'honneur est demandée).

Cette demande est conforme aux modalités prévues par la circulaire CNAV n° 2001-31 du 3 mai 2001.

RÉSULTATS 2021

Le plan de contrôle interne 2021 de la CNIEG retenu après avis du comité d'audit en décembre 2020, comptait 20 actions de contrôle couvrant les thématiques de fraude aux prestations (10 contrôles) et de fraude sur la gestion interne (10 contrôles).

Aucun cas de fraude n'a été détecté par ces contrôles.

DOSSIERS DE FRAUDES INTERVENUES À LA CNIEG

Au cours de l'année 2021, la CNIEG a été victime de plusieurs séries de fraudes externes concernant des changement de coordonnées bancaires par voie dématérialisée à la suite de l'usurpation d'identité de pensionnés :

- En janvier : 12 situations de fraude dont 2 concernant des prestataires décédés.

  Les changements de coordonnées bancaires sont ceux de la banque en ligne TREEZOR.

  Les retraites de 5 prestataires au titre de l'échéance de février 2021 ont été versées à tort pour un montant de 13 159,40 euros (Retour de fond de la banque d'un montant de 2 361,92 €, ne pouvant être rattaché à un dossier en particulier).

- En février : 3 situations de fraude.

  Les actions de sécurisation de paiement mis en place suite aux fraudes intervenues au mois de janvier ont permis de stopper les versements de retraites indus sur le mois de février et suivant.

- En mars : 9 situations de fraude, dont 1 concerne un prestataire qui avait déjà fait l'objet d'une fraude en janvier.

- En avril : 4 situations de fraude.

Ces fraudes ont donné lieu à des dépôts de plaintes groupés par courrier auprès du procureur de la république du Tribunal Judiciaire de Nantes : le 09/02/2021 (pour janvier), le 12/04/2021 (pour février), le 21/04/2021 (pour mars), le 17/05/2021 et le 09/06/2021 (pour avril).

Ces dépôts de plaintes ont également fait l'objet d'un procès-verbal établi en gendarmerie le 19/10/2021.

À ce jour, ces plaintes sont toujours en cours d'instruction.

À noter : Ces fraudes aux changements de coordonnées bancaires sont associées à des fraudes aux changements de coordonnées téléphoniques et/ou mails, dans la grande majorité des cas.

La CNIEG a également été victime d'une fraude en août 2021. La caisse a été destinataire d'une demande de changement de coordonnées bancaires par voie postale avec usurpation d'identité, accompagnées d'un RIB falsifié.

La CNIEG a déposé plainte auprès du Tribunal Judiciaire de Nantes le 30/08/2021.

Dispositif de lutte contre la fraude

BILAN DES POURSUITES ENGAGÉES

Concernant la procédure pénale, les plaintes concernant des demandes de changement de coordonnées bancaires par voie postale avec usurpation d'identité, accompagnées de RIB falsifiés (sans préjudice financier) intervenues en 2020, ont été classées sans suite motif auteur inconnu :

- 2 plaintes auprès du Procureur de la République des Tribunaux Judiciaires de Pontoise et Créteil, déposées le 13/10/2020 ;
- 3 plaintes auprès du Procureur de la République des Tribunaux Judiciaires de Castres, de Bastia et de Saint-Malo, déposées le 23 décembre 2020.

AMENDES, SANCTIONS OU AUTRES PEINES PRONONCÉES À LA SUITE DE FRAUDES

Seule la procédure de pénalités financières, prévue à l'article L. 114-17 du Code de sécurité sociale, est applicable à la caisse, celle-ci n'assurant pas la gestion du « risque maladie ».

Par décision en date du 20 septembre 2012, le conseil d'administration de la CNIEG a instauré, à compter du 1er janvier 2013, la procédure de pénalités financières au sein de la caisse et créé une commission spécifique dite Commission de pénalités financières (CPF).

Pour l'année 2021, il n'y a eu aucune amende, sanction ou autre peine prononcée à la suite de fraude.

COOPÉRATION AVEC D'AUTRES RÉGIMES OU SERVICES PUBLICS

Dans la continuité des actions déjà engagées, la CNIEG a poursuivi sa collaboration avec la DGFIP pour l'utilisation en masse de FICOBA.

En 2021 la CNIEG a contacté la préfecture de Loire-Atlantique pour demander à participer au Codaf (Comité opérationnel départemental anti-fraude) et a initié un réseau des DCF de Loire-Atlantique pour partager les bonnes pratiques en la matière.

Résultats du plan de contrôle du Directeur comptable et financier 2021

Résultats du plan de contrôle du Directeur comptable et financier 2021

IMMOBILISATIONS

L'inventaire de fin d'exercice a recensé 275 matériels sensibles et/ou mobiles affectés, dont 209 ordinateurs, 43 téléphones, 22 tablettes et 1 borne wifi. Les attestations des détenteurs de matériels existent et sont scannées, archivées sur l'application informatique GLPI gérée par DSI.

Les inventaires informatique et mobilier ont été effectués par les différents responsables, les retraits d'immobilisations ont représenté 255 k€. Les délais d'enregistrements de déclenchement des amortissements ont été respectés. Les immobilisations en cours s'élèvent à 2 045 k€. Elles concernent des projets informatiques et feront l'objet de créations définitives à la mise en service des applications.

Onze fiches investissement traitées pour une valeur totale de 1 754 k€ et concernent principalement la mise service de la relation client multicanal (engagement COG 1.4), l'optimisation de la gestion des données internes et externes (engagement COG 2.3) et la poursuite de notre engagement dans l'Inter Régime (engagement COG 2.1).

Les provisions, qui n'entrent pas dans le cadre des inventaires, ont été réactualisées, notamment la provision amiante.

FRAIS DE PERSONNEL

Les cotisations du personnel ont fait l'objet de 32 contrôles sur les flux générés par l'application RH Chor@l. Aucun écart n'a été décelé sur l'année.

92 comptes épargne temps sont ouverts pour un montant global de 1 102 k€. Une vérification a été réalisée en comptabilité pour s'assurer de la cohérence entre l'application comptable CEGID et l'application RH Chor@l.

Les traitements RH Chor@l de paye ont tous été générés dans l'application CEGID de comptabilité, avec concordance des montants.

Les salaires mensuels ont été réglés en totalité selon les sommes calculées par l'application de paie. Ils ont été mis en paiement selon les dates planifiées en début d'année.

Au 31 décembre 2021, le contrôle sur stock des Titres Restaurant (TR) ne fait ressortir aucun TR non distribué. Aucun stock de CESU n'est constaté.

Le contrôle mensuel entre les sommes comptabilisées du prélèvement à la source des agents et le montant prélevé par la DGFIP ne fait ressortir aucun écart.

GESTION DES TIERS

FOURNISSEURS

20 factures sans commande ont été recensées au titre de l'exercice sur un total 1 478 factures traitées. Elles portent sur un montant global de 82 k€ et toutes ont été justifiées.

Les régularisations de comptes, entre comptabilité générale et comptabilité analytique sur la période, ont fait l'objet de 170 demandes dont 89 pour changement d'objet de gestion et 81 pour changement d'affectation comptable.

Au 31 décembre 2021, il n'y a aucune réception (achats et prestations) en attente de factures, des charges à payer sont comptabilisées en ce sens.

Sur un échantillon représentant 67 % des factures contrôlées, un contrôle d'imputation investissements vs exploitation (montants supérieurs à 800 € HT) est réalisé, soit 840 contrôles pour un total de 1 285 factures. Aucune anomalie n'a été constatée.

CLIENTS

Au 31 décembre 2021, 14 factures de vente non réglées ont été recensées. Elles représentent un montant global de 15,5 k€. Aucune facture ne dépasse le délai de paiement de 30 jours.

Les 10 prestations, associées à des conventions, ont fait l'objet de facturations sur 2021 pour un montant global de 564,80 k€.

GESTION TECHNIQUE (COMPTABILITÉ DU RÉGIME IEG)

Les pièces justificatives nécessaires au paiement des prestations ont été reçues dans les délais. Les versements ont été réalisés selon le calendrier prévu.

Les dossiers contentieux (hors contentieux amiante), au nombre de 17, ont été analysés. La reprise sur provisions s'élève à 72,8 k€ en fin d'année au titre de la prise en compte des versements réalisés. Le montant global du reste à recouvrer est de 1 229 k€.

Le suivi des comptes individuels (apurements, remises…) fait apparaître en fin d'année des pertes pour 496,4 K€.

Les traitements issus des applications de gestion des retraites et des cotisants ont tous été comptabilisés aux dates planifiées.

La situation au 31 décembre 2021 fait apparaître, pour les 385 entreprises collectrices étudiées : 289 entreprises ayant un solde nul, 93 ayant un solde identique en comptabilité et en gestion et 3 en cours de régularisation.

Le contrôle annuel de cohérence des assiettes CSG/CRDS déclarées à l'Urssaf ne présente pas d'anomalie significative au 31 décembre 2021.

Le contrôle mensuel entre les sommes comptabilisées du prélèvement à la source des pensions versées et le montant prélevé par la DGFIP ne fait pas ressortir d'écart non justifié.

Résultats du plan de contrôle du Directeur comptable et financier 2021

TRÉSORERIE

SUIVI JOURNALIER

L'analyse mensuelle des 15 comptes bancaires suivis quotidiennement a été faite régulièrement avec vérification de la cohérence solde comptable / rapprochement bancaire / livre de position.

52 contrôles de remises de chèques ont été réalisés, sans révéler d'anomalie à incidence financière.

SUIVI MENSUEL

Les habilitations sont suivies selon les préconisations édictées (PG-PIL 01, PG-PIL 05). La vérification des pièces de paiement émises en trésorerie n'a fait ressortir aucune anomalie entre les signatures et les personnes mandatées. Les pouvoirs bancaires sont formalisés au regard des activités et des responsabilités.

Le solde journalier de trésorerie sur l'année 2021 a été suivi au travers de 260 contrôles. Aucun des comptes fusionnés CA-CIB ou Bred n'a été à découvert.

Au 31 décembre 2021, le solde des liquidités de la caisse s'élève à 654,74 € et celle de la « petite caisse » (mise à disposition des moyens internes par la trésorerie) à 196,25 €. Les contrôles de tenue des caisses réalisés n'ont pas révélés d'anomalie.

Le suivi des encaissements en attente d'affectations fait ressortir au 31 décembre 2021, 17 mouvements non affectés par manque de précision et il n'est constaté aucun prélèvement en attente d'affectation.

SUIVI TRIMESTRIEL DU RECOUVREMENT

Durant l'année 2021, sur l'ensemble des entreprises sollicitées pour confirmer le reversement RDC ou CTA, seules 11 entreprises n'ont pas répondu. Elles ont cependant toutes bien réalisé leurs reversements.

SUIVI DU FINANCEMENT

Sur l'ensemble des entreprises sollicitées pour confirmer le reversement RDC ou CTA, toutes ont répondu durant l'année 2021.

OBLIGATIONS

DÉCLARATIVES

Les obligations déclaratives auprès des organismes (8 au total) sont mensuelles, trimestrielles ou annuelles, elles ont toutes été respectées. Les versements d'un montant global de 620 M€, pour 38 paiements, ont respecté les échéances.

COMPTABLE

L'échéancier des clôtures périodiques (au nombre de 10), est décrit dans la note de doctrine DC 21001. Sur l'exercice, des décalages ont été constatés sur les dates de clôture, les reports s'expliquant par des résultats de traitements informatiques et des informations comptables non parvenus dans les délais.

Les 196 comptes comptables mouvementés du bilan ont fait l'objet d'un suivi régulier tout au long de l'exercice selon la note de doctrine DC 21001. À la date de clôture, 72 comptes ont un solde nul. Les 124 autres comptes sont justifiés.

Les états comptables réglementaires, les états financiers ainsi que le rapport du DCF de l'exercice 2021 ont tous été sauvegardés.

Sur l'année 2021, le contrôle des écritures manuelles fait ressortir 9044 lignes d'opérations comptables toutes issues de saisies réalisées par des utilisateurs habilités.

RÉGLEMENTATION

Toutes les notifications d'évolution du PCUOSS (Plan Comptable Unique des Organismes de Sécurité Sociale), ayant un impact en comptabilité sur les risques gérés par la CNIEG ont fait l'objet d'attention sur la mise à jour des référentiels comptables. En parallèle, le CHIRCOSS (Comité d'Harmonisation Inter-Régimes des Comptes des Organismes de Sécurité Sociale) a complété la doctrine comptable afin de préciser certaines natures d'opérations.

Une note « planning des arrêtés » a été créée et validée pour application sur 2021. Aucune instruction particulière n'a été enregistrée pour préciser d'autres dispositions comptables.

Axes d'amélioration pour 2022

Axes d'amélioration pour 2022

POURSUITE DE LA TRANSFORMATION DU COLLECTIF MAÎTRISE DES RISQUES

RAPPEL DE L'ORGANISATION MISE EN PLACE EN 2021

Le pilotage par les risques : cf. engagement 2.4 de la COG	Maîtrise des risques par l'Audit et le contrôle interne
La responsable PMR devient **Déléguée à la Gestion des Risques**	Les contrôleurs internes deviennent **Auditeurs internes**
Rôle : chargée de faire vivre le pilotage des risques avec les missions suivantes : - Pilotage du système management du risque ; - Animation du réseau des contributeurs à la maîtrise des risques ; - Accompagnement dans l'appropriation homogène et satisafaisant de la démarche à la Caisse ; - Appui dans la déclinaison opérationnelle de la démarche ; - Mise en place et maintenance d'un référentiel documentaire (yc cartographie des risques ; - Management de l'équipe PMR.	**Rôle :** - Réalisation d'un plan d'audit (yc supervision contrôles de niveau 2) ; - Animation du dispositif de **contrôle interne** et l'accompagnement des services ; - Organisation de l'élaboration du PCI année + 1 ; - Prise en compte des variations dans la cotation des risques en cours d'année.
Redevabilités : - Fournir au groupe d'auditeurs toutes les variations du périmètre des risques ainsi que les moyens de maîtrise associés ; - Garantir que les auditeurs ont pris en charge la supervision de ces moyens de maîtrise ; - Fournir aux porteurs d'enjeux le niveau de maîtrise des risques sur les enjeux ; - Produire une synthèse des actualités sur le pilotage des risques ; - Informer le Directeur de la Caisse et le Directeur Comptable et Financier.	**Redevabilités :** - Réalisation d'audits flash à la demande des services ou du comité des risques ; - La réalisation du reporting : tableaux de bords mensuels dont maintenance des indicateurs, rapports Directeur Comptable et Financier, rapport annuel de Contrôle interne, rapport annuel du Directeur ; - Communication des résultats et de l'analyse des résultats vers les services.

Axes d'amélioration pour **2022**

PILOTAGE PAR LES RISQUES

L'objectif est de diffuser les bonnes pratiques en termes de gestion des risques, notamment réviser les risques dès l'apparition d'un évènement ou d'incident afin de trouver les meilleures actions de maîtrise possibles qui seront prises en charge par les auditeurs internes.

Les recommandations émises lors des audits internes servent également à la révision des risques.

Ainsi, les revues de risques réalisées au fil de l'eau permettent de fournir un état des lieux en temps réel aux porteurs d'enjeu de la CNIEG.

Le comité stratégique (COSTRAT) fera un point trimestriel circonstancié sur les risques stratégiques, les risques opérationnels étant étudiés lors du comité des risques.

MAITRISE DES RISQUES

L'objectif de 2022 est la montée en compétences et en autonomie des auditeurs sur l'audit interne, conformément à l'article D.114-4-9 du code de la sécurité sociale, tout en gardant un haut niveau de service sur le contrôle interne.

Sur le volet informatique, dans le cadre de l'optimisation des processus, le pôle maîtrise des risques prépare le transfert de certaines activités de contrôles vers le Département Système d'Information. Cela permettra de détecter au plus tôt les écarts de programmation et de fluidifier les correctifs. L'auditeur interne expert en informatique pourra déclencher des audits flash pour vérifier le respect de la réglementation (article D.114-4-12 du code de la sécurité sociale).

GESTION DES INCIDENTS INFORMATIQUES

Le traitement des incidents informatiques est en constante amélioration en coordination avec le service informatique et le pôle maîtrise des risques.

L'objectif 2022 est de créer des familles d'incidents pour pouvoir élaborer des statistiques plus précises et demander la priorisation de correctifs, en fonction de la volumétrie des incidents par famille.

Glossaire

AFCDP : Association Française des Correspondants à la protection des Données à caractère Personnel

AGIRC : Association Générale des Institutions de Retraite des Cadres

ARRCO : Association des Régimes de Retraites Complémentaires

AT : Accident du Travail

CAMIEG : Caisse d'Assurance Maladie des Industries Électriques et Gazières

CESU : Chèque Emploi Service Universel

CHIRCOSS : Comité d'Harmonisation Inter-Régimes des Comptes des Organismes de Sécurité Sociale

CI : Contrôle Interne

CNAV : Caisse Nationale d'Assurance Vieillesse

CNIEG : Caisse Nationale des Industries Électriques et Gazières

CNIL : Commission Nationale de l'Informatique et des Libertés

COG : Convention d'Objectifs et de Gestion

COSTRAT : Comité Stratégique

CPF : Commission de Pénalités Financières

CRA : Commission de Recours Amiable

CTA : Contribution Tarifaire d'Acheminement

DCF : Directeur Comptable et Financier

DGFIP : Direction Générale des Finances Publiques

DPD : Délégué à la Protection des Données

FICOBA : Fichier des Comptes Bancaires

IF : Incidence Financière

MFA : Multifactor Authentification

MEP : Mise En Production

MP : Maladie Professionnelle

MSA : Mutualité Sociale Agricole

OSS : Organisme de Sécurité Sociale

PCDCF : Plan de Contrôle du Directeur Comptable et Financier

PCI : Plan de Contrôle Interne

PCUOSS : Plan Comptable Unique des Organismes de Sécurité Sociale

PIA : Privacy Impact Assessment (étude d'impact sur la vie privée)

PMR : Pôle Maitrise des Risques

QVT : Qualité de Vie au Travail

RDC : Régimes de Droit Commun

RGPD : Règlement Général de Protection des Données

RGS : Référentiel Général de Sécurité

RS : Régime Spécial

RSSI : Responsable Sécurité des Systèmes d'Information

SI : Système d'Information

SICAE : Société d'Intérêt Collectif Agricole d'Électricité

SSF : Sursalaire Familial

TEM : Traitement Échéance Mensuelle

TIF : Taux d'Incidence Financière

TJ : Traitement Journalier

TR : Ticket Restaurant

URSSAF : Union de Recouvrement des cotisations de Sécurité Sociale et d'Allocations Familiale

Informations - **Mentions Légales**

Propriété : CNIEG, 20 rue des Français Libres, CS 60415, 44204 Nantes Cedex 2 | Siret : 478 650 385 00014

Photos : © EDF/Alexandre Sargos, © EDF/Getty Images/Dylan Ellis, © EDF/Fabrice Arfaras, © EDF/Marc Didier, © EDF/Getty Images/Mike Kemp, © EDF/Getty Images/Paul Burns, © EDF/Pierre Berenger, © EDF/Archive Fenice Com © EDF/Getty Images, © BillionPhotos.com/stock.adobe.com, © Kenishirotie/stock.adobe.com, © maxsim/stock.adobe.com, © Delphine Lethu/l'Oeil à la Page

Création graphique : www.lenart-graphiste.fr | Image : Freepik.com | Crédits photos : Shutterstock.com et Fotolia.com

CNIEG

Votre retraite, notre métier

Rapport relatif au dispositif de Contrôle Interne

2021