CRCC
COMPAGNIE
REGIONALE DES
COMMISSAIRES AUX
COMPTES
PARIS

AUDIT INFORMATIQUE : TOUS CONCERNÉS !

10 FICHES PRATIQUES POUR RÉUSSIR

ÉDITO

VERS UN CAC 2.0 ?

La révolution numérique provoque des nombreux bouleversements au sein de la société, transformant nos rapports entre citoyens, consommateurs, et dans la vie des entreprises. Avec elle, sont apparus des risques nouveaux liés au traitement de masse des données via le Big Data, sans parler de la cybercriminalité qui sévit au quotidien auprès de tous les utilisateurs d'internet, quel que soit leur qualité ou leur taille. Mais elle est également synonyme de l'avènement de nouveaux droits, à commencer par ceux protégeant les données personnelles.

Autant de sujets qui ont un impact sur notre mission de commissaire aux comptes dans le cadre de l'analyse des risques, socle de notre rôle au sein des entités auprès desquelles nous intervenons.

Devenu un sujet d'enjeu stratégique pour toutes les entreprises, de la TPE à la société dont les titres sont cotés, la sécurité et la pérennité des systèmes d'information d'une entreprise poussent le CAC à repenser sa mission.

Celle-ci évolue donc pour aller vers un traitement des informations financières de plus en plus pointu et important en termes de volumétrie.

Si vous lisez cet édito, c'est que vous êtes déjà convaincu(e) que cette évolution est une réelle opportunité pour notre profession.

Une montée en compétences techniques ? Oui, cela va sans dire ! Mais là où réside réellement cette nouvelle opportunité, c'est dans notre relation avec le chef d'entreprise.

En effet, maitriser ou, a minima, savoir appréhender les questions relatives aux risques dans les systèmes d'informations renforce la plus-value de notre rôle face au dirigeant.

C'est sous cet angle que le présent outil a été pensé : un guide d'entretien pour aider votre client à réfléchir à son système d'information. Dans les structures ayant un directeur des SI, il vous permettra d'être un interlocuteur privilégié auprès de ce spécialiste de la donnée.

Si l'objectif de cet outil n'est pas de vous transformer en spécialiste de l'audit des SI, il a néanmoins la vocation, qui nous est chère, de faire de vous des généralistes éclairés et vous démontrer que l'audit informatique peut être à la portée de tous les professionnels.

Conçu en partenariat avec l'association française de l'audit et du conseil informatiques (AFAI), ce guide d'entretien est accompagné d'un glossaire que vous trouverez en fin de document, car toute maitrise technique commence par la maitrise de son vocabulaire.

Bien confraternellement,

Jean-Luc Flabeau,
président de la CRCC de Paris

CRCC DE PARIS - JUIN 2017
CONCEPTION GRAPHIQUE : ELÉONORE DE BEAUMONT
IMPRESSION : COMPÉDIT BEAUREGARD

GROUPE DE TRAVAIL AUDIT INFORMATIQUE DE LA CRCC DE PARIS

FRÉDÉRIC BURBAND

SERGE YABLONSKY

MATHIEU BARRET

ALEXANDRE BERCOVY

STÉPHANIE BENZAQUINE

VIRGINIE BOESCH

ANNE DEFRENNE

JEAN-MICHEL DENYS

CHRISTIAN GABENESCH

XAVIER GROSLIN

JÉRÔME HUBER

JEAN-PHILIPPE ISEMANN

MICHEL RETOURNÉ

MERCI

NOUS ADRESSONS NOS PLUS SINCÈRES REMERCIEMENTS AUX CO PRÉSIDENTS DU GROUPE DE TRAVAIL AUDIT INFORMATIQUE DE LA CRCC DE PARIS :

Frédéric Burband
Vice-président de la CRCC de Paris, Saint-Honoré Partenaires

Serge Yablonsky
Expert-comptable, commissaire aux comptes, président d'honneur de l'AFAI et co président du GT Audit informatique de la CRCC de Paris

AINSI QU'AUX MEMBRES QUI ONT CONTRIBUÉ À LA RÉDACTION DE CE GUIDE :

Mathieu Barret
Associé BMS Conseil, spécialisé dans les missions de conseil et d'audit informatisé du FEC

Alexandre Bercovy
Directeur chez Deloitte Risk Advisory IS

Stéphanie Benzaquine
Associée Mazars, Risk Advisory Securing Financial & IT Processes

Virginie Boesch
Directrice de mission, cabinet Exponens

Anne Defrenne
Directrice Risk Consulting, cabinet Exponens

Jean-Michel Denys
Managing Partner des activités de Consulting du cabinet CTF, Compagnie des Techniques Financières

Christian Gabenesch
DSI cabinet FIDELIANCE et auditeur des systèmes d'information

Xavier Groslin
Expert-comptable, commissaire aux comptes, Saint Honoré Partenaires

Jérôme Huber
Associé Mazars, spécialisé dans les missions de conseil et d'audit en Système d'Information

Jean-Philippe Isemann
Associé RSM, responsable de l'offre IT & Risk Advisory

Michel Retourné
Expert-Comptable, Directeur Régional Expertise, Sémaphores Expertise

RETROUVEZ LES MEMBRES DU GT ET POSEZ LEUR TOUTES VOS QUESTIONS SUR LE GROUPE DE CONVERSATION « AUDIT INFORMATIQUE, TOUS CONCERNÉS ! »

INTRODUCTION
AUDIT INFORMATIQUE, TOUS CONCERNÉS !

L'audit va disparaître… Nous parlons bien entendu de l'audit traditionnel, le papier crayon, qui subsiste encore chez certains de nos confrères mais dont les centaines de milliers de données manipulées par les entreprises leur mènent la vie dure.
Notre profession se doit d'évoluer pour continuer à accompagner les entreprises de plus en plus informatisées et conserver le contrôle des données financières analysées dans un contexte de cas de fraude en croissance permanente. Après une série de conférences et formations sur le rôle du commissaire aux comptes dans la lutte anti-fraude organisées entre 2015 et 2016, la CRCC de Paris, sous l'impulsion de Frédéric Burband, vice-président, a décidé de créer le **groupe de travail "Audit informatique"**, en partenariat avec l'AFAI, qui rassemble des **spécialistes du contrôle interne informatique et de l'analyse de données informatiques.**

POURQUOI UN GROUPE DE TRAVAIL SUR L'AUDIT INFORMATIQUE ?

Notre objectif est d'**expliquer,** de **sensibiliser** et de **convaincre nos confrères** que l'**utilisation d'outils de data mining** (ou analyses de données) dans le cadre de leur mission est un **gage d'excellence pour notre profession**, de sécurisation de leur mission et une réponse efficace aux besoins des entreprises que nous accompagnons.

Par ailleurs, il est également nécessaire de les **sensibiliser au fait que la digitalisation des processus de l'entreprise est source de risques** de perte de continuité d'activité ou encore de perte d'intégrité des données si celles-ci ne sont pas suffisamment sécurisées : soit parce que les accès aux systèmes sont trop étendus, soit parce que les programmes informatiques peuvent être modifiés sans contrôle en amont. **La transition numérique** actuelle lancée par les pouvoirs publics (FEC, DSN, facture électronique, Chorus…) n'est donc **pas un obstacle, mais bien l'opportunité** pour les professionnels que nous sommes, de donner du poids à nos contrôles.

COMMENT SENSIBILISER LES PROFESSIONNELS ?

Data mining, Data processing, sécurité informatique, FEC, contrôle informatisé…
Un **jargon de plus en plus courant dans nos échanges**, sans pour autant être toujours maitrisé. Le groupe de travail est donc là pour **réfléchir à de nouvelles manières de présenter ces concepts** et de **les rendre accessibles de tous.**

Notre groupe a donc travaillé à l'élaboration de ce recueil de fiches pratiques qui a pour objectif :

- d'**expliquer clairement et simplement** les techniques regroupées sous le terme de data mining
- de **sensibiliser nos confrères à l'intégration des systèmes d'information** dans leur démarche et à l'utilisation de ces techniques lors de leurs missions
- de **détailler les enjeux réglementaires** liés
- d'**apporter des réponses et une méthodologie** applicable directement dans leurs missions

L'AUDIT INFORMATIQUE, CE N'EST DONC PAS QUE POUR LES ETI ET LES GRANDS COMPTES ?

Et bien non. Si nous prenons l'exemple du FEC, le Fichier des Ecritures Comptables, demandé désormais par l'administration fiscale et qui contient l'ensemble des écritures d'une entreprise, il **concerne toutes les entreprises françaises qui tiennent leur comptabilité de manière informatisée**. Il soulève d'ailleurs souvent des questions de la part des entreprises, malheureusement trop tard lorsque le vérificateur s'y intéresse…

QUE FAUT-IL RETENIR DE NOS TRAVAUX ?

Le monde change, les entreprises évoluent, nos méthodes de travail aussi. **Notre groupe de travail est là pour apporter des réponses simples aux interrogations que suscite l'introduction des nouvelles technologies dans nos missions traditionnelles.**
Après une présentation lors d'une formation, le 4 juillet 2017 à la Maison de la chimie, ce recueil de fiches a vocation à être diffusé à l'ensemble des professionnels inscrits à la CRCC de Paris puis consultable librement depuis notre site : **www.crcc-paris.fr**

INTRO

COMMENT UTILISER CE GUIDE ?

Ce guide est un outil opérationnel pour tout commissaire aux comptes pour mesurer le niveau de risques en matière de systèmes d'information et d'ouverture sur le numérique.

EN QUOI EST-CE UN OUTIL OPÉRATIONNEL ?

Au-delà d'une présentation des bonnes pratiques et du rattachement aux NEP concernées, des questionnaires simples permettent au commissaire aux comptes de conduire les entretiens avec son client.
Des références sont aussi fournies pour aller plus loin dans le domaine concerné.

POURQUOI L'UTILISER ?

Pour comprendre l'organisation et l'utilisation de l'informatique et du numérique par l'entreprise et mesurer le niveau de risques afin de décider s'il faut aller plus avant sur un ou plusieurs domaines.

10 DOMAINES ABORDÉS : 10 QUESTIONNAIRES DE CONDUITE D'ENTRETIEN

Il est recommandé d'aborder tous les domaines avec son client. Néanmoins, chaque fiche et chaque questionnaire peut être utilisé indépendamment.
Des versions Word des fiches seront téléchargeables sur le site de la CRCC de Paris.

STRUCTURE DU GUIDE	FICHE	PAGE
GOUVERNANCE D'ENTREPRISE		
Ouverture sur la transformation numérique	**01**	**10**
Gouvernance des systèmes d'information	**02**	**16**
RISQUES OPÉRATIONNELS		
Contrôle des accès	**03**	**26**
Conduite de projets	**04**	**34**
Exploitation des systèmes d'information	**08**	**56**
Plan de continuité d'activité	**09**	**62**
Cybersécurité	**10**	**66**
ACTIVITÉS DE CONTRÔLE		
Utilisation des outils d'audit de données	**05**	**40**
Protection des données personnelles	**06**	**46**
Législation fiscale et SI	**07**	**50**

SOMMAIRE

OUVERTURE SUR LA TRANSFORMATION NUMÉRIQUE

01

FICHE 01
OUVERTURE SUR LA TRANSFORMATION NUMÉRIQUE

CONTEXTE ET ENJEUX

Qu'est-ce que la transformation numérique ? La transformation numérique est la création, l'utilisation et le partage de données numériques en vue de la création de nouveaux services à usage externe ou interne. Elle a impacté les offres aux consommateurs et la culture d'entreprise en modifiant leurs mentalités et leurs processus. L'adaptation à cette évolution digitale est l'une des priorités majeures pour les dirigeants qui veulent que leur entreprise reste compétitive, d'autant que cette révolution ne semble pas ralentir, bien au contraire.

Le numérique s'impose comme un enjeu stratégique majeur pour les entreprises. Pourquoi ? Parce que les implications sont multiples ; elles touchent les offres et les business models, les modes de management, les fonctionnements entre les collaborateurs, les relations avec les clients et les fournisseurs, et les technologies.

Le numérique est souvent comparé à la bulle internet dans l'informatique des années 90. Mais il n'en est rien. Cette fois, l'évolution n'est pas seulement technologique, elle implique de reconsidérer l'ensemble en profondeur : l'homme, sa culture, l'organisation, les processus et les méthodes. Le numérique fait apparaitre de nouvelles questions éthiques touchant le traitement des données personnelles des différentes parties prenantes (origine, transmission, vente, exploitation, transformation, ...) dont les usages ne sont pas toujours prévisibles et contrôlés.
Au-delà des opportunités et des perspectives positives que le numérique apporte, les changements génèrent aussi des risques nouveaux pour l'entreprise.

NEP ET TEXTES DE RÉFÉRENCE

- NEP 315 : Connaissance de l'entité et de son environnement et évaluation du risque d'anomalies significatives.
- Doctrine professionnelle relative aux prestations entrant dans le cadre de diligences de commissaire aux comptes rendu lors de l'acquisition d'entité (ex NEP 9060).
- Doctrine professionnelle relative aux prestations entrant dans le cadre de diligences de commissaire aux comptes rendu lors de la cession d'entreprise (ex NEP 9070).

FICHE 01
OUVERTURE SUR LA TRANSFORMATION NUMÉRIQUE

ANALYSE DES RISQUES ET CRITICITÉ

Les enjeux sont multiples :

Economique : Depuis l'an 2000, plus d'une entreprise sur deux du classement Fortune 500 a disparu ou a fait faillite.
La condition sine qua non de mener à bien sa transformation numérique réside dans l'engagement indéfectible du Dirigeant et de ses premières lignes.
La mesure de la performance doit être évaluée de façon globale y compris sur la transformation numérique de l'entreprise.

Stratégique : Le numérique n'est pas un effet de mode. Il doit être utilisé comme le moyen de redéfinir l'offre et l'organisation, et donc de piloter l'entreprise autrement et plus efficacement dans l'économie d'aujourd'hui. Le numérique est au service de la stratégie de l'entreprise.

Concurrentiel : Sur de nombreux secteurs, la mise en place d'une aide robotisée, la mise en place d'objets connectés, la meilleure connaissance des clients par la « data » permettent d'augmenter la compétitivité des entreprises et de mieux contribuer à son écosystème.
Ce constat est important, car la bataille du rapport qualité/prix touche désormais tous les secteurs (même nos secteurs de professionnels du chiffre) et devient une obligation cruciale pour la survie des entreprises.

Écologique : L'empreinte écologique fait désormais partie de notre quotidien, tant sur le plan personnel que professionnel. L'action écologique ne se limite donc plus au tri des déchets ménagers mais à la définition au sein même des entreprises d'une véritable stratégie prenant en compte la dimension écologique. Cette dimension impacte les nouvelles réglementations qui permettent désormais :
• De stocker des justificatifs sous un format électronique sécurisé plutôt que la version papier ;
• De fournir une comptabilité dématérialisée en cas de contrôle ;
• D'envoyer des factures dématérialisées plutôt que par courrier ;
• Etc...

Ces évolutions ne peuvent pas être négligées car elles nécessitent une transformation de la culture des entreprises mais également des approches de travail plus collaboratives. Elles ne peuvent donc pas se conduire en quelques mois et doivent s'inscrire durablement dans la stratégie de chaque entreprise.

Les facteurs clefs de criticité qui en ressortent sont les suivants :

Certaines entreprises sont nées de cette révolution numérique et sont devenues des leaders (Google, Apple, Facebook, Amazon) et d'autres ont su se transformer (Accor, Michelin...). D'autres, en revanche, n'ont pas réussi à prendre le virage du numérique (NOKIA, KODAK...).
En tant que dirigeants, les impacts liés à cette transformation doivent être anticipés et maitrisés et les investissements nécessaires réalisés.

Cette approche pousse à décomposer l'analyse de la performance par différents angles :

› Comment déployer le numérique en tenant compte de la réalité du terrain ? Comment anticiper les nouvelles tendances sur son marché ? Les projets numériques sont-ils bien en prise avec les dernières innovations ?

› Comment l'entreprise intègre-t-elle les évolutions de son environnement dans son organisation ? La veille sur les évolutions technologiques est cruciale, car elle évite les décalages.

› Quels sont les impacts des décisions sur l'environnement et sur l'ensemble des parties prenantes ? Le numérique redistribue la valeur économique en se concentrant davantage sur le service rendu au client final.

› Quelles sont les mesures prises pour s'assurer que les offres de l'entreprise collent aux attentes de ses clients ?

› Comment sont mesurées les performances opérationnelles des différentes lignes de produits et services ?

FICHE 01
OUVERTURE SUR LA TRANSFORMATION NUMÉRIQUE

QUESTIONNAIRE

(Source : cahier 33 Mesure globale de la performance durable www.lacademie.info)

Thème / Question	Enjeu / Risque associé	Interlocuteur concerné	Réponse attendue
L'entreprise a-t-elle mis en place un projet de transformation numérique dans les deux dernières années ?	Continuité d'exploitation	Le DG, le marketing, la DSI, la DRH, la DAF	OUI - Mobilité - Vente multi canal (clic and collect)
Est-ce que l'entreprise a étudié les opportunités en matière de marketing, de connaissance de ses clients, de création de nouveaux services, de changement de Business Model, d'amélioration des processus de production et de logistique ?	Continuité d'exploitation	Le DG, le marketing, la DSI, la DRH, la DAF	OUI - Objets connectés - Réseaux sociaux
L'entreprise est-elle accompagnée dans ses projets de transformation par des experts/ consultants ?	Fiabilité des données Conformité	DG	OUI
Les responsables opérationnels ont-ils compris les enjeux et les contraintes du numérique ? (nouveautés, changements de relation inter-personnelles, rythme des évolutions , ...)	Continuité d'activité	DG	OUI - Utilisation des outils collaboratifs - MOOC
L'informatique numérique dispose-t-elle de ressources spécifiques, en termes de finance, de gestion de la complexité, de maitrise de l'agilité et des interactions, d'équipes ?	Continuité d'activité	Le DG, la DSI, Chief Digital Officer	OUI - Méthodes agiles - Budget d'investissement - Pizza team
Le parcours numérique du client est-il au cœur du pilotage de la performance opérationnelle (CRM,...) ?	–	Le DG, la DSI	OUI - Mise en place du Big Data / Analytics
L'accès, la transformation et la diffusion des données personnelles sont-ils pris en compte dans les projets numériques ?	–	Le DG, la DSI	OUI - Application GDPR (cf. fiche données personnelles)
La culture de l'entreprise est-elle propice à la transformation numérique ?	–	Le DG, la DSI	OUI - Bureau dynamique - Innovation favorisée
Les évolutions numériques intègrent-elles les exigences de gestion des risques, de contrôle et d'audit en lien avec les pratiques réglementaires et éthiques ?	–	Le DG, La DSI	OUI - Plan d'audit sur les projets de transformation numérique
Les nouvelles pratiques commerciales numériques sont-elles revues systématiquement en tenant compte des circuits multicanaux, de l'intégration des réseaux sociaux et du Big Data ?	–	Le DG, La DSI	OUI - Guidage du parcours clients - Proposition d'achats sur les plateformes
L'entreprise dispose-t-elle d'un plan d'intégration des technologies dont elle aura besoin pour anticiper les évolutions de son marché et se différencier de la concurrence (celui-ci peut passer par des start-up, des équipes projets, des experts externes,...)	–	Le DG, La DSI	OUI - Mise en place d'API - Schéma directeur technique - Open innovation
Les processus sont-ils documentés et partagés au niveau de la Direction Générale et des décideurs opérationnels en charge de l'offre et s'ajustent-ils avec l'environnement grâce au numérique ?	–	Le DG, La DSI	OUI - Cartographie des processus – approche transversale Culture projet
Le numérique développe-t-il une capacité nouvelle de suivi des objectifs de qualité, coûts, délais (agilité, vélocité ...) des produits et services ?	–	Le DG, la DSI	OUI - Dashboarding - Données de workflow - Objets connectés
Le numérique améliore-t-il la gestion de la production, de la distribution et de la personnalisation de l'offre ?	–	–	OUI - RFID - Géolocalisation - Drive dans la grande distribution Impression 3D

POUR ALLER PLUS LOIN

Bibliographie :

• L'Académie des sciences et techniques comptables : Cahier 33 Mesure globale de la performance durable
• La revue fiduciaire comptable n° 450, juin 2017, La maturité « numérique » : signe de la performance de l'entreprise

GOUVERNANCE DES SYSTÈMES D'INFORMATION

02

FICHE 02
GOUVERNANCE DES SYSTÈMES D'INFORMATION

Pourquoi parler de gouvernance des systèmes d'information (SI) ? Parce qu'à une époque où les systèmes d'information sont omniprésents et de plus en plus automatisés, leur alignement avec les objectifs, l'organisation et les process de l'entreprise, est un indicateur clé, voire le garant, de la fiabilité de l'information et en particulier de l'information comptable et financière.

La gouvernance des SI recouvre de multiples dimensions.
Dans une perspective d'audit, nous en avons retenu ici quatre :

LES RÔLES ET RESPONSABILITÉS VIS-À-VIS DU SI
LA GOUVERNANCE DES DONNÉES
LE CONTRÔLE INTERNE DES SI
LA COUVERTURE ET LA COHÉRENCE DU SYSTÈME D'INFORMATION

LA COUVERTURE ET LA COHÉRENCE DU SYSTÈME D'INFORMATION

RÔLES & RESPONSABILITÉS

CONTEXTE ET ENJEUX

La répartition des rôles dans l'organisation et le pilotage du système d'information est un sujet crucial au sein des organisations dans la mesure où elle conditionne la bonne maîtrise de l'information qui est produite.
Comprendre les différentes fonctions de management des opérations liées aux applications est un point central de l'appréhension des risques, constitutif de l'information comptable et financière.

NEP ET TEXTES DE RÉFÉRENCE

- NEP 315 : Connaissance de l'entité et de son environnement et évaluation du risque d'anomalies significatives

FICHE 02
GOUVERNANCE DES SYSTÈMES D'INFORMATION

ANALYSE DES RISQUES ET CRITICITÉ

Le management des systèmes d'information fait partie intégrante du management de l'entreprise. C'est l'une des composantes de la gouvernance des SI.
De manière globale, la direction générale est la propriétaire du système d'information et doit s'assurer du bon fonctionnement de celui-ci mais aussi de sa pérennité et ce compris de sa bonne évolution et de sa sécurité.
Au regard des risques comptables et financiers, c'est le DAF qui porte in fine la responsabilité de la validité et de l'exhaustivité de l'information produite quelle que soit l'assertion. Il revient cependant à chaque propriétaire d'application ou de données, qu'il s'agisse de fonction métier ou transverse, de veiller à la disponibilité de l'information produite.

Afin de bien distinguer les deux fonctions :

- Les propriétaires d'applications sont responsables du correct fonctionnement de l'application, de l'adéquation aux besoins métiers et de la continuité d'exploitation.
- Les propriétaires de données sont responsables de l'autorisation des accès, de l'exactitude des traitements, de l'intégrité des données et de leur disponibilité.

La distinction entre les deux fonctions n'impose pas une stricte séparation entre les deux rôles de responsables d'application et de responsable de données. Il convient en revanche que l'auditeur identifie bien l'attribution de l'ensemble des rôles pour chaque application et chaque donnée, surtout dans le cadre d'organisation matricielle.

De fait, les principaux enjeux et risques associés sont :

Chaque acteur doit être identifié en lien avec ses attributions réelles afin d'appréhender correctement les risques liés au système d'information.

Les opérations, les risques et les contrôles associés doivent être rattachés à des acteurs dûment nommés afin de ne pas laisser d'inconnue ou de « trous » dans le système de contrôle interne.

En cas d'incertitude, une absence de contrôle ou une prise de décision inappropriée pourrait venir mettre en péril la chaîne de production de l'information comptable et financière.

Par ailleurs, la bonne identification des rôles et responsabilités est indispensable à l'attribution des actions de surveillance et/ou de sécurisation dans le cadre du processus d'amélioration continue.

QUESTIONNAIRE

A. ORGANISATION ET PILOTAGE

Thème / Question	Enjeu / Risque associé	Interlocuteur cible	Réponse attendue	Phase d'audit
Un organigramme de la fonction informatique est-il formalisé et actualisé de manière régulière ?	Connaissance des parties prenantes afin d'apprécier la maîtrise de : • Rôles et responsabilités des actions et des contrôles • Séparation des tâches	DSI	OUI	Intérim
Le management de la fonction informatique est attribué à une personne dédiée ?	• Centralisation des décisions en lien avec la stratégie de l'entreprise • Mise en place de points de contrôle et de reporting par la direction	DG	OUI	Intérim
Si oui, à qui est rattachée hiérarchiquement cette personne ?	Identification du niveau de contrôle	DG	DG	Intérim
Un responsable de la sécurité informatique est nommé au sein de l'organisation ?	Maîtrise et coordination des actions de sensibilisation et de surveillance de la sécurité de l'information	DG	Comité d'audit ; audit interne ; DG	Intérim
Le directeur financier a défini des points de contrôle permettant de superviser la production de l'information comptable et financière ?	Apprécier le niveau de maîtrise du système d'information par le directeur financier	DAF	OUI	Intérim

B. MANAGEMENT ET RESPONSABILITÉ

Thème / Question	Enjeu / Risque associé	Interlocuteur cible	Réponse attendue	Phase d'audit
Les fiches de poste des collaborateurs en charge de la fonction informatique sont-elles formalisées ?	Maîtrise des RACI Principe de non-répudiation renforcée	DRH	OUI	Intérim
Les fiches de postes des managers précisent-elles leur responsabilité relative au système d'information ?	Maîtrise des RACI Principe de non-répudiation renforcée	DRH	OUI	Intérim
Pour chaque application, un responsable d'application est-il nommé ?	Maîtrise du fonctionnement des applications et de leur évolution	DAF, DSI, DG, Direction métier	OUI	Intérim
Pour chaque donnée critique, un propriétaire de données est-il nommé ?	Maîtrise des inventaires, des flux et des traitements de données	DAF, DSI, DG, Direction métier	OUI	Intérim

FICHE 02
GOUVERNANCE DES SYSTÈMES D'INFORMATION

GOUVERNANCE DES DONNÉES

Pourquoi parler de gouvernance des données ? Parce que tout est donnée ! Toute entreprise, indépendamment de sa taille, de son activité ou de son volume d'affaires, s'appuie sur un SI. Son activité économique est traduite comptablement en enregistrant des transactions dans des livres comptables informatisés.

Raisonner donnée !

CONTEXTE ET ENJEUX

Toute information enregistrée sur un support numérique est composée de données.
Les données peuvent être regroupées en deux grandes familles :

- Les données **référentielles** : clients, fournisseurs, plan comptable, nomenclature, etc.
- Les données **transactionnelles** : factures, devis, bons de commandes, etc.

A l'échelle de l'entreprise, chaque type de donnée doit être identifiée, enregistrée et mise à jour de manière unique et adéquate en regard de l'activité.

Les données peuvent être stockées sur des serveurs possédés et/ou hébergés par l'entreprise, ou bien à l'extérieur, comme dans le cas du SaaS ou du cloud. Dans ces cas, il convient de contrôler les dispositions de conformité et/ou les dispositions contractuelles.

NEP ET TEXTES DE RÉFÉRENCE

- NEP 315 : Connaissance de l'entité et de son environnement et évaluation du risque d'anomalies significatives
- NEP 330 : Procédures d'audit mises en œuvre par le commissaire aux comptes à l'issue de son évaluation des risques
- Doctrine professionnelle relative aux consultations entrant dans le cadre de diligences directement liées à la mission de commissaire aux comptes portant sur le contrôle interne relatif à l'élaboration et au traitement de l'information comptable (ex NEP 9080)

ANALYSE DES RISQUES ET CRITICITÉ

Une gouvernance des données pas ou mal définie a des conséquences directes sur la fiabilité des données : référentiels clients, fournisseurs, comptables incohérents, incomplets, redondants, nomenclatures multiples, identifiants manquants, silotage entre applications, problèmes d'interfaces… La piste d'audit est directement impactée lorsque les données référentielles ne sont pas sous une responsabilité unique et mise à jour en fonction des besoins opérationnels ou règlementaires.

QUESTIONNAIRE

Thème / Question	Enjeu / Risque associé	Interlocuteur cible	Réponse attendue
Les référentiels inclus dans le périmètre de l'audit sont-ils uniques ?	Fiabilité et intégrité des données auditées. Ex. : fiche client en doublon	Personne en charge > identifier selon la taille et l'activité de l'entreprise : DSI, DAF, DG, autre…	OUI
Qui est habilité à créer, supprimer, mettre à jour les données référentielles (création d'un nouveau fournisseur, modification d'une fiche client, etc.) ?	• Fiabilité et intégrité des données • Risque de fraude si la SOD n'est pas respectée		Un nombre limité d'utilisateurs fonctionnels (mais pas un individu unique)
Qui valide les spécifications lors d'un projet (changement de logiciel comptable par exemple) ? Comment sont formalisées ces spécifications ?	• Exhaustivité • Fiabilité Ex : reprise de données		DAF
Cette responsabilité est-elle formalisée dans une charte ou une politique d'entreprise ?	Fiabilité des données si les rôles et responsabilités ne sont pas définis et/ou communiqués, ce qui introduit de l'ambigüité > nécessité d'un RACI	La DG doit être impliquée sur ce point, quelle que soit la taille et l'activité de l'entreprise	OUI
Existe-t-il un registre de classification des données ?	• Exhaustivité (plan de continuité d'activité) • Conformité • Ex. : quelles données sauvegarder, archiver et restaurer en priorité ?	Responsables métiers	OUI
Le logiciel comptable est-il hébergé en interne ou bien est-il géré par un tiers, voire dans le cloud ?	• Disponibilité des données • Conformité • Ex. : clause d'auditabilité		Selon cas
Si le logiciel est géré par un tiers, les dispositions contractuelles prévoient-elles les conditions de mise à disposition des données ?	• Disponibilité des données • Conformité • Ex. : clause d'auditabilité		OUI
Ces dispositions sont-elles testées et mesurées régulièrement ?	• Disponibilité des données • Conformité • Ex. : clause d'auditabilité		OUI
Y a-t-il un projet GDPR dans l'entreprise ?	Conformité		OUI
Quelles sont les dispositions en matière de sécurisation des données ? Sont-elles testées et à quelle fréquence ?	• Exhaustivité • Fiabilité • Risque de fraude		OUI

FICHE 02
GOUVERNANCE DES SYSTÈMES D'INFORMATION

CONTRÔLE INTERNE DES SI

CONTEXTE ET ENJEUX

Le contrôle interne propre aux SI est appelé contrôles généraux informatiques (ITGC ou Information Technology General Controls en anglais). Ces contrôles sont regroupés en six familles principales qui couvrent le cycle de vie de la donnée.

- La gestion des accès : infrastructure, applications, et donnée,
- Le cycle de développement applicatif,
- La maintenance évolutive et corrective,
- La sécurité physique des Data centers,
- Les procédures de sauvegardes et de restauration
- Les contrôles liés à l'exploitation : réseau, OS, bases de données, mise en production

Dans le cadre des travaux de vérification, il est indispensable de considérer ces dimensions car le niveau de risque et de sécurisation a un impact direct sur la fiabilité et l'exhaustivité des données financières.

NEP ET TEXTES DE RÉFÉRENCE

- NEP 315 : Connaissance de l'entité et de son environnement et évaluation du risque d'anomalies significatives
- NEP 330 : Procédures d'audit mises en œuvre par le commissaire aux comptes à l'issue de son évaluation des risques
- Doctrine professionnelle relative aux consultations entrant dans le cadre de diligences directement liées à la mission de commissaire aux comptes portant sur le contrôle interne relatif à l'élaboration et au traitement de l'information comptable (ex NEP 9080)

ANALYSE DE RISQUES ET CRITICITÉ

Un système d'information qui n'est pas suffisamment sécurisé est exposé à plusieurs risques :

- Non-respect de la SOD
- Altération, modification de données et fraude
- Non-conformité
- Cyber attaque

EXEMPLES

• **SOD :** capacité à générer un ordre d'achat et à le valider, ou saisie d'une facture fournisseur et validation du paiement associé

• **Modification non tracée d'une séquence de code en RPG** (AS/400) qui modifie la règle de calcul sur une dépréciation de stock.

• **GDPR :** non respect des dispositions légales présentes et à venir

• **Perte de données financières ou demande de rançon liées à une attaque**

QUESTIONNAIRE

Thème / Question	Enjeu / Risque associé	Interlocuteur cible	Réponse attendue
Existe-t-il une matrice de définition des rôles utilisateurs dans l'entreprise ?	Séparation des fonctions	DSI	OUI
Les autorisations d'accès font-elles l'objet de revues qualitative et quantitative ?	Analyse des comportements des utilisateurs dans le cadre de la prévention des fraudes	DSI	OUI
Les demandes d'évolution sur le SI financier sont-elles tracées ? Si oui, comment ? Quel est le processus de validation ?	Vérification des autorisations accordées en lien avec chaque modification pour prévenir l'introduction de biais dans les applications	DSI	OUI
Qui met en production les développements ? Suivant quelle procédure ?	Revue des rôles et responsabilités en lien avec la surveillance du respect de la séparation des fonctions	DSI	OUI
Les procédures de sauvegarde sont-elles formalisées ? Si cloud, les clauses contractuelles sont-elles conformes aux besoins de l'entreprise (RPO, RTO) ?	Garantie de reprise et de continuité d'activité	DSI et DAF	OUI
Des tests de restauration sont-ils menés ? Sur quel périmètre, avec quelles parties prenantes et avec quelle fréquence ?	Garantie de reprise et de continuité d'activité	DSI et DAF	OUI

COUVERTURE ET COHÉRENCE DU SYSTÈME D'INFORMATION

CONTEXTE ET ENJEUX

Le système d'information est l'épine dorsale de l'activité de l'entreprise dans la mesure où il supporte tout ou partie des processus métier et de gestion.
Il est de fait indispensable de bien connaitre les zones de couverture du SI et les liens entre chacune des applications. Cette connaissance doit également être mesurée auprès du management de l'entreprise.
Les risques ainsi supportés par chaque zone du SI permettront d'identifier en amont les principaux flux constitutifs de l'information comptable et financière.

NEP ET TEXTES DE RÉFÉRENCE

- NEP 315 : Connaissance de l'entité et de son environnement et évaluation du risque d'anomalies significatives

FICHE 02
GOUVERNANCE DES SYSTÈMES D'INFORMATION

ANALYSE DE RISQUES ET CRITICITÉ

Chaque processus de l'entreprise est traductible en information qui doit soit répondre à des besoins de pilotage soit traduire la réalité économique.
Afin de bien comprendre le cheminement de l'information et les traitements qu'elle subit, il est indispensable de bien recenser les différentes applications et de les rattacher à chaque processus ou sous-processus.

Par ailleurs, les dites applications sont également plus ou moins interconnectées (ou interfacées) laissant soit des zones de transfert et/ou de transformation des données, soit des zones de ruptures nécessitant des opérations de ressaisies manuelles.

QUESTIONNAIRE

Thème / Question	Enjeu / Risque associé	Interlo-cuteur cible	Réponse attendue	Phase d'audit
A. Composantes du SI Le système d'information est-il basé sur un ERP ?	• Niveau d'intégration du système d'information • Nombre importants d'interface à contrôler • Exposition à la conta-gion des anomalies en cas de faiblesse de contrôle	Personne en charge > identi-fier selon la taille et l'activité de l'entre-prise : DSI, DAF, DG, autre…	OUI	Intérim
A. Composantes du SI Une dépendance forte existe entre les applications, les choix technologiques et les choix d'infrastructures	• Continuité d'activité et capacité d'évolution du SI	DSI et/ou DAF	OUI	Intérim
A. Composantes du SI Existe-t-il des applications dites « périphé-riques » de type Excel ou Access ?	• Accès aux données : fichiers extra-système peu sécurisés • Intégrité : données et calculs ouverts et non protégés	DSI et/ou DAF	OUI	Intérim
B. Connaissance du SI et couverture fonctionnelle Une cartographie du système d'information est formalisée et maintenue à jour de manière régulière ?	• Connaissance des applications sources et des traitements • Maitrise des risques liés aux évolutions du SI	DSI et/ou DAF	OUI	Intérim
B. Connaissance du SI et couverture fonctionnelle Les flux ayant un impact sur l'information comptable et financière sont identifiés ?	• Connaissance des applications sources et des traitements • Maitrise des risques liés aux évolutions du SI	DSI et/ou DAF	OUI	Intérim
B. Connaissance du SI et couverture fonctionnelle Une matrice de couverture des processus par les applications est renseignée	• Connaissance des applications sources et des traitements • Maitrise des risques liés aux évolutions du SI	DSI et/ou DAF	OUI	Intérim

QUESTIONNAIRE

Thème / Question	Enjeu / Risque associé	Interlo-cuteur cible	Réponse attendue	Phase d'audit
C. Cohérence et évolution du SI Si certains processus ne sont pas couverts par le système d'information, il est envisagé de l'informatiser à court ou moyen terme	• Mise en place de contrôles automatiques et sécurisation des calculs et de l'accès aux données	DSI et/ou DAF	OUI	Intérim
C. Cohérence et évolution du SI Les évolutions métiers sont prises en compte dans le système d'information	• Mise en place de contrôles automatiques et sécurisation des calculs et de l'accès aux données	DSI et/ou DAF	OUI	Intérim
D. Interfaces applicatives Certaines interfaces reposent sur la généra-tion de fichiers de transfert stockés dans des répertoires de travail ?	• Accès au données : Les données sont sécurisées et ne peuvent être accédées ni modifiées dans le cadre de l'interface	DSI et/ou DAF	OUI	Intérim
D. Interfaces applicatives Les interfaces les plus critiques font l'objet de contrôle manuels ou par analyse de données ?	• Intégrité et exhaustivité des données : les données issues des interfaces sont complètes et n'ont pu être corrompues	DSI et/ou DAF	OUI	Intérim

CONTRÔLE DES ACCÈS

03

FICHE 03
CONTRÔLE DES ACCÈS

CONTEXTE ET ENJEUX

En informatique, le droit d'accès est, d'une façon générale, le droit nécessaire à un utilisateur pour accéder à des ressources : ordinateur, données, imprimante, etc.
Les bonnes pratiques recommandent d'accorder le minimum de droits, en fonction des besoins d'accès des utilisateurs (règle dite du « need to know » ou « besoin de connaître »)
Les droits d'accès visent à :
• garantir une sécurité des actifs (code secret, mot de passe, clés, etc.)
• un niveau de sécurité approprié pour les transactions qui requièrent l'utilisation d'un système d'information (comptabilisation d'une opération, déclenchement d'un paiement, approbation, etc.)

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

POINTS D'ATTENTION PARTICULIERS :

- Faire le lien avec la cartographie des principaux systèmes d'information qui concourent à la construction des états financiers (logiciels comptables, logiciels de gestion, logiciels métier)
- Prendre en considération l'existence d'un environnement informatique ouvert (ERP)
- Tenir compte de la volumétrie des transactions et du nombre d'intervenants sur un ou plusieurs cycles
- Prendre en compte l'incompatibilité des fonctions de développement informatique, de tests et d'exploitation.

FICHE 03
CONTRÔLE DES ACCÈS

NEP ET TEXTES DE RÉFÉRENCES

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

ANALYSE DES RISQUES ET CRITICITÉ

DROITS D'ACCÈS ET SÉPARATION DES TÂCHES (SOD)

Le droit d'accès à un actif, une ressource ou un système d'information doit par principe être proportionnel au niveau de responsabilité et à la place dans une organisation hiérarchisée. Il doit par ailleurs prendre en compte l'aspect relatif à la séparation des tâches pour, quel que soit le niveau de droit d'accès autorisé, éviter une situation d'auto-approbation, contraire aux principes élémentaires du contrôle interne.

Pour rappel, les avantages liés à une séparation des tâches satisfaisante résident dans la facilitation de la détection des erreurs (involontaires ou frauduleuses).

Plus l'organisation de l'entité est complexe (flux, SI, sites, etc.), plus la matrice de séparation des tâches est complexe et plus son suivi et sa mise à jour requièrent une volumétrie de travail élevée et régulière dans le temps.

En conséquence, plus le niveau hiérarchique est élevé / important, plus le niveau de droits d'accès est élevé, comme l'illustrent les quelques exemples présentés ci-après pour les principaux cycles.

ILLUSTRATION SUR LE CYCLE DES ACHATS :

Droit d'accès requis	Faible	Moyen	Elevé
Changer un taux de TVA			✓
Déclencher un paiement			✓
Créer / modifier / supprimer un RIB fournisseur			✓
Autoriser un investissement			✓
Passer une commande		✓	
Contrôler une réception		✓	
Comptabiliser une facture		✓	
Lettrer un compte fournisseur		✓	
Saisir une réception	✓		
Scanner une information	✓		

ILLUSTRATION SUR LE CYCLE DES VENTES :

Droit d'accès requis	Faible	Moyen	Elevé
Changer un taux de TVA			✓
Autoriser un avoir / une remise			✓
Créer / modifier / supprimer un RIB client			✓
Créer / modifier / supprimer une fiche produit / article		✓	
Réaliser / contrôler une opération d'encaissement		✓	
Effectuer / contrôler un état de rapprochement bancaire		✓	
Faire une relance client		✓	
Lettrer une balance auxiliaire / balance âgée		✓	
Valider une expédition	✓		

FICHE 03
CONTRÔLE DES ACCÈS

POINTS D'ATTENTION PARTICULIERS :

- Les tâches incompatibles entre elles par nature requièrent de disposer de droits d'accès séparés et/ou distincts.
- Le CAC doit procéder à une appréciation de l'adéquation entre les droits d'accès octroyés et la prise en compte de la séparation des tâches au sein de l'entité. Cette appréciation doit en outre se fonder sur la connaissance acquise de l'environnement de contrôle interne.

Les deux matrices suivantes illustrent les tâches incompatibles entre elles pour le cycle des achats et le cycle des ventes. Elles sont un exemple concret des tâches qui ne doivent pas être réalisées par les mêmes personnes.

Toutefois, l'organisation de l'entité et le jugement professionnel du commissaire aux comptes doit être pris en considération pour adapter ces matrices à l'environnement applicable (NEP 315).

CYCLE DES VENTES

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

CYCLE DES ACHATS

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

RISQUE SIGNIFICATIF
RISQUE MOYEN
RISQUE ACCEPTABLE

DROITS D'ACCÈS ET RISQUE DE FRAUDE (NEP 240)

Pour rappel, la fraude se définit comme une erreur intentionnelle et le CAC, lors des phases de planification et de réalisation de l'audit doit apprécier le risque d'anomalie significative résultant de fraude.

L'environnement informatique, la volumétrie des flux et transactions et tous les éléments du dispositif de contrôle interne sont par essence des éléments qui doivent être pris en compte par le CAC lors de son appréciation du risque de fraude. Quelques exemples de fraude dont l'origine est un dysfonctionnement en termes de droit d'accès à une application informatique :

- Paiement déclenché à tort dans un ERP ayant entraîné une sortie trésorerie significative
- Fraude au Président
- Création d'un salarié fictif / fournisseur fictif dans un système informatique

Les droits d'accès au patrimoine applicatif de l'entité sont une composante essentielle de l'environnement de contrôle interne

Outre le respect de la séparation des fonctions des utilisateurs, une règle essentielle en matière de contrôle interne informatique impose de séparer également strictement les fonctions de développement informatique, de tests et de production.

POINT D'ATTENTION PARTICULIER :

- Le risque associé au non-respect de cette règle serait la création et l'utilisation de fonctions secrètes, connues du concepteur des applications, qui en est également l'utilisateur, et permettant la fraude.

FICHE 03
CONTRÔLE DES ACCÈS

QUESTIONNAIRE

Les points ci-après sont issus, pour la plupart, de la norme ISO27002 (système de gestion de la sécurité de l'information).

Question	Enjeux / Risques associés	Interlocuteur concerné	Réponse attendue
L'organisation auditée a-t-elle documenté sa politique de contrôle d'accès et tient-elle à jour une matrice des autorisations ?	Accès non autorisés, fraudes…	DG	OUI
Concernant la gestion des droits d'accès : - Qui décide de l'attribution / retrait des droits d'accès ? - Qui saisit la création / suppression des droits d'accès ?	Accès non autorisés, fraudes…	DG, DSI	Liste limitée de décideurs et d'opérateurs
Une procédure formelle d'attribution /retrait des droits d'accès par utilisateur est-elle définie, avec circulation d'informations entre les services concernés ?	Accès non autorisés, fraudes…	DG, DSI, chefs de services	OUI
L'attribution des droits d'accès se fait elle par : - Aucun accès sauf autorisations explicites Ou - Accès à tout sauf interdictions explicites	Droits d'accès trop larges Fraudes	DSI	Aucun accès sauf autorisation spécifique
Les utilisateurs ont-ils l'interdiction de divulguer, communiquer, partager leur mot de passe ?	Accès non autorisés, fraudes	DG	OUI, règlement intérieur, charte informatique signée par les utilisateurs…
Les mots de passe ont-ils une obligation de complexité (longueur mini, 3 types de caractères différents…)	Accès non autorisés, fraudes	DSI	OUI
Les postes de travail se verrouillent-ils automatiquement après quelques minutes d'inutilisation?	Accès non autorisés, fraudes	DSI	OUI

QUESTIONNAIRE

Question	Enjeux / Risques associés	Interlocuteur concerné	Réponse attendue
Tout équipement (ordinateur, tablette, smartphone), connecté au système d'information a-t-il fait l'objet d'une procédure formelle et préalable d'approbation ?	Accès non autorisés, fraudes	DSI	OUI
Le réseau wifi est-il connecté au réseau de production ?	Accès non autorisés, vol de données, sabotage, fraude	DSI	NON
Les points d'accès au système d'information (serveurs, postes de travail, imprimantes, scanners…) font-ils l'objet d'une sécurité physique appropriée (porte avec verrou et badge d'entrée, surveillance, caméras…) ?	Accès non autorisés, vol de données et de matériel, sabotage, fraude	DSI	OUI
Si connexions distantes, depuis l'extérieur, existe-t-il des mesures de sécurité complémentaires, comme authentification à deux facteurs, limitation adresses IP entrantes…?	Accès non autorisés, vol de données, sabotage, fraude	DSI	OUI
Les ressources de l'entreprise, accessibles en ligne par le public, font-elles l'objet de mesures de sécurité spécifiques, régulièrement auditées ?	Accès non autorisés, vol de données, sabotage, fraude	DSI	OUI
Les journaux de connexions sont-ils examinés : - régulièrement ? - Les échecs de connexion sont-ils analysés ?	Détection des tentatives de piratages.	DSI	Analyses régulières, alertes automatiques
Existe-t-il une politique de chiffrement des données sensibles (mots de passe, supports nomades…) ?	Vol de données, accès non autorisé, fraude	DSI	Politique de chiffrement définie et respectée
Dans la liste des utilisateurs du SI, les comptes d'administration ont tous les droits. - Comment ces comptes sont-ils supervisés ? - Leurs actions sont-elles enregistrées et surveillées ?	Accès non autorisé, fraude	DSI	Supervision des comptes d'administration
Les fonctions de développement informatique, de tests et d'exploitation sont-elles séparées, avec du personnel différent ?	Fraude	DSI	OUI

CONDUITE DE PROJETS

FICHE 04
CONDUITE DE PROJETS

CONTEXTE ET ENJEUX

Pourquoi parler de conduite de projets ? Parce qu'en moyenne, 30% du budget d'une entreprise est consacré à des projets. Cela participe de l'évolution, de l'adaptation et de la transformation de toute entreprise relatif aux systèmes d'information en croissance ou non. Les projets SI ont très souvent un impact direct ou indirect sur les états financiers. Le pilotage des projets et leur réussite ou leur échec peuvent avoir des conséquences graves sur l'activité de l'entreprise.

Vis-à-vis des projets, le CAC doit donc s'assurer d'au moins deux choses :

- **En termes d'approche** : le(s) projet(s) a(ont) été mené(s) selon les règles de l'art et respecte(nt) un cadre de contrôle interne suffisant
- **En termes de données** : les données et états financiers impactés ou produits à l'issue du projet sont exhaustifs, fiables, et correctement comptabilisés.

Qu'est-ce qu'un projet ? Un projet est une entreprise temporaire décidée, engagée et financée dans le but de créer un produit, un service ou un résultat unique.

Exemples : conception d'un nouveau véhicule, mise en place d'un ERP. Le projet impacte plusieurs dimensions de l'entreprise, qu'il s'agisse de process, d'organisation, de SI ou des trois à la fois, ce qui est bien souvent le cas.

De manière triviale, on peut comparer un projet à un chantier de construction de maison (à noter qu'une grande partie du vocabulaire lié au SI est hérité du monde du BTP). Il s'agit de connaître le besoin, de le spécifier fonctionnellement, puis techniquement, de construire l'édifice, de tester, puis de valider la conformité avant de l'habiter.

S'agissant d'audit, les projets les plus directement impactants sont ceux touchant le SI financier, que cela soit dans le cadre d'un changement de logiciel, d'une migration de version, d'une intégration ou d'une cession d'activité. Ce sont là les exemples les plus évidents, mais cela ne signifie pas que les autres projets ne concernent pas le CAC !

FICHE 04
CONDUITE DE PROJETS

Un projet se pilote et s'articule autour de trois dimensions fondamentales, assorties de plusieurs attributs :

- **Le livrable** (ou solution) : c'est le résultat à atteindre qui se décline en plusieurs livrables intermédiaires. Exemple de livrables : mise en place d'un nouveau logiciel comptable, migration de version, réorganisation de la fonction financière, définition d'un processus de reporting dans le cadre d'un rachat.
- **Le budget** attribué au projet, qui doit être piloté pour respecter le business case dudit projet.
- **Le planning :** la durée prévue du projet et la date arrêtée pour le démarrage de la solution cible.

Autour de ces trois dimensions structurantes, il est indispensable de piloter les composantes du projet : périmètre, ressources, risques, conformité et tiers externes, etc.

NEP ET TEXTES DE RÉFÉRENCE

- NEP N/A
- PRINCE2, PMBOK, COBIT5

ANALYSE DE RISQUES ET CRITICITÉ

Le RACI est un outil de formalisation des rôles et responsabilités pour chaque partie prenante au projet. Cet outil est indispensable pour établir les attendus vis-à-vis de chaque partie prenante et ainsi lever toute ambiguïté dans les processus de décision.

- **R :** Responsable, ou Réalisateur
- **A :** Approbateur (« accountable » en anglais)
- **C :** Consulté
- **I :** Informé

Il ne peut y avoir qu'un seul **A** par tâche.

EXEMPLES

Description de l'activité	DAF	Directeur comptable	DSI	Intégrateur
Tâche 1	**A**	**R**	**C**	**I**
Tâche 2	**R**	**A**	**C**	**I**
Tâche 3	**C**	**R**	**A**	**I**
Tâche 4	**I**	**R**	**C**	**A**

Les phases du projet :
Comme n'importe quel chantier, un projet est découpé en phases logiques. L'enchaînement, la durée et l'ordonnancement de ces phases varient en fonction de la méthodologie utilisée (cycle en V, agile, hybride,...). Mais leur nature demeure identique afin de respecter un ordre logique de conception : **Expression du besoin > modélisation détaillée > paramétrage > tests > cycle de validation de conformité > mise en production**.
A chaque phase correspondent des risques spécifiques, (cf. tableau pour exemples).

QUESTIONNAIRE

Thème / Question	Enjeu / Risque associé	Interlo-cuteur cible	Réponse attendue ou éléments à collecter	Phase d'audit
Quels sont les projets en cours ou prévus au cours de l'exercice fiscal ?	Implication suffisante des équipes comptabilité/finance	DSI, DAF	Liste des projets	Intérim
Ces projets ont-ils un impact sur les process et/ou les états financiers ?	Impact sur la certification des comptes	DAF	Une réponse claire et argumen-tée	Intérim
Pour chaque projet, une charte a-t-elle été écrite, partagée et acceptée par les parties prenantes ?	Ambiguïté sur le résultat attendu et les rôles et responsabilités des parties prenantes	Toutes les parties prenantes et en particulier DAF et DSI.	oui	Intérim
Quelle est la date cible de livraison du projet ?	Périmètre de l'audit Cut-off	DAF et DSI.	Début d'exercice ou en cours d'exercice	Intérim
Existe-t-il un RACI ? Si oui, a-t-il été formalisé et communiqué à toutes les parties prenantes ?	Ambiguïté sur le résultat attendu et les rôles et responsabilités des parties prenantes	Sponsor du projet	OUI	Intérim
Qui valide les spécifications et de quelle manière ?	Impact sur les process et/ou les états finan-ciers (ex. : refonte de la clé comptable)	Equipe comptable DAF Equipe projet	DAF, DG ou toute personne ayant l'autorité de valiser les process cibles	Intérim
Qui valide la reprise de données et de quelle manière ?	Exhaustivité, fiabilité, intégrité des données	Equipe comptable avec responsabi-lité du DAF	DAF, DG	Intérim
La mise en production du nouveau logiciel comptable a-t-elle lieu au démarrage du nouvel exercice ou bien en cours d'exercice ?	Cut-off Reprise des encours en cours d'exercice	Equipe projet	Démarrage si possible	Intérim
Le DAF participe-t-il effectivement au comité de pilotage ?	Sponsor suffisant en termes de manage-ment	DAF	OUI	Intérim

FICHE 04
CONDUITE DE PROJETS

Thème / Question	Enjeu / Risque associé	Interlo-cuteur cible	Réponse attendue ou élément à collecter	Phase d'audit
Si migration vers une solution cloud, le ctt prévoit-il les clauses ad hoc (auditabilité, réversibilité, GDPR) ?	Conformité Délai d'accès aux données sur demande du CAC.	Equipe projet DAF Juridique	Oui	Intérim
Phase : cadrage Le planning est-il réaliste ?	Retard du projet. Complexité d'un démarrage en cours d'exercice.	DAF, DSI	Oui	Intérim
Phase : cadrage Un PAQ a-t-il été écrit et validé par les parties prenantes ?	Détection et communication des risques projet. Rôles et responsabilités des parties prenantes. Arbitrage. Gestion des litiges.	Equipe projet DAF DSI	Oui	Intérim
Phase : Spécifications La définition des processus est-elle conforme au besoin ?	Non respect des règles de gestion, des procédures et des principes de séparation des fonctions. Non conformité	Equipe projet Utilisateurs	Oui + demander l'accès aux spécifications fonction-nelles	Intérim
Phase : Paramétrage La solution est-elle utilisée dans sa version standard ? Sinon, quelle est la proportion de développements spécifiques	Non respect des règles de gestion. Difficulté de maintenance de migration future.	DAF DSI	Proportion de customisations	Intérim
Phase : Paramétrage Combien y a-t-il d'interfaces entrantes et sortantes autour de la nouvelle solution ? Quel est le niveau d'intégration global ?	Exhaustivité et fiabilité des données : risque de déficience des mécanismes d'alimentation et de déversement des données en entrée et en sortie de la nouvelle application.	DSI Equipe projet technique	Cartographie des interfaces	Intérim
Phase : Tests • Quelle est la stratégie de tests ? • Sur quel volume de données sont-ils réalisés ? • Qui a rédigé les scénarios ?	Exhaustivité Fiabilité des données Régression fonctionnelle	Chef de projet DSI, responsable informatique	Stratégie de tests Scénarios de tests	Intérim
Phase : Reprise de données Nettoyage des données à reprendre Transcodification des règles et référentiels comptables	Risque d'exhaustivité et d'intégrité des données reprises dans le nouveau système. Exactitude des schémas comptables, exhaustivité, auditabilité.	Equipe projet DAF/DC Equipe SI	Documenta-tion Conservation des éléments techniques temporaires (base pivot, fichiers intermédiaires)	Intérim
Le DAF participe-t-il effectivement au comité de pilotage ?	Sponsor suffisant en termes de management.	DAF	OUI	Intérim

Thème / Question	Enjeu / Risque associé	Interlo-cuteur cible	Réponse attendue ou élément à collecter	Phase d'audit
Phase : Recette Quelle est l'organisation de la recette en termes de : • Receteurs • Données de recette • Remontée et traitement des anomalies (outil de ticketing) • Formalisation de l'acceptation	Fiabilité des processus	DAF, DC, respon-sable fonction-nel	Cahier de recette PV de réception dûment signé	Intérim
Conduite du changement • Quelles sont les actions de communication et d'accompagnement ? • Quelle est la répartition de ces actions sur le planning projet ?	Absence de sponsor Implication insuffisante des utilisateurs. Echec du projet Inadéquation de la solution.	DG	Démarche	Intérim
Phase : mise en production Quelle est la politique d'archivage de l'historique ?	Risque de perte de traçabilité de l'informa-tion. Perte d'accès aux informations utiles à l'activité ou réglemen-tairement requises.	DAF	Politique formalisée	Intérim
Phase : support post-production Quelle est l'organisation en place pour traiter les anomalies et répondre aux questions des utilisateurs pendant et après la mise en production (n.b. : sujet concernant également la recette et la conduite du changement)	Sécurité de l'environnement informatique : risque de perte de maîtrise dans les processus de gestion des anomalies, des incidents, de la sécurité de l'application et de l'exploitation informatique	DSI	Description de l'organisation du support	Intérim
Documentation La documentation liée au projet est-elle suffisante en qualité et en quantité. Exemples : expression des besoins, planning, note de cadrage, spécifications (fonction-nelles et techniques), cahier de recette,...	Auditabilité du projet Conformité	DG, DAF, DSI	Accès à la documentation	Intérim
Amortissement Le projet fait-il l'objet d'un amortissement ?	Exactitude de la comptabilisation des coûts liés au projet (opex vs. capex). Run/build et risque de finir le projet en bascu-lant les coûts en TMA.	DG, DAF	Détail de la comptabilisa-tion des dépenses liées au projet	Intérim
Subventions Le projet fait-il l'objet d'un CIR ?	Correcte imputation des subventions	DG, DAF	En fonction de la réponse	Intérim

UTILISATION DES OUTILS D'AUDIT DE DONNÉES

05

FICHE 05
UTILISATION
DES OUTILS D'AUDIT
DE DONNÉES

CONTEXTE ET ENJEUX

La prise en compte de l'environnement informatique par le commissaire aux comptes est un facteur clé de réussite des missions d'audit, en particulier lorsque l'entité à auditer a un recours extensif aux applications informatiques et lorsqu'elle est confrontée à une volumétrie de transactions importante.

Les outils informatiques d'audit de données facilitent le travail du commissaire aux comptes et permettent une atteinte plus aisée de l'assurance raisonnable ainsi qu'une documentation appropriée de l'approche d'audit par les risques.

En outre, c'est un moyen de répondre au risque de fraude tel qu'il est défini dans la **NEP 240**.

- Plus la volumétrie des transactions est importante, moins l'approche substantive (tests) est pertinente
- Plus la volumétrie des transactions est importante, plus l'utilisation d'outils adaptés à l'analyse des données est pertinente.

NEP ET TEXTES DE RÉFÉRENCE

- **NEP 240 :** Prise en considération de la possibilité de fraudes et d'erreurs lors de l'audit des comptes
- **NEP 250 :** Prise en compte du risque d'anomalies significatives dans les comptes. Le CAC doit s'enquérir auprès de la direction du respect des textes et prendre connaissance des correspondances reçues des autorités administratives et de contrôles. On ne peut pas obliger le client à fournir le FEC.
- **NEP 265 :** Communication des faiblesses du contrôle interne
- **NEP 315 :** Prise de connaissance de l'entité et de son environnement.
Cela implique notamment l'environnement réglementaire et numérique.
- **NEP 330 :** Procédures d'audit mises en œuvre par le commissaire aux comptes à l'issue de son évaluation des risques

FICHE 05
UTILISATION DES OUTILS D'AUDIT DE DONNÉES

ANALYSE DES RISQUES ET CRITICITÉ

Les principaux outils du marché (Caseware Idea et ACL) sont une réponse appropriée à la mise en œuvre par l'auditeur de l'analyse des données. Le maniement de ces outils reste adapté à un professionnel n'ayant pas nécessairement de formation informatique spécifique.

Les fichiers sources possibles :

- **Fichier des Ecritures comptables (FEC) :** l'utilisation du FEC comme fichier source possible d'un outil d'analyse de données permet une vérification exhaustive des écritures comptables enregistrées par l'entité en ce compris les écritures manuelles (OD). A ce titre, leur analyse devient plus aisée avec la possibilité de faire des tris et sélections sur la base de critères jugés pertinents par le commissaire aux comptes (jour et heure, personne habilitée, montant, etc.).
- **Fichier contenant les écritures comptables au format texte, excel, ou base de données.** Ces formats d'export sont présents chez tous les éditeurs de logiciel et d'ERP. L'utilisation de ce type d'exports nécessite une bonne maîtrise dans le traitement des fichiers car des retraitements sont, la plupart du temps, nécessaires avant d'effectuer une analyse à l'aide d'un des logiciels cités précédemment.
- **Fichier contenant des données opérationnelles (stocks, factures, expéditions, référentiels).** Ces données vont permettre à l'auditeur de valider les procédures de contrôle interne, détecter des indices de fraude et être un complément à l'analyse des écritures comptables.

Les fonctionnalités nécessaires des outils d'analyse :

Afin de permettre l'analyse des données intégrées dans l'outil, les fonctionnalités suivantes ont été identifiées comme nécessaires afin de rendre l'analyse pertinente et une restitution appropriée des travaux au client :

- Récupération de données disponibles dans de multiples formats
- Tris et index
- Sélection d'enregistrements
- Jointures entre fichiers
- Analyses de corrélation
- Fonctions de calcul des données (dates, chiffres, textes)
- Contrôles de conformité
- Recherche de doublons, ruptures de séquences numériques
- Recherches en « logique floue »
- Analyses statistiques
- Stratification
- Balances âgées
- Analyse selon la loi de Benford
- Totalisations
- Représentation graphique des données
- Sélection aléatoire d'un échantillon de données
- Automatisation des contrôles
- Piste d'audit

Les outils d'analyse de données par l'auditeur permettent également une restitution des travaux d'audit novatrice auprès des clients. Ce sont donc des outils utiles de sensibilisation du chef d'entreprise en lien avec le risque de fraude ou de transaction non fondée.

QUESTIONNAIRE

Thème / Question	Enjeux et Risques associés	Interlocuteur concerné	Réponse attendue
Obtenir la cartographie des SI de l'entreprise : identifier les applications et les interfaces gérant les données entrant dans le périmètre de l'audit de l'exercice et compte tenu de votre analyse des risques	Ne pas identifier les SI sources de l'information financières	DSI, Directeur comptable ou DG	Cartographie claire des différents logiciels et ERP utilisés par le client et des exports possibles de données
Sur la base de votre analyse des risques, de la cartographie des SI et des conclusions de votre revue du contrôle interne, déterminer : - les risques à couvrir - les fichiers et champs à obtenir - la nature de contrôle à réaliser - les formats de fichiers à vous transmettre - les paramètres d'extraction (bornes des périodes, SI source, champs etc...)	Comprendre les données disponibles	DSI, Directeur comptable ou DG	Réponses à obtenir : - Liste des accès aux données et procédures - Contrôle du caractère inaltérable des données saisies - Liste des champs exportables - Formats d'export autre que PDF ou papier
Pour chaque contrôle à réaliser, obtenez les informations suivantes : - le(s) fichier(s) source(s) nécessaire(s) - les principes de codifications des champs de codes (N° client, d'article etc.) - les totaux de contrôles à vous transmettre avec le fichier (nombre d'enregistrements, totaux à retrouver etc.)	- Fichiers / données non conformes aux demandes - Données invalides	DSI, Directeur comptable ou DG	- Obtenir les mêmes éléments que ceux présents dans l'ERP ou le logiciel - S'assurer que les fichiers sont bien exploitables et que l'ensemble des données y sont présentés

FICHE 05
UTILISATION DES OUTILS D'AUDIT DE DONNÉES

Thème / Question	Enjeux et Risques associés	Interlocuteur concerné	Réponse attendue
Validation des fichiers transmis avant analyse. Pour chaque fichier reçu, vérifier les points suivants : - conformité avec votre demande (période, champs, format des champs etc.) - rapprochement des totaux des champs numériques avec les documents / totaux de contrôles transmis - valeurs suspectes (valeur à zéro, montant négatifs, dates hors période, codifications hors normes) ... - contrôles de cohérence (répartition par mois, jour de la semaine, valeur moyenne, mini, maxi ...)	- Fichiers / données non conformes aux demandes - Données invalides	DSI, Directeur comptable ou DG	S'assurer de la bonne conformité du fichier avant de réaliser des tests plus approfondis. Si non, demander de nouveaux fichiers en investiguant les raisons de leur non conformité.
Préparation des données pour l'analyse : - harmoniser les champs entre les différents fichiers obtenus (type de champ, format des dates /heures etc.) - isoler les enregistrements atypiques pouvant perturber les analyses à venir - identifier les travaux spécifiques à mener spécifiquement sur ces anomalies - identification et analyse des doublons anormaux. Ajouter les champs à calculer qui seront nécessaires aux tests à venir	Fiabilité et pertinence des tests réalisés	DSI, Directeur comptable ou DG	Les différents fichiers analysés doivent s'harmoniser pour garantir une bonne analyse. Par exemple : si les dates sont dans des formats différents, l'harmonisation est le seul moyen de garantir l'analyse de 100% des dates présentes dans le fichier.
Mise en œuvre des contrôles : - réaliser les tests tels que défini durant la phase de préparation - analyser chaque anomalie afin d'identifier les faux positifs. Transmettre à la société pour analyse les anomalies identifiées par les contrôles mis en œuvre.	Conclusion erronée	DSI, Directeur comptable ou DG	Présenter au client la liste des anomalies identifiées en expliquant les enjeux. Transmettre les informations nécessaires à l'analyse par le client

POUR ALLER PLUS LOIN

EXEMPLES D'AUDIT DE DONNÉES

CONTRÔLES TRANSVERSAUX

- Schémas comptables atypiques (ventes/achats passés directement par comptes de trésorerie, écritures de régularisation)
- Nombre d'écritures de régularisation ou d'ajustement par utilisateur
- Rapprochement des comptes mouvementés par des écritures d'individus et leur département / fonction de rattachement
- Recherche textuelle dans le libellé des transactions / écritures / notes de frais / mails
- Balances âgées des comptes de tiers clients, fournisseurs, personnel, organismes sociaux, état
- Calcul de ratios financiers et comparaison avec ceux du secteur, comptes N-1

PERSONNEL

- Modifications du fichier du personnel (quoi, qui, quand)
- Rapprochement des feuilles de temps-badgeuses et rubriques des fiches de paie
- Stratification des salaires par catégorie de personnel, âge, localisation, etc.
- Recalcul des commissions sur ventes selon les contrats de travail
- Numéro de SS erroné ou en doublon
- Rapprochement feuilles de temps / badgeuses et fichier du personnel
- Employés sans fiche de paie – fiches de paie non rapprochées avec le registre du personnel
- Ecritures manuelles sur les comptes de personnel (tiers et charges)
- Règlements multiples à un même employé le même mois
- Pas de retenue des charges sociales ou erronées
- Employés sans évolution de salaires N/N-1
- Employés sans prise de congés ou insuffisants
- Employés sans augmentation de salaire

FOURNISSEURS – ACHATS

- Totalisation des achats en quantité et en valeur par fournisseur, acheteur
- Stratification des paiements et ceux proches des seuils de validation
- Transactions avec montants arrondis
- Pourcentage d'appels d'offres gagnés par rapport aux appels d'offres répondus par fournisseur

CLIENTS – VENTES - STOCKS

- Stratification des factures de vente par tranches proches des seuils de validation
- Rapprochement des adresses de livraison aux clients avec celles des employés de l'entité auditée et de ceux du groupe
- Recherche d'encaissements clients non cohérents avec les factures (lettrage multiple et non par paire)
- Quantités en stocks excessives par rapport aux ventes de la période
- Stocks d'articles obsolètes
- Calcul et analyse du prix unitaire par article
- Ruptures de séquence numérique et de dates (bons d'expédition, factures ...)

COMPTES DE TRÉSORERIE

- Rupture des séquences numériques des chèques émis enregistrés dans les comptes bancaires
- Rapprochement des écritures comptables passées dans les comptes de trésorerie avec les flux enregistrés par les banques
- Contreparties anormales des écritures dans les comptes de trésorerie
- Ecritures manuelles dans les comptes de trésorerie

ETATS FINANCIERS

- Rapprochement budgets/réalisations et analyse des écarts
- Calcul des variations N / N-1 et analyse des variations anormales
- Recalcule des états de synthèse, balances générales depuis les écritures détaillées et rapprochement avec les états publiés, déclarations fiscales
- Ecritures manuelles passées le dernier jour de clôture périodique (« test de 11H »)
- Ecritures passées à des dates, jours ou heures inhabituels (jours fériés, le WE, hors heures d'ouverture, jours de fermeture)
- Ecritures manuelles dans des comptes usuellement mouvementés par interface
- Ecritures avec des montants multiples de 1 000, 10 000 etc.
- Ecritures manuelles dans des comptes normalement alimentés automatiquement
- Cohérence entre séquences des numéros d'écritures et les dates comptables
- Ecritures passées les derniers jours de clôture de fin de période

PROTECTION DES DONNÉES PERSONNELLES

06

FICHE 06
PROTECTION DES DONNÉES PERSONNELLES

CONTEXTE ET ENJEUX

Le Règlement général sur la protection des données du 27 avril 2016 dit «RGPD» (ou GDPR, General data protection regulation) changera radicalement l'approche des entreprises en matière de traitement des données personnelles. Pas de transposition nationale, il sera applicable tel quel dès son entrée en vigueur le 25 mai 2018. La Cnil a publié un FAQ sur comment les entreprises doivent se préparer.

Le RGPD vise à contraindre les entreprises à prendre leurs traitements au sérieux. **En termes de sanction financière, le montant pourra atteindre 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial.** D'où un risque d'impact significatif sur les comptes des entreprises.

L'entreprise devient garante du respect de la vie privée. La déclaration préalable à la Cnil est supprimée, remplacée par l'obligation de tenir un **registre** dans lequel sont consignées les mêmes informations que dans la déclaration. L'entreprise est responsable de la **sécurité** informatique nécessaire au respect de la protection des données.

Attention, à l'instar d'autres réglementations, c'est maintenant à l'entreprise de démontrer qu'elle est en conformité. Le RGDP introduit aussi une obligation de notification par les responsables de traitement, en cas de violations de données à caractère personnel. Ils doivent alerter la Cnil dans les meilleurs délais, si possible dans les 72 heures après en avoir pris connaissance.

Elle instaure également l'obligation de nommer un DPO (data protection officer) dans les établissements publics et les entreprises qui effectuent des traitements sur des données sensibles ou des traitements à grande échelle. La nomination est systématique pour les entreprises de plus de 250 personnes. Une clinique ou une société de vidéosurveillance dont le respect de la vie privée est au coeur de son activité est concernée.

FICHE 06
PROTECTION DES DONNÉES PERSONNELLES

Autres obligations, le **« privacy by design »** et le **« privacy by default »**. Le premier vise à prendre en compte le respect de la vie privée dès la conception des systèmes d'information et le second vise par défaut à respecter un niveau très élevé de protection avant le lancement de tout nouveau traitement. Les risques d'atteinte au respect de la vie privée doivent être analysés et des analyses d'impact réalisées et documentées lorsque les risques sont avérés.

Les citoyens de l'UE doivent donner un **consentement** positif et explicite afin que leurs données soient recueillies. Une personne peut solliciter la **suppression** de données personnelles dans certains cas, comme par exemple lorsqu'un organisme recueillant des données n'est pas conforme aux conditions prévues par le RGPD. Les personnes concernées doivent également être tenues informées de toute **violation** de leurs données personnelles si tel était le cas. Les citoyens de l'UE peuvent **transférer** leurs données d'un système à un autre, et ce sans que l'organisme contrôlant les données, représenté par le délégué à la protection des données, ne puisse intervenir. Les délégués à la protection des données devront explicitement fournir aux particuliers **le délai de détention** de leurs données personnelles. De ce fait, les citoyens acquièrent plus de droits leur permettant de contester des décisions les concernant qui seraient basées sur un ensemble d'algorithmes.

Le règlement s'appliquera à la fois aux entreprises établies dans l'Union européenne mais aussi aux entreprises établies en dehors de l'UE qui traitent les données relatives aux activités des entreprises et des organisations de l'UE. Les sociétés hors UE seront également soumises au règlement si elles ciblent les résidents de l'UE. Ainsi, une entreprise américaine possédant une succursale au sein de l'Union (ou une entreprise faisant affaire avec des citoyens de l'Union européenne) sera soumise à ces mêmes régulations.

Un transfert vers un pays tiers de données à caractère personnel ne peut avoir lieu que si les conditions définies par le règlement sont respectées par le responsable de leur traitement et son sous-traitant. Ce point mérite des interprétations du G29 (rassemblement de toutes les CNIL européennes). Les groupes internationaux ont en effet des difficultés à comprendre comment répartir leurs serveurs et leurs données.

L'application du nouveau règlement devrait concerner les nouvelles applications. Les traitements existants ne devraient pas avoir à être mis à niveau pour mai 2018 . Des précisions du G29 sont nécessaires sur ce point.

A noter que la CNIL et le G29 émettent régulièrement des interprétations et des recommandations concernant le RGDP.
L'AFAI a réalisé un modèle de maturité des entreprises dans l'application du RGDP. Les questions ci-après sont une synthèse de ce modèle.

TEXTES DE RÉFÉRENCE :

- **NEP 250 :** Prise en compte de risques d'anomalies significatives dans les comptes résultants du non respect des textes légaux et réglementaires
- **NEP 315 :** Connaissance de l'entité et de son environnement et évaluation du risque d'anomalies significatives
- Nouveau règlement européen sur la protection des données personnelles paru au journal officiel de l'Union européenne qui entrera en application le 24 mai 2018

ANALYSE DES RISQUES ET FACTEURS DE CRITICITÉ :

Risque de non-conformité avec des sanctions très lourdes en cas de manquements aggravés.

QUESTIONNAIRE

Thématique	Question	Interlocuteurs	Réponse et niveau de risque
RGPD applicabilité	La société effectue-t-elle des traitements sur des données sensibles ou des traitements à grande échelle ?	CIL DPO DSI	OUI
Gouvernance / déontologie	Les données personnelles ont été collectées de manière loyale, licite et transparente ? L'objectif de la collecte et du traitement de la donnée est-il légitime ? Les données sont-elles accessibles en dehors de l'Union européenne ?	CIL DPO DSI Directions métiers	Demande d'accord expresse sur les sites Enquête de satisfaction Localisation des Data Center en Union Européenne, sinon accord de respect du RGPD
Information	Le(s) responsable(s) des traitements ont-ils été identifiés et peuvent être sollicités en cas de demande par l'intéressé ? La finalité du traitement, les catégories et sources de données ont-elles été portées à la connaissance de l'intéressé ? Les droits attribués à l'intéressé lui-ont-ils été communiqués (accès, rectification, opposition, effacement, portabilité) ?	CIL DPO DSI Directions métiers	L'entreprise elle-même est désignée comme responsable des traitements Information expresse Documentation des traitements et des catégories de données Réponse aux demandes d'effacement. Portabilité des informations au niveau des banques.
Autorisation	Accès non autorisé, fraude La collecte des données a reçu le consentement de son intéressé ?	CIL DPO DSI	Demande d'accord express
Management	Les modalités du droit à l'information sont-elles établies et appliquées ? Un registre des données et des traitements par finalité est formalisé et tenu à jour ? Les responsabilités en termes de gestion des données personnelles dans l'entreprise et par les sous-traitants sont-elles établies ? En cas d'incidents, un processus de recensement et de communication est-il prévu ?	CIL DPO DSI	Formalisation de procédures Nomination d'un DPO Tenue du registre Nouveaux contrats de sous-traitance Procédure de communication sur les informations volées pour les personnes concernées et la CNIL
Sécurité	Security by design, la sécurité est-elle prévue dans le cadre de la conduite de projet ? Les accès aux traitements et aux données sont-ils tracés et analysés ? Des mesures spécifiques sont-elles prises pour assurer la confidentialité, la continuité, l'intégrité des données ?	CIL DPO DSI RSSI	Prise en compte de la sécurité et du respect des données personnelles dans la méthodologie projet. Logs des traitements et des accès.

POUR ALLER PLUS LOIN

- AFAI : Modèle de maturité www.isaca.org/chapters6/paris
- CNIL : www.CNIL.fr
- Académie des sciences et techniques comptables : cahier 28 Gouvernance des données personnelles et analyse d'impact http://www.lacademie.info/content/download/9033/143186/version/1/file/cahier+28_V2.pdf

LÉGISLATION FISCALE & SI

FICHE 07
LÉGISLATION FISCALE ET SI

07

CONTEXTE ET ENJEUX

Depuis le 01/01/2014, le contribuable doit satisfaire à son obligation de représentation de la comptabilité en remettant une copie des fichiers des écritures comptables sous forme dématérialisée répondant aux normes fixées par l'article A. 47 A-1 du LPF. Cette modification dans les échanges avec l'administration fiscale n'est pas sans danger pour les entreprises. Cette réglementation s'inscrit dans une politique de modernisation et d'automatisation du contrôle fiscal. Les contrôles des professionnels doivent donc évoluer de la même manière.
Depuis 2014, ce sujet est approfondi, faisant apparaître de plus en plus d'enjeux :
- Importance de la numérisation des factures et de la fourniture d'une piste d'audit fiable
- Obligation de faire certifier son logiciel de caisse
- Fourniture du fichier FEC à date à la demande du vérificateur

Pour l'ensemble de ces sujets, les sociétés sont trop peu informées, accompagnées et sensibilisées.

NEP ET TEXTES DE RÉFÉRENCE

› **NEP 250 :** Prise en compte du risque d'anomalies significatives dans les comptes. Le CAC doit s'enquérir auprès de la direction du respect des textes et prendre connaissance des correspondances reçues des autorités administratives et de contrôles. On ne peut pas obliger le client à fournir le FEC.

› **NEP 315 :** Prise de connaissance de l'entité et de son environnement. Cela implique notamment l'environnement réglementaire et numérique.

› Le respect des principes de tenue des comptabilités manuelles ou informatisées constitue « la condition nécessaire du caractère régulier, sincère et probant des comptabilités informatisées » (BOI-BIC-DECLA-30-10-20-40-20131213 § 40).

› Les livres comptables, la documentation comptable et les pièces justificatives, doivent respecter ces principes, qui ont leur traduction dans le FEC.

› PCG, art. 921-3 : Le caractère définitif des enregistrements du livre-journal et du livre d'inventaire est assuré, pour les comptabilités tenues au moyen de systèmes informatisés, par une procédure de validation, qui interdit toute modification ou suppression de l'enregistrement.

› Une comptabilité est dite « informatisée », dès lors qu'elle est tenue, même partiellement, à l'aide d'une application informatique ou d'un système informatisé (BOFIP-BIC-DECLA-30-10-20-40- §30-13/12/2013).

› Analyse des données comptables simplifiées avec l'exploitation du FEC :
- Exhaustivité des analyses même sur de grands volumes
- Concentration des travaux sur les exceptions et anomalies détectées
- Amélioration de la documentation et de la valeur probante des travaux

› Factures électroniques :
- Conservation pendant 6 ans (LPF art. 102 B) et restitution à l'identique (CGI, annexe II - art.96 I bis)
- Déclaration du lieu de stockage au SIE (LPF, L. 102 C) si stockage hors de France (dans un pays ayant signé une convention d'assistance mutuelle).

FICHE 07
LÉGISLATION FISCALE ET SI

ANALYSE DES RISQUES ET CRITICITÉ

Sanctions en cas de remise d'un FEC non conforme ou d'absence de remise d'un FEC :

- Amende de 5.000 € par exercice non conforme (y compris l'exercice en cours)
- Si le montant des rectifications est plus élevé, une majoration de 10 % des droits est mise à la charge du contribuable
- Rejet possible de la comptabilité
- Numérotation des écritures continue : plusieurs rejets de FEC pour absence de numérotation continue des écritures.

Les éléments clefs à connaître sur le FEC :

• En cas de changement de logiciel en cours d'année, il est possible de remettre le FEC de l'exercice concerné sous la forme de deux fichiers distincts ; le premier fichier étant produit par l'ancien logiciel et le second par le nouveau. Ces deux fichiers doivent être remis de manière simultanée et respecter le format défini à l'article A. 47 A-1 du LPF.
• Les principaux éditeurs de logiciels comptables garantissent un FEC respectant la législation, mais attention aux versions anciennes des logiciels qui ne sont pas forcément toutes FEC compatibles, les mises à jour devant absolument avoir été faites.
• Il convient de faire attention aux logiciels de gestion, qui sont la plupart du temps accessibles en mode SaaS (via internet). Vous devez vous assurer qu'ils respectent bien les normes du FEC, si ce n'est pas le cas, en fin d'exercice vous serez dans l'impossibilité de générer votre fichier FEC !
• Le logiciel doit nécessairement proposer soit un outil, soit une fonction permettant de générer un FEC. Si ce n'est pas le cas, alors risque !
• Deux journaux différent ne doivent pas avoir le même libellé (exemple BQ1 = Banque et BQ2 = Banque).
• Attention à l'utilisation de libellés pouvant attirer l'attention (anomalie, inexistant, ...)
• Les cumuls ne peuvent pas être repris s'ils proviennent d'un fichier de type tableur. Les opérations doivent être saisies en détail. Le seul cas où la reprise d'un cumul est possible est lorsque les cumuls proviennent d'un logiciel métier indépendant de la comptabilité.
• L'administration fiscale tolère que la date de comptabilisation soit la date mentionnée sur la pièce justificative.
• Le CFCI (Contrôle Fiscal des Comptabilités Informatisé) est souvent sous-estimé par les entreprises, or il ne se limite pas à la fourniture d'un FEC mais s'inscrit avant tout dans une démarche de documentation du système d'information et d'assurance de la continuité de la piste d'audit
• Le CFCI englobe le FEC et l'ensemble des extractions des données opérationnelles présents dans le système d'information de l'entreprise (Stocks, factures, ...)

QUESTIONNAIRE

QUESTIONS SUR LE CONTRÔLE DU SI – INDISPENSABLE

Question	Enjeux / Risques associés	Interlocuteur concerné	Réponse attendue
La dernière mise à jour de votre logiciel est-elle antérieure à 2016 ?	Non-conformité / Amende et/ou rejet de la comptabilité	DSI, Directeur comptable ou DG	OUI
Est-il possible de générer le FEC pour les périodes concernées ?	Non-conformité / Amende et/ou rejet de la comptabilité	DSI, Directeur comptable ou DG	OUI
La conformité formelle du FEC a-t-elle été vérifiée ?	Non-conformité / Amende et/ou rejet de la comptabilité	DSI, Directeur comptable ou DG	OUI
En cas de vérification formelle du FEC, des anomalies significatives ont-elles été relevées ? 1. Le nom du FEC est-il conforme ? 2. Les champs obligatoires sont-ils remplis à 100% ?	Non-conformité / Amende et/ou rejet de la comptabilité	DSI, Directeur comptable ou DG	NON 1. Numéro SIREN + mention FEC + date de clôture de l'exercice 2. 100% pour chaque colonne
Avez-vous vérifié la cohérence des données de votre FEC : 1. Cohérence des dates entre elles 2. Montant au débit ou crédit nul 3. Le FEC cadre-t-il avec la balance générale et avec la liasse fiscale ? 4. Les numéros de comptes respectent-t-ils le PCG ?	Non-conformité / Amende et/ou rejet de la comptabilité	DSI, Directeur comptable ou DG	OUI 1. Cohérence entre les dates des pièces comptables, de comptabilisation et de validation des écritures 2. Vérifier si ces écritures n'ont pas été modifiées et comprendre pourquoi elles sont à 0 3. La liasse fiscale étant constituée à partir de la balance générale, il est important de valider la cohérence des soldes de la balance avec ceux reconstitués à partir du FEC 4. Les numéros de comptes doivent respecter les numéros définis dans le PCG
L'organisation comptable, les processus comptables et le système d'information ont-ils été documentés ?	Non-conformité / Amende et/ou rejet de la comptabilité	DSI, Directeur comptable ou DG	OUI
Les modalités de classement et d'archivage des pièces justificatives (plan d'archivage) sont-elles claires et écrites ?	Non-conformité / Amende et/ou rejet de la comptabilité	DSI, Directeur comptable ou DG	OUI
L'archivage des factures électroniques permet-elle une consultation des pièces pendant 6 ans ?	Non-conformité / Amende et/ou rejet de la comptabilité	DSI, Directeur comptable ou DG	OUI

FICHE 07
LÉGISLATION FISCALE ET SI

07

QUESTIONS SUR LE CONTRÔLE DU SI – APPROFONDISSEMENT

Question	Enjeux / Risques associés	Interlocuteur concerné	Réponse attendue
La société utilise-t-elle un logiciel standard ou un ERP ? En cas d'utilisation d'un ERP, il est conseillé de faire appel à un spécialiste pour analyser le FEC.	Non-conformité / Amende et/ou rejet de la comptabilité	DSI, Directeur comptable ou DG	Standard
La cohérence des dates et particulièrement de la date de validation a-t-elle été vérifiée ?	Redressement fiscal et/ou rejet de la comptabilité	DSI, Directeur comptable ou DG	OUI
La présence d'une numérotation continue et chronologique des écritures comptables validées a-t-elle été vérifiée ?	Redressement fiscal et/ou rejet de la comptabilité	DSI, Directeur comptable ou DG	OUI
La saisie des écritures comprend-t-elle la référence aux pièces justificatives (piste d'audit) ?	Redressement fiscal et/ou rejet de la comptabilité	DSI, Directeur comptable ou DG	OUI
La concordance du FEC avec la déclaration fiscale annuelle a-t-elle été vérifiée ?	Redressement fiscal et/ou rejet de la comptabilité	DSI, Directeur comptable ou DG	OUI
Impossibilité de modifier ou supprimer les écritures comptables validées ?	Redressement fiscal et/ou rejet de la comptabilité	DSI, Directeur comptable ou DG	OUI
Cohérence des dates entre elles et par rapport au calendrier des jours fériés (anomalies de procédures ?)	Redressement fiscal et/ou rejet de la comptabilité	DSI, Directeur comptable ou DG	OUI
Analyse des schémas d'écritures utilisés afin d'identifier ceux ne respectant pas le PCG et la doctrine comptable	Redressement fiscal et/ou rejet de la comptabilité	DSI, Directeur comptable ou DG	OUI
Recherche de doublons de factures ou de paiements	Redressement fiscal et/ou rejet de la comptabilité	DSI, Directeur comptable ou DG	OUI
Vérification du respect des délais de paiement fournisseurs et clients	Redressement fiscal et/ou rejet de la comptabilité	DSI, Directeur comptable ou DG	OUI
Analyse de la caisse : mouvements supérieurs à 3 K€ ?	Redressement fiscal et/ou rejet de la comptabilité	DSI, Directeur comptable ou DG	NON
Présence d'écritures ayant un compte de TVA déductible et un libellé contenant « voiture », « hôtel », « cadeau »	Redressement fiscal et/ou rejet de la comptabilité	DSI, Directeur comptable ou DG	NON
La société est-elle capable d'extraire les données opérationnelles en cas de demande dans le cadre d'un CFCI ?	Redressement fiscal et/ou rejet de la comptabilité	DSI, Directeur comptable ou DG	OUI Les exports du FEC et des données opération-nelles (Stocks, factures, ...) sont stockés et sécurisés sur le serveur de l'entreprise
Une cartographie claire permet-elle d'identi-fier les liens entre les fichiers ?	Redressement fiscal et/ou rejet de la comptabilité	DSI, Directeur comptable ou DG	OUI Le document doit permettre d'identifier les clefs entre les différents fichiers afin de garantir l'intégralité de la piste d'audit

POUR ALLER PLUS LOIN :

Bibliographie : Questions - réponses du groupe de travail entre l'Ordre et la DGFiP sur le FEC .**Autres outils mis à disposition** : Smart FEC – outil de la CNCC, en téléchargement sur son site L'académie : le contrôle fiscale informatisé, comment s'y préparer ? http://www.lacademie.info/evenements/les_conferences/cahier_n_20_le_controle_fiscal_informatise_comment_s_y_preparer

EXPLOITATION DES SYSTÈMES D'INFORMATION

FICHE 08
EXPLOITATION DES SYSTÈMES D'INFORMATION

CONTEXTE, PÉRIMÈTRE ET ENJEUX

L'exploitation des systèmes d'information est la fonction qui permet de maintenir l'efficacité, l'efficience, la confidentialité, l'intégrité, la disponibilité, la conformité, la fiabilité et la sécurité du système d'information, aussi bien dans ses éléments matériels (serveurs, postes de travail, smartphones, équipements réseau et télécom...) qu'immatériels (logiciels standards, logiciels spécifiques, systèmes d'exploitation, données...).

LES BASES

Les procédures d'exploitation doivent être documentées.
Les changements apportés aux matériels, aux logiciels, aux systèmes d'exploitation doivent être contrôlés et approuvés.
Les fonctions et les équipements de développement, de tests et d'exploitation doivent être rigoureusement séparés.
La prestation de services par des tiers doit être encadrée et gérée.
L'évolution des besoins liés à la croissance des volumes ou à la modification des règles de traitements doit être anticipée et planifiée.
L'intégrité des systèmes et la confidentialité des données doivent être préservées par une protection appropriée contre les codes informatiques non autorisés et/ou malveillants, présents sur les équipements de l'entreprise et sur les équipements personnels des utilisateurs, connectés au système d'information.
Les données doivent être sauvegardées, au minimum tous les jours. Le bon fonctionnement des sauvegardes est suivi selon une procédure formelle. Des tests de restauration sont menés régulièrement.
La sécurité des réseaux doit être assurée, par un contrôle des équipements autorisés à se connecter et par un filtrage des données. Les connexions distantes, depuis l'extérieur, font l'objet de mesures de sécurité complémentaires.
Les supports amovibles font l'objet d'une procédure d'autorisation et d'un suivi, pour préserver la confidentialité des données.
Les ressources de l'entreprise accessibles en ligne par le public, font l'objet de mesures de sécurité spécifiques, régulièrement auditées.
L'ensemble des systèmes fait l'objet d'une surveillance, avec analyse régulière et permanente des logs et des alertes générés automatiquement par les équipements informatiques.

FICHE 08
EXPLOITATION DES SYSTÈMES D'INFORMATION

NORMES ET RÉFÉRENTIELS APPLICABLES

NEP 240 pour la prise en compte de la possibilité de fraude, NEP 330 pour l'évaluation du contrôle interne, NEP 620 pour les experts tiers, SSAE18, SOC1, SOC2, ISAE3402 pour l'externalisation de tout ou partie du SI, ISO27001 pour la gestion de la sécurité.

ANALYSE DES RISQUES ET FACTEURS DE CRITICITÉ

Les risques découlant d'une fonction "exploitation des systèmes" mal gérée sont : interruption des services, fraude, perte et vol de données, intrusion, perte de contrôle des coûts, inadaptation des outils et démotivation des utilisateurs...

QUELQUES EXEMPLES

Augmentation des volumes pas anticipée et pas de surveillance :
Saturation des disques et interruption de services.

Pas de séparation des tâches développement/exploitation :
Création de fonctions secrètes par le développeur, dans les logiciels. Ces fonctions secrètes peuvent être utilisées par lui pour commettre des fraudes qui échapperont aux procédures de contrôle interne.

Pas de protection contre les codes informatiques non autorisés et/ou malveillants :
Dans un environnement à fort enjeu de sécurité et de confidentialité (par exemple bureau d'études dans une entreprise de haute technologie), un utilisateur pourrait chercher à installer un logiciel de contrôle à distance, pour voler des données en dehors des heures de travail, en toute discrétion. Risque aussi de virus sur les matériels personnels des utilisateurs.

Pas de sécurité des réseaux :
Un réseau wifi connecté au réseau de production est une porte ouverte pour les pirates. Casser une clé wifi est un jeu d'enfant !

Pas de suivi des sauvegardes et pas de tests de restauration :
Cas fréquent d'une sauvegarde mal paramétrée : le compte rendu affiché indique : « 0 erreurs de sauvegarde ». La personne en charge du suivi est satisfaite. Mais juste au-dessus de « 0 erreurs de sauvegarde », il est noté « 0 fichiers sauvegardés – 0 octets sauvegardés » ! En cas de panne ou de vol du serveur, la perte de données est certaine.

Pas de surveillance des logs ou des alertes :
Si un des deux disques en miroir sur un serveur est en panne, le serveur fonctionne quand même ! Si la panne du premier disque n'est pas détectée et remédiée, la panne du deuxième disque entrainera une interruption des services. Autre exemple : le journal de sécurité du serveur indique un échec de connexion, avec erreur de mot de passe, plusieurs fois par seconde. Cela signifie un piratage en cours, avec recherche automatique du mot de passe par tests de toutes les combinaisons de caractères possibles. Si ce piratage n'est pas détecté, au bout de quelques jours ou de plusieurs mois, le mot de passe pourra être trouvé par le pirate.

QUESTIONNAIRE

L'audit de la fonction « exploitation des systèmes d'information » peut être réalisé en phase d'intérim.
Il faut commencer par identifier la ou les personnes en charge de l'exploitation. Dans les petites structures, les responsabilités et les tâches liées à l'exploitation des systèmes d'information sont peu ou mal définies. Par commodité, la personne en charge de l'exploitation est désignée "DSI" dans le questionnaire ci-dessous.

Thème / Question	Enjeu / Risque	Interlocuteur	Réponse attendue
Les procédures d'exploitation sont-elles documentées ?	Interruption de services, fuite de données	DG, DSI	Idéalement : OUI Mais rare dans les petites structures
Les changements apportés aux matériels, aux logiciels, aux systèmes d'exploitation sont-ils contrôlés et approuvés, selon une procédure formelle ?	Inadaptation des outils informatiques, achats inutiles, perte de temps	DG	OUI
Les fonctions de développement, de tests et d'exploitation sont-elles séparées ?	Fraude	DG	OUI
Les équipements de développement, de tests et d'exploitation sont-ils séparés ?	Fraude	DG	Idéalement : OUI Mais rare dans les petites structures
La prestation de services par des tiers est-elle encadrée et gérée ?	Fraude, coûts inutiles, vol de données	DG	OUI
Externalisation, sous-traitance, Cloud... : les risques associés sont-ils évalués et des clauses de réversibilité sont-elles prévues ?	Fraude, coûts inutiles, vol ou perte de données, interruption de services....	DG	OUI.
L'évolution des besoins liés à la croissance des volumes ou à la modification des règles de traitements est-elle anticipée et planifiée ?	Interruption de services, coûts	DG, DSI	OUI
Existe-il un antivirus sur tous les équipements de l'organisation auditée ?	Interruption de services, vol de données...	DG, DSI	OUI

FICHE 08
EXPLOITATION DES SYSTÈMES D'INFORMATION

Thème / Question	Enjeu / Risque	Interlocuteur	Réponse attendue
Existe-t-il une gestion centralisée et une remontée automatique d'alertes pour les antivirus ?	Interruption de services, vol de données…	DG, DSI	OUI
L'existence d'un antivirus est-elle exigée sur les équipements personnels des utilisateurs, avant autorisation de se connecter au système d'information ?	Interruption de services, vol de données…	DG	OUI
Tout logiciel présent sur les équipements connectés au système d'information a-t-il fait l'objet d'une procédure formelle et préalable d'approbation ?	Vol de données, fraude…	DG	OUI
Les données sont-elles sauvegardées automatiquement au moins une fois par jour ?	Perte de données, indisponibilité des systèmes	DG, DSI	Obligatoirement OUI
Le bon fonctionnement des sauvegardes est-il suivi selon une procédure formelle ?	Perte de données, indisponibilité des systèmes	DG, DSI	Obligatoirement OUI
Des tests de restauration sont-ils menés régulièrement ?	Perte de données, indisponibilité des systèmes	DG, DSI	Obligatoirement OUI
Tout équipement (ordinateur, tablette, smartphone) connecté au système d'information a-t-il fait l'objet d'une procédure formelle et préalable d'approbation ?	Vol de données, interruption de services, fraude…	DG, DSI	OUI

Thème / Question	Enjeu / Risque	Interlocuteur	Réponse attendue
La connexion à Internet est-elle sécurisée par un pare feu suivi et administré ?	Vol de données, interruption de services, fraude…	DG, DSI	OUI
Le réseau wifi est-il connecté au réseau de production ?	Vol de données, interruption de services, fraude…	DG, DSI	NON. Si OUI, justifier pourquoi et évaluer les mesures de sécurité compensatoires.
Si connexions distantes, depuis l'extérieur, existe-t-il des mesures de sécurité complémentaires, comme authentification à deux facteurs, limitation adresses IP entrantes…?	Vol de données, interruption de services, fraude…	DG, DSI	OUI
Les supports amovibles font-ils l'objet d'une procédure d'autorisation et d'un suivi ?	Vol de données	DG, DSI	OUI
Les ressources de l'entreprise accessibles en ligne par le public, font-elles l'objet de mesures de sécurité spécifiques, régulièrement auditées ?	Vol de données, interruption de services, fraude…	DG, DSI	OUI
Les logs, les journaux, les alertes générés automatiquement par les équipements informatiques font-ils l'objet d'un suivi régulier et permanent ?	Vol de données, interruption de services, fraude…	DG, DSI	OUI

PLAN DE CONTINUITÉ D'ACTIVITÉ

FICHE 09
PLAN DE CONTINUITÉ D'ACTIVITÉ

CONTEXTE ET ENJEUX

Le plan de continuité d'activité (PCA) doit permettre à une entité la reprise et la continuité de ses activités à la suite d'un sinistre ou d'un événement perturbant gravement son fonctionnement normal. Il doit également permettre à l'organisation de répondre à ses obligations externes (réglementaires, contractuelles) ou internes (survie de l'entreprise, risque d'image, risque de perte de marché etc.) et de tenir ses objectifs.

NEP ET TEXTES DE RÉFÉRENCE

A ce titre, les diligences du commissaire aux comptes en la matière s'inscrivent dans le cadre des **NEP 315** et **570** relatives respectivement à la connaissance de l'entité et la continuité d'exploitation. Dans le cas d'une externalisation du système d'information, un rapport **ISAE 3402** est souvent fourni par le prestataire informatique aux auditeurs pour leur permettre d'avoir une assurance raisonnable sur les contrôles effectués chez le fournisseur. L'analyse de ce rapport constitue un premier niveau de contrôle mais des tests de procédures peuvent être diligentés pour conforter cette analyse.

ANALYSE DES RISQUES ET CRITICITÉ

Pour cerner les **facteurs de criticité d'un PCA**, l'auditeur doit en connaître la démarche d'élaboration. Elle s'organise généralement en 5 étapes.

› Etape 1 : Identifier les objectifs et les activités essentielles
Lors de cette étape, l'entreprise a dû identifier les activités qui sont nécessaires à l'atteinte de ses objectifs, préciser les apports de ces activités pour le fonctionnement de l'organisation et décrire les objectifs de chaque activité essentielle.

› Etape 2 : Déterminer les attentes de sécurité pour tenir les objectifs
Lors de cette étape, les besoins de continuité ont été recensés et formalisés. Il en existe 6 catégories : disponibilité, intégrité, confidentialité, traçabilité, évolutivité et sûreté. La quantification du niveau du besoin de continuité est effectuée selon 3 indicateurs : niveau de service minimum, niveau d'indisponibilité minimum, ressources restant indispensables.
Les ressources restant indispensables ont dû être identifiées avec précision. Il existe 5 catégories de ressources : infrastructures, systèmes d'information, ressources humaines, ressources intellectuelles / informations et prestations externes.

FICHE 09
PLAN DE CONTINUITÉ D'ACTIVITÉ

› Etape 3 : Identifier, analyser, évaluer et traiter les risques

Le recensement des risques a été effectué suivant 4 catégories : risques de nature stratégique, risques opérationnels, risques liés à la gouvernance et risques juridiques. L'évaluation des risques a consisté à hiérarchiser les risques en tenant compte de leur probabilité et de leur impact potentiel sur les activités essentielles.
Les scenarii de sinistre à prendre en compte ont été recensés. Ils ont été formalisés en indiquant s'il y a les mesures particulières de prévention, les impacts principaux sur l'organisation et ses capacités, les indices permettant d'identifier le début de la crise et les critères permettant de mesurer l'ampleur du sinistre.

› Etape 4 : Définir la stratégie de continuité d'activité

Des objectifs de continuité ont été fixés compte tenu des besoins dans l'absolu et des scenarii de sinistre retenus. Ces objectifs portent sur les activités et donc sur les processus et les ressources critiques.
Pour répondre aux objectifs de continuité, les exigences sur les ressources nécessaires au PCA, y compris celles des partenaires, ont été définies.

› Etape 5 : Mettre en œuvre et assurer l'appropriation

Après validation par la direction, le PCA a été transmis à chaque responsable de ressource critique pour définir ce qui est attendu (disponibilité de certains composants, délais de bascule etc.). Ces responsables ont dû confirmer les modalités de mise en œuvre : délais, coûts, arbitrages etc. qui ont été consolidés pour validation par la direction. Il a été ensuite demandé aux responsables des processus concernés par les activités essentielles de décliner les actions dans leurs propres processus.

Une cellule de crise a été définie : composition et gouvernance de la cellule de crise, procédures etc. Enfin, le maintien du PCA en condition opérationnelle a été prévu : vérifications périodiques, exercices et entraînement etc.

QUESTIONNAIRE

1. Définir le contexte : identifier les objectifs et les activités essentielles

Thème / Question	Enjeu / Risque	Interlocuteur	Réponse attendue
La direction est-elle fortement impliquée ?	Opérationnel	DG	OUI
Un chef de projet doté des compétences, de l'autorité et de l'autonomie nécessaire a-t-il été nommé ?	Opérationnel	DSI	OUI
Les objectifs, les activités essentielles, les flux et les ressources critiques ont-ils été identifiés ?	Opérationnel	DSI	OUI préciser
Les flux entre les systèmes d'information supportant les processus ont-ils été cartographiés ?	Opérationnel	DSI	Préférable

2. Déterminer les attentes de sécurité pour tenir les objectifs

Thème / Question	Enjeu / Risque	Interlocuteur	Réponse attendue
Les systèmes de téléphonie, serveurs de fichiers et messagerie ont-ils été intégrés dans les systèmes critiques de l'organisation ?	Opérationnel	DSI	Préférable
Les ressources critiques matérielles ont-elles été prises en compte ?	Opérationnel	DSI	OUI
Les niveaux de fonctionnement en mode dégradé sont-ils explicités ? Ont-ils été validés en liaison avec les clients ?	Opérationnel/ Image / Juridique	DSI	OUI Préférable
Les niveaux dégradés de prestations des fournisseurs ont-ils été pris en compte ?	Opérationnel	DG/DSI	Préférable

3. Identifier, analyser, évaluer et traiter les risques

Thème / Question	Enjeu / Risque	Interlocuteur	Réponse attendue
L'analyse des risques a-t-elle permis d'identifier ceux contre lesquels il est prioritaire de se protéger ?	Opérationnel	DSI	Préférable
Le PCA prend-t-il en compte les risques opérationnels pour lesquels l'interruption d'activité résulte de la perte de ressources critiques ?	Opérationnel	DSI	OUI
Les partenaires susceptibles d'être concernés par les scenarii ont-ils été identifiés ?	Opérationnel / Image / Juridique	DG/DSI	Préférable

4. Définir la stratégie de continuité d'activité

Thème / Question	Enjeu / Risque	Interlocuteur	Réponse attendue
La stratégie a-t-elle été validée par la direction ?	Opérationnel /Image	DG	OUI
Les objectifs de continuité en mode dégradé et pour la reprise d'activité sont- ils cohérents avec les scénarii de risques retenus ?	Opérationnel	DSI	OUI
L'ordre de priorité des procédures, des ressources, de la reprise et du basculement progressif sur les systèmes normaux est-il identifié ?	Opérationnel	DSI	OUI
Les exigences vis à vis des partenaires ont-elles été prise en compte de manière réciproque ?	Opérationnel / Image / Juridique	DG/DSI	Préférable

5. Mettre en oeuvre et assurer l'appropriation

Thème / Question	Enjeu / Risque	Interlocuteur	Réponse attendue
Les actions de communication nécessaires au lancement, à l'appropriation et à la mise en œeuvre du PCA ont-elle été prévues ?	Opérationnel	DG/DSI	OUI
Les mesures à mettre en œuvre et les procédures associées sont-elles simples et accessibles ?	Opérationnel	DG	OUI
Les personnels responsables sont-ils désignés, informés et formés aux procédures prévues dans le PCA ?	Opérationnel Réglementaire	DG	OUI
Les procédures de sauvegarde/récupération et moyens critiques du PCA sont-ils contrôlés périodiquement ?	Opérationnel Réglementaire	DSI	OUI

CYBERSÉCURITÉ

FICHE 10
CYBERSÉCURITÉ

CONTEXTE ET ENJEUX

La cybersécurité permet de lutter contre la cybercriminalité qui désigne les délits perpétrés à distance par des systèmes de communication comme Internet. La cybercriminalité concerne non seulement les formes traditionnelles de criminalité, opérées dans le cas d'espèce via Internet, mais aussi l'atteinte à la confidentialité, l'intégrité et la disponibilité des systèmes d'information.

LES DEUX CATÉGORIES DE CYBERATTAQUES

Elles peuvent être distinguées :

- **L'attaque technique par le canal internet :** ces attaques exploitent une faille technique du site web ou du réseau de l'entreprise pour ensuite s'introduire dans son système d'information ou installer des logiciels malveillants. Ce type d'attaque nécessite des outils informatiques capables de contourner les dispositifs de sécurité du système d'information.
- **L'ingénierie sociale :** ces attaques exploitent les failles humaines, le maillon faible de la sécurité informatique. Grâce à des techniques manipulatoires, les cybercriminels amènent les collaborateurs de l'entreprise à compromettre la sécurité du système d'information.

NEP ET TEXTES DE RÉFÉRENCE

La cybercriminalité a toutes les caractéristiques de la fraude telles que définies par la **NEP-240**. Conformément à cette norme, le commissaire aux comptes doit évaluer les risques d'anomalies significatives dans les comptes résultant de ce type de fraude.

ANALYSE DES RISQUES ET FACTEURS DE CRITICITÉ

Les failles usuellement exploitées par **les attaques techniques** concernent principalement la sécurité des applications Web. Trois raisons peuvent en être à l'origine :
1. La gestion incorrecte de l'authentification, des habilitations et du contrôle d'accès.
2. L'injection de données qui est une technique consistant à insérer des données en entrée d'un programme informatique afin de les détourner de leur fonction d'origine.
3. Les fuites d'information si les fonctionnalités ou composants internes à une application ne sont pas suffisamment « cloisonnés ».

Certes **l'ingénierie sociale** tire profit de la naïveté et de la crédulité de ses victimes mais plusieurs autres facteurs de criticité sont de nature à favoriser ce type de cyberattaques :
1. La facilité d'accès aux informations décrivant l'organisation de l'entreprise
2. L'accès aux informations personnelles des collaborateurs via les réseaux sociaux
3. L'utilisation par les collaborateurs de technologies non sécurisées
4. La complexité et la décentralisation des organisations
5. Le nomadisme professionnel et le télétravail
6. Le manque d'exemplarité des dirigeants
7. Et bien évidemment, le manque de contrôle interne et de formations associées.

FICHE 10
CYBERSÉCURITÉ

QUELQUES EXEMPLES RÉCENTS

Virus Cryptolocker

Un mail intitulé « relance facture impayée » est envoyé au comptable d'une entreprise. Le document joint contient un virus qui va chiffrer toutes les données accessibles par l'ordinateur contaminé et les rendre inutilisables. La clé de déchiffrement est fournie contre le paiement d'une rançon.

Fraude aux virements

Un important groupe industriel français a reçu un avis de changement de RIB, expédié soit disant par un fournisseur, juste avant le règlement d'échéances importantes. Cette escroquerie a permis de dérober 1,6 M€ à la victime.

Espionnage économique

Un Ministère français a fait l'objet d'une intrusion informatique et d'un vol de données. Le point de départ a été l'ouverture de fichiers contaminés par des utilisateurs manipulés et crédules.

QUESTIONNAIRE

Le contrôle le plus difficile et le plus sensible est sans doute celui relatif à la prise en compte des risques de cybercriminalité par la direction générale. Le plus difficile, car l'exercice fait appel à la subjectivité des dirigeants. Le plus sensible, car de cette prise de conscience dépendent les investissements informatiques et les mesures mises en œuvre. Ce contrôle peut être mené en phase d'interim.

Thème / Question	Enjeu / Risque	Interlocuteur	Réponse attendue
La direction générale a-t-elle mobilisé les compétences requises pour comprendre les risques de cybercriminalité et déterminer si le management prend les actions appropriées ?	Opérationnel Juridique	DG	OUI en précisant lesquelles
La direction générale bénéficie-t-elle d'un retour direct du responsable de la sécurité pour lui expliquer en des « termes opérationnels et stratégiques » les cyberrisques et leur prévention ?	Opérationnel Juridique Image	DG	OUI
Une attention suffisante est-elle aussi bien consacrée à la défense a priori contre les attaques qu'aux opérations de remise en état des systèmes a posteriori ? La DG a-t-elle mis en place un reporting pour centraliser et suivre les différentes tentatives de fraude au sein de l'organisation ?	Opérationnel Juridique Image	DG	OUI
Les fonctions essentielles de l'entreprise ont-elles été sécurisées pour préserver la résilience de l'entreprise en cas d'attaque ?	Opérationnel	DG	OUI
La DG a-t-elle mis en place une cartographie des risques ? La DG a-t-elle identifié les scénarios possibles en fonction des types d'attaques ? Les données sensibles sont-elles identifiées et protégées ? Les plans d'actions en cas de crise sont-ils effectivement mis à jour en fonction des évolutions technologiques ou opérationnelles ?	Opérationnel Juridique Image	DG	OUI

Après avoir analysé la prise en compte des risques par la direction générale, l'auditeur pourra se consacrer à **l'évaluation des dispositifs de prévention de l'entreprise** avec des questions telles que :

Thème / Question	Enjeu / Risque	Interlocuteur	Réponse attendue
Existe-t-il une structure dédiée à la gestion de la sécurité de l'information : un comité sécurité, un responsable de la sécurité du système d'information (RSSI) et des correspondants sécurité dans les unités ?	Opérationnel	DSI	OUI
Existe-t-il une attribution claire des responsabilités pour la mise en œuvre et le suivi des évolutions à apporter en matière de sécurité du SI ?	Opérationnel	DSI	OUI
Existe-t-il des procédures d'autorisation de nouveaux matériels ou logiciels ?	Opérationnel	DSI	OUI
Existe-t-il des procédures applicables à l'accès aux informations par des tiers ?	Opérationnel	DSI	OUI
Existe-t-il des modalités de réaction aux incidents de sécurité et aux défauts de fonctionnement : • signalement rapide des incidents de sécurité • signalement dysfonctionnements de logiciels • capitalisation sur la résolution d'incidents • processus disciplinaire	Opérationnel	DSI	OUI
Les connexions à distance sont-elles réalisées de manière sécurisée ? (VPN par exemple)	Opérationnel	DSI	OUI
Les échanges d'informations sont-ils réalisés de manière chiffrée ?	Opérationnel	DSI	OUI
Les PC et les serveurs de l'organisation sont-ils tous protégés par un anti-virus ?	Opérationnel	DSI	OUI
L'organisation s'assure-t-elle que tous les anti-virus sont à jour et fonctionnent correctement ? Si possible de façon centralisée, sinon selon une procédure documentée.	Opérationnel	DSI	OUI
Les règles de contrôle d'accès sont-elles formalisées dans un format « tout est interdit sauf » plutôt que « tout est permis sauf » ? Ces règles sont-elles transmises aux salariés ?	Opérationnel	DSI	OUI
La gestion des mots de passe et les systèmes de déconnexion automatique vérifient-ils les règles suivantes : • tout compte utilisateur doit être protégé par un mot de passe ; • engagement des utilisateurs à ne pas divulguer leur mot de passe ; ne pas écrire leur mot de passe de façon trop évidente ; ne pas stocker leur mot de passe dans une procédure automatique ; changer leur mot de passe dès qu'ils le soupçonnent d'être compromis ; • contrôle qu'un mot de passe temporaire est envoyé pour la première utilisation et qu'il est bien changé par l'utilisateur dès la première utilisation ; • contrôle que les mots de passe temporaires sont transmis aux utilisateurs de manière sûre ; • contrôle que le système impose un changement régulier du mot de passe ; • contrôle que le système impose le choix de mots de passe robustes ; • déconnexion automatique en cas d'inactivité prolongée.	Opérationnel	DSI	OUI

GLOSSAIRE

TERME	DÉFINITION	N° DE FICHE	N° DE PAGE
ANSSI	L'Agence nationale de la sécurité des systèmes d'information est un service à compétence nationale rattaché au Secrétaire général de la défense et de la sécurité nationale (SGDSN), autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. L'agence assure la mission d'autorité nationale en matière de sécurité des systèmes d'information. À ce titre, elle est chargée de proposer les règles à appliquer pour la protection des systèmes d'information de l'État et de vérifier l'application des mesures adoptées. Dans le domaine de la défense des systèmes d'information, elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques, notamment sur les réseaux de l'État.	**10**	**- ***
API	Pour « Applications Programming Interface », désigne la programmation d'une interface entre deux applications/logiciels/outils pour échanger des données. Ce système a pour but de faciliter les échanges d'informations entre différents outils pour faciliter l'expérience utilisateur.	**1**	15
APT	Pour « Advanced Persistent Threat ». Une attaque furtive via le canal Internet ciblant une entité en particulier.	**10**	**-**
BACKDOOR	Programme informatique dissimulé qui offre aux pirates un accès Internet vers une machine cible, en toute discrétion. Ces backdoors s'installent rapidement, par n'importe quel utilisateur ayant accès à l'équipement informatique, ne serait-ce qu'une seule fois. Intérêt : se connecter à l'ordinateur compromis afin de voler des données, ou pour « pivoter » (action de se connecter à une seconde machine depuis la première) et ainsi remonter dans tout le réseau.	**10**	**-**
BIG DATA / ANALYTICS	Le Big data est le terme qui désigne les très grands volumes de données. La multiplication des données à gérer et stocker par les entreprises à donner naissance à ce terme. Afin de maîtriser et analyser ces volumes, il est nécessaire de faire appel à des techniques d'Analytics qui désigne les techniques informatiques permettant de contrôler ces données.	**1**	14, 15
BUREAU DYNAMIQUE	Le Big data Des espaces où les salariés n'ont plus de poste de travail attitré ni d'espace personnel. On parle également de salariés « sans bureau fixe ».	**1**	14
CARTOGRAPHIE DES SI	Document permettant d'avoir une vision exhaustive et actualisée en permanence du SI de l'entreprise : infrastructure, logiciels, découpage fonctionnel, description des processus, interface etc. Il permet également de comprendre les interactions entre les différents acteurs – utilisateurs – département.	**2 et 5**	24, 43
CHARTE INFORMATIQUE	La Charte d'utilisation des systèmes d'information s'inscrit dans la PSSI. La charte définit les règles d'usage des ressources informatiques d'une organisation, dans le respect des lois et de la vie privée, pour protéger les intérêts de l'organisation et préciser les responsabilités de chaque utilisateur. Le non-respect de cette charte engage normalement la responsabilité personnelle de l'utilisateur.	**3 et 10**	32
Cheval de Troie informatique	Un cheval de Troie est un logiciel en apparence légitime, mais qui contient une fonctionnalité malveillante. Le rôle du cheval de Troie est de faire entrer ce parasite sur l'ordinateur et de l'y installer à l'insu de l'utilisateur.	**10**	24, 43
CIL	Correspondant Informatique et Libertés	**6**	47, 49
CLIC AND COLLECT	Ce terme désigne l'action de commander son produit en ligne et de le récupérer dans un point de vente choisi. Ce procédé a pour but de limiter le temps d'attente en caisse.	**1**	14
CLOUD	Le cloud computing, ou l'informatique en nuage, est l'exploitation de la puissance de calcul ou de stockage de serveurs informatiques distants par l'intermédiaire d'un réseau, généralement internet.	**2, 4 et 8**	20, 21, 23, 38, 59

TERME	DÉFINITION	N° DE FICHE	N° DE PAGE
Conformité formelle du FEC	Le FEC doit répondre à un certain nombre de critère pour être conforme. Parmi les principaux critères le FEC doit contenir au minimum 18 colonnes (pour un BIC) dont la plupart doivent être renseignées à 100%, le fichier doit être au format texte, … L'ensemble de ces critères sont listés dans l'article A. 47 A-1 du LPF et complétés par les questions réponses publiées sur le site de l'administration fiscale.	**7**	53
CRM	Pour « Customer Relationship Management » ou encore Gestion de la Relation Client en français. Ce terme désigne l'ensemble des sujets liés au marketing, support et relation client. On parle régulièrement de logiciel CRM qui désigne donc un logiciel permettant de suivre ou d'animer la relation avec le client (gestion des devis, relances clients, base d'information client, support technique etc…).	**1**	14
CRYPTOLOCKER	Un crypto-verrouilleur ou ransomware est une classe de logiciel malveillant. Ce type de rançongiciel se diffuse principalement via des courriels infectés, déguisés en factures. Une fois activé, il chiffre les données personnelles de l'utilisateur avec une clé secrète – stockée sur des serveurs pirates – et demande une rançon (payable en bitcoins ou par des services externes) pour les rendre à nouveau accessibles. Le message d'alerte s'accompagne d'un compte à rebours de 72 ou 100 heures qui menace de supprimer les données si la rançon n'est pas payée. En fait, une fois arrivé à zéro, il augmente fortement le montant de la rançon.	**10**	68
Cybercriminalité	La cybercriminalité désigne les délits perpétrés à distance par des systèmes de communication comme Internet. La cybercriminalité concerne non seulement les formes traditionnelles de criminalité, opérées dans le cas d'espèce via Internet, mais aussi l'atteinte à la confidentialité, l'intégrité et la disponibilité des systèmes d'information.	**10**	67, 68
DARKNET	Réseau anonymisé et encrypté, de plus ou moins grande taille, qui concurrence le Web. Le trafic y est souvent lent et les usagers insaisissables. Citons ainsi les réseaux Tor, I2P ou encore FreeNet qui sont particulièrement plébiscités pour leur capacité à héberger des services cachés (« hidden services »). Autrement dit, il s'agit de sites Internet dont l'adresse IP n'est pas référencée par les fournisseurs de noms de domaine (DNS Providers).	**10**	-
DASHBOARDING	Le dashboarding est l'activité ou le dispositif de création de tableaux de bord à vocation commerciale ou marketing. Il est souvent visuel et permet une meilleure lisibilité d'une situation et de l'environnement afin de facilité la prise de décision.	**1**	15
DPO	Pour « Data Protection Officer » qui succèdera au CIL à compter de 2018. Il s'agit généralement de l'individu en charge de la protection des données personnelles et du respect de la réglementation relatives à ces données au sein d'une organisation.	**6**	47, 49
DSI	Directeur des systèmes d'information. Il est responsable de l'ensemble des composants matériels (postes de travail, serveurs, équipements de réseau, systèmes de stockage, de sauvegarde et d'impression, etc.) et logiciels du système d'information, ainsi que du choix et de l'exploitation des services de télécommunications mis en œuvre.	Ensemble du document	
ERP	Pour « Enterprise Resource Planning », désigne les logiciels paramétrables et adaptables à l'environnement de l'entreprise. Ces logiciels font donc l'objet d'un déploiement et d'une adaptation aux contextes des entreprises. Ils sont donc plus ouverts que les logiciels standards du marché et doivent donc faire l'objet d'un contrôle renforcé pour s'assurer qu'ils respectent bien la réglementation et que certaines adaptations au contexte de l'entreprise ne le rendent pas non conforme.	**2, 3, 4, 5 et 7**	24, 27, 31, 35, 42, 43, 54
Factures électroniques	La facture électronique est désignée par le fait de stocker une pièce comptable sous la forme dématérialisée. Attention, cependant, à ne pas confondre : il ne suffit pas de stocker une facture scannée ou au format PDF pour qu'elle soit certifiée « facture électronique ». Il existe des logiciels spécifiques qui garantissent la conformité de la facture et son caractère inviolable.	**7**	51

TERME	DÉFINITION	N° DE FICHE	N° DE PAGE
FEC	Fichier des Ecritures Comptables. Fichier informatique standard qui peut être exporté à partir de n'importe quel logiciel comptable compatible avec la réglementation française et qui est exigé par l'administration fiscale en cas de contrôle fiscal. Ce fichier est normé et doit respecter ces normes sous peine d'amende ou de rejet de la comptabilité. Il sera bientôt à déposer en même temps que la liasse fiscale.	**5, 7**	**41, 42, 51, 52, 53, 54, 55**
G29	ou Groupe de travail Article 29 sur la protection des données (en anglais Article 29 Data Protection Working Party) est un organe consultatif européen indépendant sur la protection des données et de la vie privée.	**6**	48
GDPR	General data protection regulation ou Règlement général sur la protection des données du 27 avril 2016 (Règlement UE 2016/679).	**1, 2, 4 et 6**	**14, 21, 22, 38, 47, 49**
Ingénierie sociale	De l'anglais « Social Engineering ». Ensemble des techniques de manipulation consistant à exploiter la faiblesse humaine dans le but d'obtenir des informations sensibles. Les pirates trouvent par la persuasion une faille qui mène vers une ressource convoitée : mots de passe, données bancaires, fichiers clients, brevets, etc.	**10**	67
Injection de données	Attaque technique par le canal Internet consistant à insérer des données en entrée d'un programme informatique afin de le détourner de sa fonction d'origine.	**10**	67
Jointures entre fichiers	Lier deux fichiers sur la base d'un ou de plusieurs champs communs. Exemple : jointure entre le fichier des bons d'expédition avec les factures de vente sur la base du numéro du bon d'expédition pour identifier les expéditions non facturées et les factures sans bon d'expédition.	**5**	42
Logique floue	Démarche ne se basant pas sur une égalité parfaite mais avec un degré variable de concordance. Exemple : « Jean » est comparable à « Jan ».	**5**	42
Logs	Journal des évènements, enregistré automatiquement par un système informatique (serveur, équipement télécom…). Précieux pour le diagnostic des pannes et la détection des anomalies.	**6 et 8**	**49, 57, 58, 61**
Méthodes agiles	Désigne l'ensemble des méthodes qui permettent dans un projet de prendre en considération au maximum le besoin initial du client et les contraintes qu'impose le projet pour permettre une plus grande réactivité à ses demandes.	**1**	14
MOOC	Pour « Massive Open Online Courses », désigne les formations en ligne ouvertes à n'importe quel participant, autrement dit des cours en ligne. L'avantage étant la possibilité de réunir un grand nombre de personnes sans limite géographique.	**1**	14
Open Innovation	Innovation ouverte. Elle désigne des modes d'innovation fondés sur le partage et la collaboration dans les domaines de la recherche et du développement.	**1**	15
Outils collaboratifs	Le travail collaboratif désigne un mode de travail qui ne tient pas compte de l'organisation hiérarchique traditionnel dans une entreprise. Les outils collaboratifs sont donc l'ensemble des outils qui permettent de simplifier cet échange collaboratif ou chaque participant peut donner son avis et défendre son point de vue.	**1**	14
PCA	Le Plan de continuité d'activité s'inscrit dans la PSSI. Le PCA doit permettre à une organisation la reprise et la continuité de ses activités à la suite d'un sinistre ou d'un événement perturbant gravement son fonctionnement normal. Il doit permettre à l'organisation de répondre à ses obligations externes (réglementaires, contractuelles) ou internes (survie de l'entreprise, risque d'image, risque de perte de marché etc.) et de tenir ses objectifs.	**9**	**63, 64, 65**

TERME	DÉFINITION	N° DE FICHE	N° DE PAGE
Piste d'audit fiable	Désigne la facilité avec laquelle le vérificateur peut remonter d'une écriture comptable à la pièce comptable d'origine. Cette « piste d'audit fiable » nécessite d'être documentée et de respecter un certain nombre de critères de stockage des documents.	**7**	51
Pizza team	Concept d'organisation de projet informatique venant d'Amazon. Il définit une taille idéale de l'équipe pour développer un projet efficace : celle-ci ne doit pas dépasser le nombre que l'on peut nourrir avec deux pizzas, soit 8 personnes. Les membres doivent être suffisamment nombreux pour que l'équipe soit créative, mais pas au point que la cohésion et la communication se perdent.	**1**	14
PRA	Le Plan de reprise d'activité s'inscrit dans le PCA. Il permet, en cas de crise majeure ou sinistre, de pouvoir assurer les activités essentielles en basculant, pendant une durée déterminée, sur un système de relève qui fournira les services nécessaires à la survie de l'entreprise. De façon transitoire, pendant la bascule sur le système de relève, le PRA peut autoriser une coupure intégrale du service.	**9**	-
Principe de non répudiation renforcée	Capacité à s'assurer de l'authenticité de l'émetteur d'un message.	**2**	19
PSSI	La Politique sécurité des systèmes d'information est un plan d'actions et un ensemble de règles définies par une organisation pour maintenir ses systèmes d'information à un certain niveau de sécurité.	**9**	-
RACI	Le RACI est un outil de formalisation des rôles et responsabilités pour chaque partie prenante au projet. Cet outil est indispensable pour établir les attendus vis-à-vis de chaque partie prenante et ainsi lever toute ambiguïté dans les processus de décision. • R : Responsable, ou Réalisateur • A : Approbateur (« Accountable » en anglais). • C : Consulté • I : Informé Il ne peut y avoir qu'un seul A par tâche.	**2 et 4**	19, 21, 36, 37
RFID	Pour « Radio Frequency Identification », désigne la technologie permettant de scanner des produits en masse sans avoir à les voir ni les toucher. Cette technologie d'identification automatique permet ainsi un gain de temps dans le stockage et la recherche de produits.	**1**	15
RPO	Pour « Recovery Point Objective » ou Perte de Données Maximale Admissible. Cet indicateur désigne la durée maximale d'enregistrement des données qu'il est acceptable de perdre lors d'une panne. Ce critère définit l'état dans lequel doit se trouver le nouveau système après basculement.	**2 et 9**	23

TERME	DÉFINITION	N° DE FICHE	N° DE PAGE
RTO	Pour « Recovery Time Objective » ou Durée maximale d'interruption admissible. C'est le délai de rétablissement d'un processus, à la suite d'un incident majeur, pour éviter des conséquences importantes associées à une rupture de la continuité d'activité. Il définit le temps alloué pour faire le basculement vers le nouveau système.	**2 et 9**	23
SaaS	Pour « software as a service », ou logiciel en tant que service, est un modèle d'exploitation commerciale des logiciels dans lequel ceux-ci sont installés sur des serveurs distants plutôt que sur la machine de l'utilisateur.	**2 et 7**	20, 52
SDSI	Schéma directeur du système d'information. Il planifie et organise sur le long terme les évolutions du système d'information en accord avec la stratégie d'entreprise pour aboutir à un modèle de développement optimal. Ce document de synthèse est établi par la direction informatique et validé par la direction générale de l'organisation.	-	
SIEM	Pour « Security Information Management System ». Dispositif situé entre la périphérie et le cœur du réseau local où sont hébergées les données sensibles. L'outil centralise et enregistre l'activité des utilisateurs pour consultation ultérieure et traquer les événements qui surviennent. Le SIEM exploite le fait qu'une attaque informatique laisse toujours des traces au sein des différents journaux d'activités du système.	**10**	-
SOD	Pour « Segregration of duties » ou séparation des droits et accès. Il s'agit de séparer les responsabilités entre plusieurs personnes afin d'éviter les risques de conflits d'intérêts et de fraudes. Une seule personne ne peut effectuer ou masquer seule des actions de fraude ou des erreurs.	**2 et 3**	21, 22, 28
Vente multi canal	Le canal étant une interface par laquelle le client passe à l'acte d'achat, le multi canal se caractérise par le fait de pouvoir vendre son produit par plusieurs canaux (magasins, site e-commerce, application pour téléphone...).	**1**	14
Virus informatique	Un virus informatique est un automate autoréplicatif conçu pour se propager à d'autres ordinateurs en s'insérant dans des logiciels légitimes, appelés « hôtes ». Il peut perturber plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut se répandre par tout moyen d'échange de données numériques comme les réseaux informatiques et les cédéroms, les clefs USB, les disques durs, etc. Les virus informatiques ne doivent pas être confondus avec les vers informatiques, qui sont des programmes capables de se propager et de se dupliquer par leurs propres moyens sans contaminer le programme hôte.	**10**	58, 68
Zero day	Se dit d'une faille dans un logiciel ou système d'exploitation qui n'a pas encore été publiée sur Internet et qui, par conséquent, n'est connue que de quelques-uns. Dès lors, ces initiés peuvent exercer un chantage en menaçant les entreprises qui utilisent l'applicatif vulnérable de publier la faille sur des sites spécialisés.	**10**	-

* non présent dans le document, donné à titre informatif.

L'audit va disparaître... Nous parlons bien entendu de l'audit traditionnel, le papier crayon, qui subsiste encore chez certains de nos confrères mais dont les centaines de milliers de données manipulées par les entreprises leur mènent la vie dure.

Notre profession se doit d'évoluer pour continuer à accompagner les entreprises de plus en plus informatisées et conserver le contrôle des données financières analysées dans un contexte de cas de fraude en croissance permanente. Après une série de conférences et formations sur le rôle du commissaire aux comptes dans la lutte anti-fraude organisées entre 2015 et 2016, la CRCC de Paris, sous l'impulsion de Frédéric Burband, vice-président, a décidé de créer le **groupe de travail "Audit informatique"**, en partenariat avec l'AFAI, qui rassemble des **spécialistes du contrôle interne informatique et de l'analyse de données informatiques.**

CRCC
COMPAGNIE REGIONALE DES COMMISSAIRES AUX COMPTES
PARIS

50, RUE DE LONDRES
75008 PARIS
01 53 83 94 33
WWW.CRCC-PARIS.FR