

Caisse Nationale de l'Assurance Maladie

des Travailleurs Salariés

Sécurité Sociale

Circulaire CNAMTS

Date :
08/06/98

Origine :
ACCG
DISI

MMES et MM les Directeurs et Agents Comptables

- des Centres de Traitement Informatique

(Pour Attribution)

Réf. :

ACCG n° 16/98 - DISI n° 6/98

Plan de classement :

113					
-----	--	--	--	--	--

Objet :

INSTRUCTION DE CONTROLE INTERNE DES CENTRES DE TRAITEMENT INFORMATIQUE.

Pièces jointes :

--	--

Liens :

Date d'effet :

Dossier suivi par :

Téléphone :

@

Date de Réponse :

Anne de CADEVILLE - Valérie DEBONO

01/42/79/35/18

01/42/79/42/25

Agence Comptable / Contrôle de Gestion
Direction de l'Informatique et des Systèmes d'Information

08/06/98

MMES et MM les Directeurs et Agents Comptables

- des Centres de Traitement Informatique

Origine :
ACCG
DISI

(Pour Attribution)

N/Réf. : DISI n° 6/98 - ACCG n° 16/98

Objet : Instruction de contrôle interne des Centres de Traitement Informatique

Par circulaire du 27 novembre 1995, nous vous avons transmis en application du décret du 10 août 1993, l'instruction de contrôle interne portant sur le dispositif de contrôle interne à mettre en place dans les Centres de traitement informatique.

Ce dispositif repose sur l'association du Directeur et de l'Agent Comptable du C.T.I. pour déterminer les moyens à mettre en oeuvre, afin de pallier les risques, notamment financiers, inhérents à l'environnement informatique et au traitement des flux.

Les centres de traitement informatique ont apporté des réponses très diversifiées, qui ont été retracées dans les plans de contrôle interne annuels transmis pour la plupart à la Caisse Nationale.

Après plus de deux ans de mise en place de ce nouveau dispositif, il convient d'établir un bilan et de compléter les instructions initiales, afin d'intégrer des modes opératoires efficaces à la mise en oeuvre de nouveaux applicatifs informatiques et principalement du système SESAM VITALE, et de s'assurer que les centres de traitement informatique ont tous atteint en juin 1999 un niveau de référence a minima en matière de contrôle interne.

1 - LE BILAN

Pour réaliser le bilan de mise en oeuvre de ce nouveau dispositif, la Caisse Nationale a procédé à une étude régulière des plans de contrôle et des plans pluriannuels d'actions que les CTI sont tenus de lui communiquer, et a organisé l'exposé de différents plans de contrôle interne.

Le constat fait apparaître des points forts et des points faibles.

1.1 - Points forts

l'association entre le Directeur et l'Agent Comptable du CTI s'est manifestée concrètement à l'occasion de la mise en oeuvre d'actions de contrôle interne,

le protocole CPAM-CTI relatif aux traitements effectués par le CTI a favorisé la définition des responsabilités respectives des parties signataires, et a aidé à l'harmonisation des approches lors des fusions,

la majorité des centres de traitement informatique a procédé à un audit interne,

la majorité des centres de traitement informatique dispose d'un plan pluriannuel d'actions,

avec l'opération CTI 98, tous les centres de traitement informatique doivent désormais comprendre dans leur effectif un DIAC (Délégué Informatique de l'Agent Comptable) et un RSSI (Responsable de la Sécurité des Systèmes d'Information).

1.2 - Points faibles

la majorité des centres de traitement informatique ne dispose pas d'un plan de contrôle interne opérationnel, avec des modes opératoires formalisés : la démarche de maîtrise des risques n'est pas perçue comme indispensable,

les approches divergent sensiblement ; rares sont les CTI où une démarche alliant applicatifs de contrôle et formalisation des modes opératoires a été initialisée de manière équilibrée,

une absence de synergie apparaît dans la plupart des cas entre les différents acteurs du contrôle interne (Responsable Exploitation, Responsable Réseau, Responsable micros et réseau local, Responsable Système, D.I.A.C., R.S.S.I., ...) au sein du CTI,

les applications nationales n'incluent pas ou insuffisamment les contrôles automatisés de base qui permettraient aux Directeurs et aux Agents Comptables de remplir leurs obligations inscrites au décret du 10 août 1993 (équations de contrôle des flux en nombre et en montant, par exemple), ce qui favorise l'émergence d'applicatifs locaux.

Ces remarques ont une portée générale et peuvent ne pas concerner chacun des C.T.I. dont les travaux ont fait l'objet d'une exploitation. En effet dans certains sites et pour certains cas analysés dans le cadre du dispositif de contrôle interne, les observations précédemment énoncées ne sont pas justifiées puisque, au contraire, on remarque des liens établis parfaitement entre les différentes structures, une appropriation par les différents acteurs des principes de contrôle interne et une efficacité réelle des résultats.

Ainsi s'il est nécessaire de refonder le dispositif de contrôle interne en fonction des enseignements tirés sur le passé proche, il n'en demeure pas moins qu'il ne faut pas nier les avancées déjà effectuées et remettre en cause les orientations initiales contenues dans l'instruction de contrôle interne du 27 novembre 1995.

2 - LA DEFINITION D'UN SOCLE COMMUN ET A MINIMA POUR LE PLAN D'ACTIONS 1998-99

21 - Objectifs de contrôle interne a minima pour Juin 1999

La diversité d'approche et de résultat des travaux réalisés depuis deux ans dans le cadre du plan de contrôle interne conduit à définir un socle de base des objectifs à atteindre à la fin du mois de juin 1999.

Ce socle de base est la garantie que chaque CTI contribue à assurer un niveau de qualité et de sécurité face aux risques de toute nature encourus par l'Assurance Maladie en matière de systèmes d'information.

Il ne se substitue pas aux actions qui ont été programmées par chaque CTI pour les années 1998-99, pour répondre par ordre de priorité aux risques détectés dans leur propre environnement. Si pour des raisons de faisabilité, le plan d'actions du CTI était modifié afin d'assurer la réalisation du socle d'actions a minima, la nouvelle version devrait être renvoyée à la Caisse Nationale.

Le socle d'actions à réaliser a minima comprend pour juin 1999 :

Thème "RESEAUX" :

Audit des procédures existantes et formalisation des modes opératoires pour les sous-thèmes :

Contrôle des accès au réseau

Administration du réseau

En particulier les modes opératoires réalisés comprennent les modalités de supervision et de contrôle, de façon à s'assurer de l'efficacité des dispositifs, ainsi qu'une cartographie à jour issue d'un logiciel d'administration pilotant le réseau.

Thème transversal "GESTION DES INCIDENTS" QUELLE QUE SOIT LEUR ORIGINE

La gestion des incidents a été identifiée comme l'une des missions du DIAC dans la fiche emploi validée par le CTGI.

L'apport d'outils de reporting est certes important, mais la gestion des incidents repose d'abord sur une évolution de leur prise en compte.

Aussi une gestion centralisée des incidents, d'actions correctives et de communication, doit être mise en place. Le Directeur et l'Agent Comptable doivent disposer d'un tableau de bord quotidien indiquant les incidents et les actions effectuées.

Une gestion centralisée ne peut être efficace que si elle représente une aide aux intervenants du CTI et non pas seulement une contrainte ; aussi les modes opératoires doivent-ils permettre à chaque intervenant de disposer de consignes formalisées sur lesquelles appuyer ses actions.

Thème "CONTROLE DES TRAITEMENTS" :

Evaluation des procédures existantes, formalisation de nouveaux modes opératoires, avec éventuellement utilisation d'une application locale, portant sur :

Contrôle du noyau " Paiements " en nombre et en montant

Les différentes sources d'information existantes (utilisation du gestionnaire de compteurs CEP, utilisation d'outils comme CASE,...) servent à comparer les entrées et les sorties de la chaîne PM en nombre et en montant.

Exemple d'un contrôle en nombre:

Nombre d'enregistrements lus = Nombre d'enregistrements traités,
et exemple de contrôles inter-programmes

Nombre d'enregistrements en sortie = Nombre d'enregistrements en entrée
(éventuellement de plusieurs applications)

Exemple d'un contrôle en montant, celui de la journée comptable:

(Flux LASER (PRELLE)+ Flux IRIS PPNA + Flux IRIS externes + Flux V1 + Flux INVA + Flux Rentes + Libération Flux en Instancier Tiers) = (Titres et Valeurs + Dettes + Mise en Instance Tiers)

Thèmes "SECURITE DES DEVELOPPEMENTS ET DE L'EXPLOITATION" :

Cloisonnement des environnements d'Intégration et d'Exploitation

Pour ce sous-thème, l'objectif est de s'assurer que les mesures déjà prises pour cloisonner les environnements, y compris pour les procédures de "reprise à chaud" en cas d'incident, sont toujours efficaces (audit). Si une mise à jour s'avère nécessaire, l'adaptation des modes opératoires de cloisonnement s'effectue en tenant compte de l'évolution du contexte de travail (par exemple moins d'applicatifs locaux à maintenir), de celle des techniques de sécurisation, et des difficultés éventuellement rencontrées dans l'application au quotidien des consignes précédentes.

Thème "CONTINUITE DE L'ACTIVITE" :

Plan de secours réseau, production, gestion du risque

Le plan de secours doit être formalisé pour ces trois domaines. Les procédures de back-up sont toutes testées au moins une fois par an (Convention avec le Centre National de Secours) et mises à jour, l'intégrité et l'exhaustivité des sauvegardes étant vérifiées à cette occasion.

Protocole d'accord C.T.I./CPAM :

Signature du protocole d'accord C.T.I./CPAM avec ses annexes

En fonction des évolutions survenues depuis la première rédaction du protocole et de ses annexes, leur contenu est revu et proposé au Comité de Direction du CTI.

Les modes opératoires comprennent des dispositifs de supervision et de contrôle.

22 - Organisation

Le contrôle interne et la sécurité se positionnent dans le cadre de la maîtrise des risques. Le Directeur et l'Agent Comptable ont dans ces domaines des responsabilités communes.

L'analyse des actions prioritaires prévues dans les plans pluriannuels des CTI pour répondre aux risques encourus montre que l'effort à fournir justifie qu'en phase de montée en charge du P.C.I., le R.S.S.I. et le D.I.A.C. occupent leur fonction à temps complet et qu'ils puissent compter sur le concours de l'encadrement du CTI.

Les outils informatiques diffusés nationalement sont à mettre en oeuvre dans le cadre de la constitution du socle de base.

3 - LES DISPOSITIONS DE L'INSTRUCTION DE CONTROLE INTERNE DU 27 NOVEMBRE 1995

Les dispositions de l'instruction de contrôle interne du 27 novembre 1995 demeurent en vigueur.

**Le Directeur de l'Informatique et des
Systèmes d'Information**

Robert GRANDI

L'Agent Comptable

Alain BOUREZ