

AUDIT INFORMATIQUE : TOUS CONCERNÉS !

LE GUIDE PRATIQUE COMPLET 2019



SUR LE CHEMIN DE LA RECONQUÊTE

ÉDITO

Voici 2 ans que le groupe de travail Audit informatique (GT) a diffusé son premier recueil de fiches pratiques avec l'objectif de vous aider à mieux appréhender le système d'informations dans le cadre de votre mission de certification, et de développer les opportunités d'échange avec votre client.

Un client dont le besoin de sécurité et de conformité ne fait qu'augmenter à mesure qu'il s'équipe de nouveaux outils numériques de gestion et de production, et échange des données en quantité de plus en plus importante sur différents réseaux.

Ces 2 dernières années marquées par les cyberattaques à l'échelle mondiale, l'entrée en vigueur du RGPD, pour ne citer que ces exemples, ont renforcé la volonté du GT de vous apporter des clés pour répondre aux besoins d'accompagnement des chefs d'entreprise face à ces nouveaux risques et nouvelles régulations.

Ont également vu le jour à son initiative, les Matinales, un nouveau rendez-vous bimestriel pour enrichir votre veille technologique grâce aux éclairages d'experts, démos d'outils et témoignages : de la data analyse à la cybersécurité, en passant par la Business intelligence, la blockchain, le big data et les ICO, ...

Ces Matinales sont organisées depuis décembre 2018 en partenariat avec le comité Innovation de l'OEI Paris Ile-de-France avec qui nous avons également uni nos forces pour créer un observatoire, le Lab50, dont la mission est d'analyser les impacts de l'intelligence artificielle sur nos métiers. Le Lab50 livre ses décryptages, diffuse les témoignages inspirants, composantes d'un changement de culture profond au sein de la profession comptable et bientôt ira plus loin à travers des propositions concrètes.

Ce changement de culture est également la conséquence des bouleversements réglementaires qui impactent nos professions.

L'adoption de Pacte bouleverse la profession de commissaire aux comptes. Pour autant, face à cette nouvelle donne, nous devons nous repositionner avec vigueur et créativité pour répondre aux attentes du marché et imaginer de nouvelles voies.

Le GT Audit informatique poursuit son ambition d'aider les consœurs et les confrères à développer une offre de services dans le domaine de l'audit des systèmes d'information.

Dans cette perspective, il a conçu plusieurs SACC en lien avec les fiches pratiques du guide de 2017 que vous pourrez découvrir en deuxième partie du guide mis à jour et enrichi d'une synthèse de cartographie des risques.

Enfin, nous souhaitons saluer les initiatives parallèles portées par d'autres CRCC, ainsi que la CNCC à travers notamment le développement de l'outil CyberAudit, participant ainsi à un élan général de transformation des compétences des auditeurs.

Nous remercions Farouk Boulbarhi, président de la CRCC d'Aix Bastia, et Christelle Dorison Fourquet, élue, présidente de la commission Intelligence économique et Cybersécurité de cette CRCC, pour s'être associés à la réalisation de ce guide nouvelle version.

Bien confraternellement,

Olivier Salustro,
président de la CRCC de Paris

GROUPE DE TRAVAIL AUDIT INFORMATIQUE DE LA CRCC DE PARIS



FRÉDÉRIC BURBAND



SERGE YABLONSKY



FLORIAN ABEGG



JEAN-LUC AUSTIN



JEAN-MICHEL DENYS



SÉBASTIEN DIENE



CHRISTELLE DORISON
FOURQUET



CHRISTIAN GABENESCH



DIENEBA GANDEGA



JÉRÔME HUBER



JEAN-CLAUDE
N'GUESSAN



MICHEL RETOURNÉ

AUDIT INFORMATIQUE : TOUS CONCERNÉS !
LE GUIDE PRATIQUE COMPLET 2019

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

Serge Yablonsky

Expert-comptable, commissaire aux comptes, président d'honneur de l'AFAI

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

Florian Abegg

Directeur Audit IT chez Grant Thornton

Jean-Luc Austin

Associé Audit et Conseil SI chez Exponens

Jean-Michel Denys

Managing Partner des activités de Consulting du cabinet CTF, Compagnie des Techniques Financières

Sébastien Diene

Superviseur audit chez Grant Thornton

Christelle Dorison Fourquet

Commissaire aux comptes, Présidente de la commission Intelligence Economique et Cybercriminalité des Entreprises à la CRCC Aix-Bastia

Christian Gabenesch

DSI cabinet FIDELIANCE et auditeur des systèmes d'information

Dieneba Gandega

Expert-comptable, commissaire aux comptes, Groupe AFIGEC

Jérôme Huber

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

Jean-Claude N'Guessan

Senior Manager chez RSM France

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 ! »
PLUS DE 250 MEMBRES !

INTRODUCTION

AUDIT INFORMATIQUE, TOUS CONCERNÉS !

Notre profession accompagne des entreprises de plus en plus informatisées, collectant et traitant des millions de données. Elle se doit donc d'évoluer pour conserver le contrôle des données financières analysées dans un contexte de cas de fraude en croissance permanente. Après une série de conférences sur le rôle du commissaire aux comptes dans la lutte anti-fraude organisées dès 2015, 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 depuis 2016 est d'ouvrir nos consœurs et confrères à l'**utilisation des outils d'analyse de données** répondant au double objectif de sécurisation de leur mission et d'efficacité dans les réponses à apporter aux besoins des entreprises que nous accompagnons.

Par ailleurs, il est également nécessaire de les **sensibiliser sur les risques de la digitalisation des processus de l'entreprise** tels que la perte de continuité d'activité ou encore la 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 engagée 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, contrôle informatisé...

Un jargon de plus en plus courant dans nos échanges, sans pour autant être toujours maîtrisé. Le groupe de travail est donc là pour réfléchir à de nouvelles manières de présenter ces concepts et de les rendre accessibles à tous.

Notre groupe a donc travaillé à l'élaboration de ce guide pratique dans l'objectif de :

- 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** qui y sont liés
- d'**apporter des réponses et une méthodologie** applicable directement dans leurs missions
- de leur **permettre de développer une offre de services d'audit informatique**

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...

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 pour mesurer son niveau d'ouverture sur le numérique et d'exposition aux risques.

INTRO

La synthèse de **cartographie des risques, sous forme de rosace**, traduit visuellement ces niveaux et facilite la communication avec le client. Elle l'aide à prendre des décisions de mise en œuvre de missions plus pointues sur un ou plusieurs domaines dans le cadre de services autres que la certification des comptes.

Un **glossaire** est fourni pour ne rien manquer des termes techniques applicables ainsi que des références pour aller plus loin dans le domaine concerné.

COMMENT UTILISER CE GUIDE ?

11 DOMAINES ABORDÉS : 10 QUESTIONNAIRES DE CONDUITE D'ENTRETIEN ET 11 SACC POUR DEVELOPPER VOTRE OFFRE DE SERVICE EN AUDIT DES SI

Afin d'avoir une vision globale de son système d'informations et lui présenter une cartographie exhaustive des risques (cf. rosace), il est recommandé d'aborder tous les domaines avec son client. Néanmoins, chaque questionnaire peut être utilisé indépendamment des autres.

Des versions Word des fiches seront téléchargeables sur le site de la CRCC de Paris.

La mise en œuvre des SACC dépendra de la teneur de l'entretien avec le chef d'entreprise et du niveau de risque détecté.

STRUCTURE DU GUIDE

GOVERNANCE D'ENTREPRISE
Ouverture sur la transformation numérique
Gouvernance des systèmes d'information
Audit de services externalisés
RISQUES OPÉRATIONNELS
Contrôle des accès
Conduite de projets
Exploitation des systèmes d'information
Plan de continuité d'activité
Cybersécurité - Cybercriminalité
ACTIVITÉS DE CONTRÔLE
Utilisation des outils d'audit de données
Protection des données personnelles
Législation fiscale et SI

PARTIE 1 : FICHES PRATIQUES AUDIT INFORMATIQUE

FICHE 01 Ouverture sur la transformation numérique	12
FICHE 02 Gouvernance des systèmes d'information	18
FICHE 03 Contrôle des accès	30
FICHE 04 Conduite de projets	38
FICHE 05 Utilisation des outils d'audit de données	46
FICHE 06 Protection des données personnelles	52
FICHE 07 Législation fiscale et SI	58
FICHE 08 Exploitation des systèmes d'information	66
FICHE 09 Plan de continuité d'activité	72
FICHE 10 Cybersécurité	78
SYNTHÈSE DE LA CARTOGRAPHIE DES RISQUES I	84

PARTIE 2 : SACC AUDIT INFORMATIQUE

FICHE 01 Ouverture sur la transformation numérique	92
FICHE 02 Gouvernance des systèmes d'information	98
FICHE 03 Contrôle des accès	104
FICHE 04 Conduite de projets	110
FICHE 05 Utilisation des outils d'audit de données	116
FICHE 06 Protection des données personnelles	118
FICHE 07 Législation fiscale et SI	126
FICHE 08 Exploitation des systèmes d'information	132
FICHE 09 Plan de continuité d'activité	138
FICHE 10 Cybercriminalité	144
FICHE 11 Audit de services externalisés	152
GLOSSAIRE I	158
POUR ALLER PLUS LOIN I	166

PARTIE 1

10 FICHES PRATIQUES POUR RÉUSSIR

OUVERTURE SUR LA TRANSFORMATION NUMÉRIQUE

AUDIT INFORMATIQUE : TOUS CONCERNÉS !
10 FICHES PRATIQUES POUR RÉUSSIR

FICHE 01

OUVERTURE SUR LA TRANSFORMATION NUMÉRIQUE

01

CONTEXTE ET ENJEUX

Qu'est-ce que la transformation numérique ? La transformation numérique encore appelée transformation digitale est la création, l'utilisation et le partage de données numériques en vue de création de nouveaux services à usage externe ou interne. C'est donc le processus permettant aux entreprises d'intégrer l'usage de toutes les technologies digitales relatives à leurs activités. Elle a impacté les offres aux consommateurs tout comme la pratique des consommateurs, ainsi que la culture d'entreprise en modifiant les mentalités et ses processus. L'adaptation à cette évolution digitale est l'une des priorités majeures pour les entreprises voulant rester compétitives, d'autant que cette révolution ne semble pas ralentir, bien au contraire.

Le numérique s'impose comme un enjeu stratégique majeur de vie ou de mort pour les entreprises. Pourquoi ? Parce que les implications sont multiples ; elles touchent les offres et les business model, 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 apparaître 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.

Le pilier technologique de la transformation digitale comprend le déploiement de différentes techniques telles que le cloud, la réalité virtuelle et l'intelligence artificielle. Une transformation numérique réussie doit intégrer l'ensemble de ces volets afin de mieux exploiter les données accumulées depuis des années par les entreprises.

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 de la CNCC relative aux prestations entrant dans le cadre des Services Autres que la Certification des Comptes (SACC).

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 des ses managers.

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, de la mise en place d'objets connectés, de la meilleure connaissance des clients par la « data » permettent d'augmenter la compétitivité des entreprises et de mieux contribuer à son écosystème.

Une meilleure connaissance du client passe par une meilleure exploitation de la data qui reste une source d'informations précieuses en matière de transformation digitale. Il est judicieux de faire parler les données accumulées depuis plusieurs années.

Ce constat est important, car la bataille du rapport qualité/prix touche désormais tous les secteurs (y compris les professionnels du chiffre) et en devient une obligation cruciale pour la survie des entreprises.

Écologique : L'empreinte écologique fait désormais partie de notre quotidien, tant sur des plans personnels que professionnels. 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 impact 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 entité.

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 ont mal pris le virage du numérique (NOKIA, KODAK...). En tant que Dirigeants, les impacts liés à cette transformation doivent être anticipés, maîtrisés, et les investissements nécessaires effectués.

Cette approche pousse à décomposer l'analyse de la performance selon 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 ses offres collent aux émotions et attentes de ses clients ?
- Comment sont mesurées les performances opérationnelles des différentes lignes de produits et services ?

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

FICHE 01

OUVERTURE SUR
LA TRANSFORMATION NUMÉRIQUE



Thème / Question	Enjeu / Risque associé	Interlocuteur concerné	Réponse attendue
Les responsables opérationnels ont-ils compris les enjeux et les contraintes du numérique ? (nouveautés, changements de relations inter-personnelles, rythme des évolutions , ...)	Continuité d'activité	DG	OUI - Utilisation des outils collaboratifs - MOOC
L'informatique numérique dispose de ressources spécifiques, en termes de finance, de gestion de la complexité, de maîtrise 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 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 pris en compte dans les projets numériques ?	-	Le DG, la DSI	OUI - Application GDPR (cf. fiche données personnelles)
La culture de l'entreprise est propice à la transformation numérique	-	Le DG, la DSI	OUI - Bureau dynamique - Innovation favorisée
Les évolutions numériques intègrent 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 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 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

Thème / Question	Enjeu / Risque associé	Interlocuteur concerné	Réponse attendue
Les processus sont documentés et partagés au niveau de la Direction Générale et des décideurs opérationnels en charge de l'offre et s'ajustent avec l'environnement grâce au numérique.	-	Le DG, La DSI	OUI - Cartographie des processus - approche transversale Culture projet
Le numérique développe 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 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

MATURITÉ DE L'ENTREPRISE EN MATIÈRE DE TRANSFORMATION NUMÉRIQUE :

Ce tableau sera repris dans la synthèse globale de cartographie des risques en fin de première partie.

Le niveau de risque sera noté comme suit :

- > 1 : Faible
- > 2 : Moyen
- > 3 : Elevé

Evaluation du risque	Niveau de risque	Commentaire
Incidence		
Probabilité d'occurrence		

EXEMPLES DE BONNES PRATIQUES :

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

- > Intégrer la digitalisation dans la stratégie globale de l'entreprise
- > Mettre le client au centre de ses préoccupations
- > Ne pas négliger la data et s'équiper pour la collecter
- > Former le personnel au numérique

FICHE 02

GOUVERNANCE DES SYSTÈMES D'INFORMATION

02

Pourquoi parler de gouvernance des 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 processus 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. L'alignement du système d'information avec les besoins métiers de l'entreprise est au cœur même du référentiel COBIT.

En effet, le COBIT promeut un SI, à travers les technologies de l'information, cohérent avec les objectifs et la stratégie de l'entité. Ainsi, il donne une liste détaillée de plusieurs objectifs (300) sur lequel l'auditeur des systèmes d'information doit s'appuyer pour vérifier cet alignement.

Permettant une évaluation de la maturité des processus et de la maîtrise du système d'information, le COBIT est donc un outil de dialogue entre la direction et le directeur du système d'information (DSI).

Le COBIT peut permettre de mettre en place un modèle de gouvernance du système d'information qui lui permettra d'identifier les axes d'amélioration et les pistes de progrès. La gouvernance des SI recouvre de multiples dimensions. Dans une perspective d'audit, nous en avons retenu 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**

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 comme la propriété des applications et des données est un point central de l'appréhension des risques constitutifs de l'information comptable et financière.

GOUVERNANCE DES SYSTÈMES D'INFORMATION

FICHE 02

GOVERNANCE DES SYSTÈMES D'INFORMATION

NEP ET TEXTES DE RÉFÉRENCE

- **NEP 315** : Connaissance de l'entité et de son environnement et évaluation du risque d'anomalies significatives.
- **COBIT** (Common Objectives for Business Information Technology) qui a pour but l'alignement des objectifs et la stratégie de l'organisation avec les technologies de l'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, comprenant sa bonne évolution et 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, mais il appartient également à chaque propriétaire d'application et chaque propriétaire 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 des prises de décision inappropriées pourraient 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
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
Le management de la fonction informatique est-il 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
Si oui, à qui cette personne est-elle rattachée hiérarchiquement ?	Identification du niveau de contrôle	DG	DG
Un responsable de la sécurité informatique a-t-il été 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
Le directeur financier a-t-il défini des points de contrôle permettant de superviser la production de l'information comptable et financière ?	Appréciation du niveau de maîtrise du système d'information par le directeur financier	DAF	OUI

B. MANAGEMENT ET RESPONSABILITÉ

Thème / Question	Enjeu / Risque associé	Interlocuteur cible	Réponse attendue
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
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
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
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



FICHE 02

GOVERNANCE DES SYSTÈMES D'INFORMATION

GOVERNANCE 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.

Raisonnement 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 de la CNCC relative aux prestations entrant dans le cadre des Services Autres que la Certification des Comptes (SACC)
- **COBIT** (Common Objectives for Business Information Technology) qui a pour but l'alignement des objectifs et la stratégie de l'organisation avec les technologies de l'information

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, comptes 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 réglementaires.

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'ambiguïté > 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 RGPD 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 de la CNCC relative aux prestations entrant dans le cadre des Services Autres que la Certification des Comptes (SACC)
- **COBIT** (Common Objectives for Business Information Technology) qui a pour but l'alignement des objectifs et la stratégie de l'organisation avec les technologies de l'information

ANALYSE DES 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
- Cyberattaque

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.
- **RGPD** : 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 qualitatives et quantitatives ?	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



FICHE 02

GOVERNANCE DES SYSTÈMES D'INFORMATION

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 connaître 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.
- **COBIT** (Common Objectives for Business Information Technology) qui a pour but l'alignement des objectifs et la stratégie de l'organisation avec les technologies de l'information.

ANALYSE DES 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) faisant apparaître 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	Interlocuteur cible	Réponse attendue
A. Composantes du SI Le système d'information est-il basé sur un ERP ?	<ul style="list-style-type: none"> • Niveau d'intégration du système d'information • Nombre importants d'interface à contrôler • Exposition à la contagion des anomalies en cas de faiblesse de contrôle 	Personne en charge > identifier selon la taille et l'activité de l'entreprise : DSI, DAF, DG, autre...	OUI
A. Composantes du SI Une dépendance forte existe-t-elle entre les applications, les choix technologiques et les choix d'infrastructures ?	<ul style="list-style-type: none"> • Continuité d'activité et capacité d'évolution du SI 	DSI et/ou DAF	OUI
A. Composantes du SI Existe-t-il des applications dites « périphériques » de type Excel ou Access ?	<ul style="list-style-type: none"> • Accès aux données : fichiers extra-système peu sécurisés • Intégrité : données et calculs ouverts et non protégés 	DSI et/ou DAF	OUI
B. Connaissance du SI et couverture fonctionnelle Une cartographie du système d'information est-elle formalisée et maintenue à jour de manière régulière ?	<ul style="list-style-type: none"> • Connaissance des applications sources et des traitements • Maîtrise des risques liés aux évolutions du SI 	DSI et/ou DAF	OUI
B. Connaissance du SI et couverture fonctionnelle Les flux ayant un impact sur l'information comptable et financière sont-ils identifiés ?	<ul style="list-style-type: none"> • Connaissance des applications sources et des traitements • Maîtrise des risques liés aux évolutions du SI 	DSI et/ou DAF	OUI
B. Connaissance du SI et couverture fonctionnelle Une matrice de couverture des processus par les applications est-elle renseignée ?	<ul style="list-style-type: none"> • Connaissance des applications sources et des traitements • Maîtrise des risques liés aux évolutions du SI 	DSI et/ou DAF	OUI



FICHE 02

GOVERNANCE DES SYSTÈMES D'INFORMATION

QUESTIONNAIRE

Thème / Question	Enjeu / Risque associé	Interlocuteur cible	Réponse attendue
C. Cohérence et évolution du SI Si certains processus ne sont pas couverts par le système d'information, est-il 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
C. Cohérence et évolution du SI Les évolutions métiers sont-elles 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
D. Interfaces applicatives Certaines interfaces reposent sur la génération 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
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

MATURITÉ DE L'ENTREPRISE EN MATIÈRE DE GOUVERNANCE SI :

Ce tableau sera repris dans la synthèse globale de cartographie des risques en fin de première partie.

Le niveau de risque sera noté comme suit :

- 1 : Faible
- 2 : Moyen
- 3 : Elevé

Evaluation du risque	Niveau de risque	Commentaire
Incidence		
Probabilité d'occurrence		

EXEMPLES DE BONNES PRATIQUES :

- Formaliser l'organigramme de la fonction informatique et l'actualiser de manière régulière ;
- Formaliser et maintenir à jour la cartographie du système d'information ;
- Définir les rôles et responsabilités de chaque membre de la direction SI et formaliser les fiches de poste ;
- Formaliser les politiques et les procédures liées à la gouvernance du SI y compris les différents comités et les modalités afférentes (fréquence, participants...);
- Formaliser toutes les demandes d'évolution du SI et conserver toutes les procédures de validation ;
- S'assurer que les SI permettent de faciliter la mise en œuvre de la stratégie de l'entreprise.



CONTRÔLE DES ACCÈS

AUDIT INFORMATIQUE : TOUS CONCERNÉS !
10 FICHES PRATIQUES POUR RÉUSSIR

FICHE 03 CONTRÔLE DES ACCÈS

03

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 :

- la 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 fonctionnalités), ce qui suppose une communication permanente pour une mise à jour des profils utilisateurs et droits d'accès correspondant en fonction de l'évolution des effectifs (entrées / 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.

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)

FICHE 03 CONTRÔLE DES ACCÈS

ANALYSE DES RISQUES ET CRITICITÉ

DROITS D'ACCÈS ET SÉPARATION DES TÂCHES

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			X
Déclencher un paiement			X
Créer / modifier / supprimer un RIB fournisseur			X
Autoriser un investissement			X
Passer une commande		X	
Contrôler une réception		X	
Comptabiliser une facture		X	
Lettrer un compte fournisseur		X	
Saisir une réception	X		
Scanner une information	X		

ILLUSTRATION SUR LE CYCLE DES VENTES :

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

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).

FICHE 03
CONTRÔLE DES ACCÈS



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	gris	rouge	rouge	jaune	jaune	rouge	vert	vert	vert
2	RIB fournisseur	rouge	gris	rouge	vert	vert	rouge	jaune	jaune	vert
3	Passation de commande	rouge	rouge	gris	jaune	jaune	rouge	vert	vert	vert
4	Réception	jaune	vert	jaune	gris	jaune	rouge	vert	vert	vert
5	Contrôle facture fournisseur	jaune	vert	jaune	jaune	gris	rouge	jaune	vert	vert
6	Paiement fournisseur	rouge	rouge	rouge	rouge	gris	rouge	rouge	jaune	jaune
7	État de rapprochement bancaire	vert	jaune	vert	vert	jaune	rouge	gris	jaune	vert
8	Lettrage compte fournisseur	vert	jaune	vert	vert	rouge	jaune	gris	vert	vert
9	Rapprochement BA / BG	vert	vert	vert	vert	jaune	vert	vert	vert	gris

CYCLE DES VENTES

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

■ 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. Lors des phases de planification et de réalisation de l'audit, le CAC 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.

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 audité 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

FICHE 03 CONTRÔLE DES ACCÈS

QUESTIONNAIRE

Question	Enjeux / Risques associés	Interlocuteur concerné	Réponse attendue
L'attribution des droits d'accès se fait-elle selon la règle : «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 minimum, 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
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

QUESTIONNAIRE

Question	Enjeux / Risques associés	Interlocuteur concerné	Réponse attendue
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

MATURITÉ DE L'ENTREPRISE EN MATIÈRE DE CONTRÔLE DES ACCÈS :

Ce tableau sera repris dans la synthèse globale de cartographie des risques en fin de première partie.

Le niveau de risque sera noté comme suit :

- 1 : Faible
- 2 : Moyen
- 3 : Elevé

Evaluation du risque	Niveau de risque	Commentaire
Incidence		
Probabilité d'occurrence		

EXEMPLES DE BONNES PRATIQUES :

- Bien choisir son mot de passe : Longueur minimal de 8 caractères avec des caractères de types différents (majuscules, minuscules, chiffres, caractères spéciaux et n'ayant aucun lien avec vous (nom, date de naissance..) et ne figurant pas dans le dictionnaire ;
- Modifier régulièrement les mots de passe (tous les 3 mois par exemple) ;
- Mettre en place une double authentification pour les accès sensibles (administrateur, ...);
- Avoir une politique claire de gestion des droits d'accès (attribution / création / retrait / suppression des droits d'accès) ;
- Interdire aux collaborateurs de préenregistrer/ communiquer/ partager ou mettre sur un post-it leurs mots de passe ;
- Avoir une politique claire de chiffrement des données ;
- Sécuriser l'accès wifi de votre entreprise, avec un réseau spécifique pour les invités.

CONDUITE DE PROJETS

AUDIT INFORMATIQUE : TOUS CONCERNÉS !
10 FICHES PRATIQUES POUR RÉUSSIR

FICHE 04 CONDUITE DE PROJETS

04

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** : les projets ont été menés selon les règles de l'art et respectent un cadre de contrôle interne suffisant.
- **En termes de données** : les données et états financiers impactés ou produits à l'issue des projets 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

- PRINCE2
- PMBOK
- COBIT5

ANALYSE DE RISQUES ET CRITICITÉ

Le **RACI** est un outil de formalisation des rôles et responsabilités de 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'ordonnement 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	Interlocuteur cible	Réponse attendue ou éléments à collecter
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
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 argumentée
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
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
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
Qui valide les spécifications et de quelle manière ?	Impact sur les process et/ou les états financiers (ex. : refonte de la clé comptable)	Equipe comptable DAF Equipe projet	DAF, DG ou toute personne ayant l'autorité de valiser les process cibles
Qui valide la reprise de données et de quelle manière ?	Exhaustivité, fiabilité, intégrité des données	Equipe comptable avec responsabilité du DAF	DAF, DG

FICHE 04
CONDUITE DE PROJETS

QUESTIONNAIRE

Thème / Question	Enjeu / Risque associé	Interlocuteur cible	Réponse attendue ou élément à collecter
La mise en production du nouveau logiciel comptable a-t-elle lieu au démarrage du nouvel exercice ou bien en cours d'exercice ?	<ul style="list-style-type: none"> Cut-off Reprise des encours en cours d'exercice 	Equipe projet	Démarrage si possible
Le DAF participe-t-il effectivement au comité de pilotage ?	<ul style="list-style-type: none"> Sponsor suffisant en termes de management 	DAF	OUI
Si migration vers une solution cloud, le contrat prévoit-il les clauses ad hoc (auditabilité, réversibilité, RGPD) ?	<ul style="list-style-type: none"> Conformité Délai d'accès aux données sur demande du CAC. 	Equipe projet DAF Juridique	OUI
Phase : Cadrage <ul style="list-style-type: none"> Le planning est-il réaliste ? 	<ul style="list-style-type: none"> Retard du projet. Complexité d'un démarrage en cours d'exercice. 	DAF, DSI	OUI
Phase : Cadrage <ul style="list-style-type: none"> Un Plan d'Assurance Qualité a-t-il été écrit et validé par les parties prenantes ? 	<ul style="list-style-type: none"> Détection et communication des risques projet. Rôles et responsabilités des parties prenantes. Arbitrage. Gestion des litiges. 	Equipe projet DAF DSI	OUI
Phase : Spécifications <ul style="list-style-type: none"> La définition des processus est-elle conforme au besoin ? 	<ul style="list-style-type: none"> 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 fonctionnelles
Phase : Paramétrage <ul style="list-style-type: none"> La solution est-elle utilisée dans sa version standard ? Sinon, quelle est la proportion de développements spécifiques ? 	<ul style="list-style-type: none"> Non respect des règles de gestion. Difficulté de maintenance de migration future. 	DAF DSI	Proportion de customisations
Phase : Paramétrage <ul style="list-style-type: none"> Combien y a-t-il d'interfaces entrantes et sortantes autour de la nouvelle solution ? Quel est le niveau d'intégration global ? 	<ul style="list-style-type: none"> 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
Phase : Tests <ul style="list-style-type: none"> Quelle est la stratégie de tests ? Sur quel volume de données sont-ils réalisés ? Qui a rédigé les scénarios ? 	<ul style="list-style-type: none"> Exhaustivité Fiabilité des données Régression fonctionnelle 	Chef de projet DSI, responsable informatique	Stratégie de tests Scénarios de tests

QUESTIONNAIRE

Thème / Question	Enjeu / Risque associé	Interlocuteur cible	Réponse attendue ou élément à collecter
Phase : Reprise de données <ul style="list-style-type: none"> Nettoyage des données à reprendre Transcodification des règles et référentiels comptables 	<ul style="list-style-type: none"> 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	Documentation Conservation des éléments techniques temporaires (base pivot, fichiers intermédiaires)
Phase : Recette Quelle est l'organisation de la recette en termes de : <ul style="list-style-type: none"> Recetteurs Données de recette Remontée et traitement des anomalies (outil de ticketing) Formalisation de l'acceptation 	Fiabilité des processus	DAF, DC, responsable fonctionnel	Cahier de recette PV de réception dûment signé
Conduite du changement <ul style="list-style-type: none"> Quelles sont les actions de communication et d'accompagnement ? Quelle est la répartition de ces actions sur le planning projet ? 	<ul style="list-style-type: none"> Absence de sponsor Implication insuffisante des utilisateurs. Echec du projet Inadéquation de la solution. 	DG	Démarche
Phase : Mise en production <ul style="list-style-type: none"> Quelle est la politique d'archivage de l'historique ? 	<ul style="list-style-type: none"> Risque de perte de traçabilité de l'information. Perte d'accès aux informations utiles à l'activité ou réglementairement requises. 	DAF	Politique formalisée
Phase : Support post-production <ul style="list-style-type: none"> 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) 	<ul style="list-style-type: none"> 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
Documentation <ul style="list-style-type: none"> La documentation liée au projet est-elle suffisante en qualité et en quantité ? Exemples : expression des besoins, planning, note de cadrage, spécifications (fonctionnelles et techniques), cahier de recette,... 	Auditabilité du projet Conformité	DG, DAF, DSI	Accès à la documentation



FICHE 04

CONDUITE DE PROJETS

04

QUESTIONNAIRE

Thème / Question	Enjeu / Risque associé	Interlocuteur cible	Réponse attendue ou élément à collecter
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 basculant les coûts en Tierce Maintenance Appllicative	DG, DAF	Détail de la comptabilisation des dépenses liées au projet
Subventions Le projet fait-il l'objet d'un Crédit d'impôt recherche ?	Correcte imputation des subventions	DG, DAF	En fonction de la réponse

MATURITÉ DE L'ENTREPRISE EN MATIÈRE DE CONDUITE DE PROJETS :

Ce tableau sera repris dans la synthèse globale de cartographie des risques en fin de première partie.

Le niveau de risque sera noté comme suit :

- 1 : Faible
- 2 : Moyen
- 3 : Elevé

Evaluation du risque	Niveau de risque	Commentaire
Incidence		
Probabilité d'occurrence		

EXEMPLES DE BONNES PRATIQUES :

- Mettre en place une équipe pour chaque projet et nommer un responsable de projet ;
- Définir les rôles et responsabilité de chaque partie prenante (formaliser par exemple un RACI) ;
- Formaliser par écrit une charte par projet et la faire approuver par l'ensemble des parties prenantes ;
- Documenter chaque projet (expression des besoins, planning, spécifications fonctionnelles et techniques, cahier de recette...);
- Faciliter la communication et la coopération entre les différentes parties prenantes ;
- Effectuer un suivi périodique de l'avancement du projet ;
- Adopter une démarche d'amélioration continue.

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 transaction 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. L'analyse des données constitue alors une approche qualitative qui permet au commissaire aux comptes de s'assurer de la correcte traduction dans les comptes des données qui peuvent parfois se déverser de manière automatique dans les différents systèmes de gestion de l'entreprise.

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

Enfin, l'analyse des données crédibilise le commissaire aux comptes, améliore son image et lui offre des opportunités de missions spécifiques à forte valeur ajoutée vis-à-vis du client.

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.

UTILISATION DES OUTILS D'AUDIT DE DONNÉES

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.

Ci-dessous un tableau de comparaison des principaux outils d'analyse de données :

Critères	ACL	IDEA	EXCEL	BASE DE DONNÉES
Capacité volumétrique	Illimitée	Illimitée	Limitée à 65 536 lignes	Illimitée
Capacité de traitement	Suffisante	Suffisante	Limitée	Illimitée
Type de fichier importé	Tout type de fichier	Tout type de fichier	Majorité des fichiers ASCII	Majorité des fichiers ASCII
Intégrité des données	Garantie	Garantie	Impossible	A réaliser
Piste d'audit	Garantie	Garantie	Impossible	A réaliser
Investissement financier	Elevé	Elevé	Faible	Elevé
Recherche	Extract	Extract	Copier/coller	Requête d'extraction

Les fichiers sources possibles :

➤ **Fichier des Écritures 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 y 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, et la rendre pertinente pour le client, les fonctionnalités suivantes ont été identifiées comme nécessaires pour 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 de sensibilisation du chef d'entreprise en lien avec le risque de fraude ou de transaction non fondée.

L'analyse des données peut être envisagée soit :

- Lors de l'intérim : cibler les zones à risques ou éliminer les risques hypothétiques non avérés ;
- Lors de la phase finale : apporter des constats chiffrés et étayer l'opinion du commissaire aux comptes.

05

FICHE 05

UTILISATION DES OUTILS D'AUDIT DE DONNÉES

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 est présenté
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, montants 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 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 - identifier et analyser 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.

QUESTIONNAIRE

Thème / Question	Enjeux et Risques associés	Interlocuteur concerné	Réponse attendue
Mise en œuvre des contrôles : - réaliser les tests tels que définis 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

MATURITÉ DE L'ENTREPRISE EN MATIÈRE D'UTILISATION DES OUTILS D'AUDIT DES DONNÉES :

Ce tableau sera repris dans la synthèse globale de cartographie des risques en fin de première partie.

Le niveau de risque sera noté comme suit :

- 1 : Faible
- 2 : Moyen
- 3 : Elevé

Evaluation du risque	Niveau de risque	Commentaire
Incidence		
Probabilité d'occurrence		

EXEMPLES DE BONNES PRATIQUES :

- Déterminer le périmètre et les objectifs de contrôle ;
- Identifier les fichiers nécessaires et respecter certaines règles quant à l'extraction de ces fichiers ;
- Anticiper la demande des fichiers suffisamment à l'avance de manière officielle (par mail par exemple) ;
- Toujours contrôler l'intégrité des fichiers obtenus lors de l'importation (« butée de contrôle » : obtenir au moment de l'extraction, un état ou une copie d'écran qui totalise la population auditée extraite du SI de l'entreprise).

PROTECTION DES DONNÉES PERSONNELLES

AUDIT INFORMATIQUE : TOUS CONCERNÉS !
10 FICHES PRATIQUES POUR RÉUSSIR

FICHE 06 PROTECTION DES DONNÉES PERSONNELLES

06

CONTEXTE ET ENJEUX

Le Règlement général sur la protection des données s'inscrit dans un contexte Européen. Entré en vigueur depuis le 25 mai 2018, le RGPD a pour objectif de :

- › Renforcer les droits des personnes (portabilité des données personnelles, droit à l'oubli avec preuve, consentement sur les traitements, information si violation...);
- › Responsabiliser les acteurs traitants les données (renversement de la charge de la preuve, obligation de notifier les violations du RGPD à la CNIL et aux personnes concernées...);
- › Crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données des Etats membres, qui pourront notamment adopter des décisions communes lorsque les traitements de données seront transnationaux, et des sanctions renforcées.

Rappelons qu'une donnée à caractère personnel est toute information se rapportant à une personne physique identifiée ou identifiable.

Les données peuvent être directement identifiantes (nom, prénom, numéro sécurité sociale...) ou indirectement identifiantes (localisation, empreinte digitale, plaque d'immatriculation...).

Toute entreprise est soumise au RGPD en cas de possession des données à caractère personnel et quel que soit le mode de traitement (informatisé ou manuel).

Ainsi, elle sera tenue de maintenir un registre des traitements et de désigner un délégué à la protection des données - DPO¹ (data protection officer) dans les mêmes conditions qu'un responsable de traitement.

Cette tenue de registre obligatoire remplace les déclarations à la CNIL et permet de consigner les mêmes informations que dans la déclaration.

De par le RGPD, l'entreprise est responsable de la sécurité informatique nécessaire au respect de la protection des données. La sécurité informatique devient ainsi une obligation légale.

L'entreprise devient garante du respect de la vie privée.

¹ Selon l'article 37 du RGPD, la désignation est obligatoire dans les cas suivants :

- Être une autorité ou un organisme public ;
- Avoir une activité nécessitant un suivi régulier et systématique des personnes à grande échelle ;
- Traiter de données sensibles comme celles qui se rattachent à l'origine raciale, aux opinions politiques, philosophiques ou religieuses, à la santé, vie sexuelle etc.

A noter que la désignation d'un DPO est encouragée par le CNIL et les autorités Européennes

FICHE 06

PROTECTION DES DONNÉES PERSONNELLES

Cette nouvelle réglementation Européenne apporte une protection plus forte mais des contraintes et des responsabilités plus lourdes pour les entreprises.

Les risques sont importants et nécessitent une analyse particulière de la part du commissaire aux comptes, ce qui pourrait apporter une forte valeur ajoutée au client.

La non-conformité au RGPD est sanctionnée de 10 à 20 millions d'euros ou de 2 à 4% du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu en fonction de la gravité du non-respect du règlement.

De plus, l'entreprise peut être confrontée à un risque accru sur la réputation et l'image (perte de clientèle) et un droit à réparation dans le cadre d'une action collective intentée par les personnes concernées.

Attention, à l'instar d'autres réglementations, c'est maintenant à l'entreprise de démontrer qu'elle est en conformité. Le RGPD 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.

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 à 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'applique 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 non-européennes sont 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) est soumise à ces mêmes réglementations.

Un **transfert**, vers un pays tiers (hors UE et EEE) de données à caractère personnel qui sont destinées à faire l'objet d'un traitement après ce transfert ne peut avoir lieu qu'à condition d'assurer un niveau de protection des données suffisant et approprié, y compris pour les transferts ultérieurs de données à caractère personnel au départ du pays tiers vers un autre pays tiers.

A noter que la CNIL et le G29 (l'ensemble des CNIL européennes) émettent régulièrement des interprétations et des recommandations concernant le RGPD.

L'AFAI a réalisé un modèle de maturité des entreprises dans l'application du RGPD. Les questions ci-après sont une synthèse de ce modèle.

BILAN 1 AN APRÈS L'ENTRÉE EN APPLICATION :

- 2 044 notifications de violation de données en France et 89 271 au niveau européen ;
- Une augmentation considérable des plaintes adressées à la CNIL : plus de 11 900 plaintes en France (+ 30 %) et 144 376 plaintes au niveau européen ;
- Plus de 19 000 délégués à la protection des données (personnes physiques ou morales) ont été désignés par plus de 53 000 organismes ;
- 70 % des Français se disent aujourd'hui plus sensibles aux problématiques de protection des données.

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 est entré en application le 25 mai 2018.

06

FICHE 06 PROTECTION DES DONNÉES PERSONNELLES

ANALYSE DES RISQUES ET FACTEURS DE CRITICITÉ :

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

QUESTIONS POUR ÉVALUER LES RISQUES :

Ce questionnaire peut être réalisé en phase intérimaire comme en phase finale.

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 ?	DPO DSI	OUI
Gouvernance / déontologie	Les données personnelles ont-elles 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 ?	DPO DSI Directions métiers	Demande d'accord exprès sur les sites Enquête de satisfaction Localisation des Data Center en Union Européenne, sinon accord de respect du RGPD
Information	Les responsables des traitements ont-ils été identifiés et peuvent-ils 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) ?	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	La collecte des données a-t-elle reçu le consentement de son intéressé ?	DPO DSI	Demande d'accord exprès
Management	Les modalités du droit à l'information sont-elles établies et appliquées ? Un registre des données et des traitements par finalité est-il 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 ?	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.

MATURITÉ DE L'ENTREPRISE EN MATIÈRE DE DONNÉES PERSONNELLES :

Ce tableau sera repris dans la synthèse globale de cartographie des risques en fin de première partie.

Le niveau de risque sera noté comme suit :

- 1 : Faible
- 2 : Moyen
- 3 : Elevé

Evaluation du risque	Niveau de risque	Commentaire
Incidence		
Probabilité d'occurrence		

EXEMPLES DE BONNES PRATIQUES :

- Sensibiliser les utilisateurs aux enjeux en matière de sécurité et de vie privée ;
- Rédiger une charte informatique et lui conférer une force contraignante ;
- Documenter et mettre à jour de manière régulière toutes les procédures d'exploitation de données personnelles ;
- Mettre à niveau les contrats avec les prestataires pour préciser leurs responsabilités.

FICHE 07 LÉGISLATION FISCALE ET SI

CONTEXTE ET ENJEUX

Depuis le 01 janvier 2014, le contribuable doit satisfaire à une 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 :

- › La fourniture d'une piste d'audit fiable et sa documentation ;
- › Obligation de faire certifier son logiciel de caisse ;
- › Fourniture du fichier FEC à date à la demande du vérificateur ;
- › Conformité au règlement eIDAS¹ en matière de signature électronique ;
- › Conformité aux règles d'archivage numérique ;

Pour l'ensemble de ces sujets, les sociétés sont souvent 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).
- › Article L.13 du LPF (Livre des Procédures Fiscales) modifié par la loi de finance 1990, article L.102B du LPF : l'administration fiscale a la possibilité d'effectuer un contrôle portant sur « les informations, données et traitements informatiques, qui concourent directement ou indirectement, à la formation des résultats comptables ou fiscaux ainsi que sur la documentation relative aux analyses, à la programmation et à l'exécution des traitements ».

¹ Le règlement eIDAS s'applique à l'identification électronique, aux services de confiance et aux documents électroniques au sein du marché Européen.

FICHE 07

LÉGISLATION FISCALE ET SI

07

- Analyse des données comptables simplifiée avec l'exploitation du FEC :
 - Exhaustivité des analyses même sur de grands volumes de données ;
 - 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).

- Archivage numérique : facture papier numérisée dans les conditions fixées à l'article A. 102 B-2 du LPF.

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 clés 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 différents 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 présent dans le système d'information de l'entreprise (Stocks, factures, ...)

Sanctions en cas de non-utilisation d'un logiciel de caisse certifié :

- Amende de 7 500 € et une régularisation dans les 60 jours.

S'agissant de la signature électronique, elle est régie par le règlement n° 910/2014/UE, adopté le 23 juillet 2014, sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.

Selon le règlement, un moyen d'identification doit :

- Avoir été délivré conformément à un schéma d'identification électronique notifié par l'Etat membre concerné et figurant sur la liste publiée par la Commission.
- Selon le règlement, un schéma d'identification électronique est un système pour l'identification électronique en vertu duquel des moyens d'identification électronique peuvent être délivrés à des personnes physiques ou morales. Les États membres peuvent notifier des schémas d'identification électronique depuis le 29 septembre 2015.
- Avoir un niveau de garantie égal ou supérieur à celui requis par l'organisme du secteur public concerné pour accéder à ce service en ligne, à condition que ce niveau soit substantiel ou élevé. Cette reconnaissance mutuelle ne concerne ainsi que les organismes du secteur public qui exigent, pour accéder à l'un de leurs services en ligne, une identification électronique répondant au moins aux exigences du niveau substantiel.

S'agissant de l'archivage numérique, il est régi par l'article A. 102 B-2 du LPF.

Afin de garantir l'intégrité des fichiers issus de la numérisation, chaque document ainsi numérisé est conservé sous format PDF (Portable Document Format) ou sous format PDF A/3 (ISO 19005-3) et est assorti :

- Soit d'un cachet serveur fondé sur un certificat conforme, au moins, au référentiel général de sécurité (RGS) de niveau une étoile ;
- Soit d'une empreinte numérique ;
- Soit d'une signature électronique fondée sur un certificat conforme, au moins, au référentiel général de sécurité (RGS) de niveau une étoile ;
- Soit de tout dispositif sécurisé équivalent fondé sur un certificat délivré par une autorité de certification figurant sur la liste de confiance française (Trust-service Status List -TSL).

Chaque fichier est horodaté, au moins au moyen d'une source d'horodatage interne, afin de dater les différentes opérations réalisées.

FICHE 07

LÉGISLATION FISCALE ET SI

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-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



QUESTIONNAIRE

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
La cohérence des dates entre elles et par rapport au calendrier des jours fériés (anomalies de procédures ?) a-t-elle été vérifiée ?	Redressement fiscal et/ou rejet de la comptabilité	DSI, Directeur comptable ou DG	OUI
L'analyse des schémas d'écritures utilisés afin d'identifier ceux ne respectant pas le PCG et la doctrine comptable a-t-elle été vérifiée ?	Redressement fiscal et/ou rejet de la comptabilité	DSI, Directeur comptable ou DG	OUI
La recherche de doublons de factures ou de paiements a-t-elle été vérifiée ?	Redressement fiscal et/ou rejet de la comptabilité	DSI, Directeur comptable ou DG	OUI
La vérification du respect des délais de paiement fournisseurs et clients a-t-elle été effectuée ?	Redressement fiscal et/ou rejet de la comptabilité	DSI, Directeur comptable ou DG	OUI
L'analyse de la caisse fait-elle apparaître des mouvements supérieurs à 3 K€ ?	Redressement fiscal et/ou rejet de la comptabilité	DSI, Directeur comptable ou DG	NON

FICHE 07

LÉGISLATION FISCALE ET SI

07

QUESTIONNAIRE

QUESTIONS SUR LE CONTRÔLE DU SI - APPROFONDISSEMENT

Question	Enjeux / Risques associés	Interlocuteur concerné	Réponse attendue
Existents-ils des 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 opérationnelles (Stocks, factures, ...) sont stockés et sécurisés sur le serveur de l'entreprise
Une cartographie claire permet-elle d'identifier 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

MATURITÉ DE L'ENTREPRISE EN MATIÈRE DE LÉGISLATION FISCALE ET SI :

Ce tableau sera repris dans la synthèse globale de cartographies des risques en fin de première partie.

Le niveau de risque sera noté comme suit :

- 1 : Faible
- 2 : Moyen
- 3 : Elevé

Evaluation du risque	Niveau de risque	Commentaire
Incidence		
Probabilité d'occurrence		

EXEMPLES DE BONNES PRATIQUES :

- Effectuer une cartographie du SI ;
- Vérifier les dernières mises à jour des logiciels utilisés (intégrant le FEC) ;
- Effectuer une clôture de caisse quotidienne avec ventilation des recettes par TVA et par nature, ventilation par mode d'encaissement, justification des écarts de caisse... ;
- Créer une stratégie d'archivage des données pérenne et en respectant notamment le RGPD ;
- Documenter le traitement et la comptabilisation des données.

EXPLOITATION DES SYSTÈMES D'INFORMATION

AUDIT INFORMATIQUE : TOUS CONCERNÉS !
10 FICHES PRATIQUES POUR RÉUSSIR

FICHE 08

EXPLOITATION DES SYSTÈMES D'INFORMATION

08

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 traitement 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

08

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, inadéquation des outils et démotivation des utilisateurs.

QUELQUES EXEMPLES

› Augmentation des volumes non anticipée et sans 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, un 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 erreur de sauvegarde ». La personne en charge du suivi est satisfaite. Mais juste au-dessus de « 0 erreur de sauvegarde », il est noté « 0 fichier sauvegardé - 0 octet sauvegardé » ! 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 entraînera 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 qu'un piratage est 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 ?	Inadéquation 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

08

QUESTIONNAIRE

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
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

MATURITÉ DE L'ENTREPRISE EN MATIÈRE D'EXPLOITATION DES SYSTÈMES INFORMATIQUES :

Ce tableau sera repris dans la synthèse globale de cartographie des risques en fin de première partie.

Le niveau de risque sera noté comme suit :

- 1 : Faible
- 2 : Moyen
- 3 : Elevé

Evaluation du risque	Niveau de risque	Commentaire
Incidence		
Probabilité d'occurrence		

EXEMPLES DE BONNES PRATIQUES :

- Documenter les procédures d'exploitation ;
- Documenter et approuver tous les changements apportés aux matériels, aux logiciels, aux systèmes d'exploitation ;
- Définir une politique d'utilisation des services externalisés (prestation par des tiers, externalisation, cloud...);
- Séparer les fonctions et les équipements/environnements de développement, de tests et d'exploitation;
- Effectuer des sauvegardes et des tests de restauration de manière régulière.

PLAN DE CONTINUITÉ D'ACTIVITÉ

AUDIT INFORMATIQUE : TOUS CONCERNÉS !
10 FICHES PRATIQUES POUR RÉUSSIR

FICHE 09 PLAN DE CONTINUITÉ D'ACTIVITÉ

09

CONTEXTE ET ENJEUX

Le plan de continuité d'activité (PCA ou Business Continuity Plan - BCP) vise à établir un plan d'actions pour assurer la continuité des activités de l'entreprise en cas de sinistre important. Il intègre un volet informatique souvent appelé le plan de secours informatique.

Le 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.

Les questions suivantes ont tout intérêt à être soulevées lors de l'entretien avec le dirigeant ou le responsable du système d'information :

- › Combien de temps l'entreprise peut-elle fonctionner si l'outil informatique est hors de service ?
- › Quelles sont les applications les plus indispensables dans l'entreprise ?
- › Comment opérationnellement s'effectuerait la restauration du système informatique ?
- › Combien coûterait la remise en place d'un système informatique en cas de sinistre ?
- › Existe-il des procédures dégradées pour fonctionner temporairement en mode manuel ou avec un système d'information limité ?

La démarche d'un plan de continuité d'activité n'a de sens que si elle est formalisée et testée de manière régulière.

NEP ET TEXTES DE RÉFÉRENCE

- › **NEP 315** : Connaissance de l'entité et de son environnement et évaluation du risque d'anomalies significatives
- › **NEP 570** : Continuité d'exploitation
- › **ISAE 3402** : dans le cadre de l'externalisation de l'exploitation 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.

FICHE 09 PLAN DE CONTINUITÉ D'ACTIVITÉ

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.

➤ 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 scénarii 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 scénarii 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 scénarii ont-ils été identifiés ?	Opérationnel / Image / Juridique	DG/DSI	Préférable

FICHE 09

PLAN DE CONTINUITÉ D'ACTIVITÉ

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 prises 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 oeuvre du PCA ont-elles été prévues ?	Opérationnel	DG/DSI	OUI
Les mesures à mettre en oeuvre 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

MATURITÉ DE L'ENTREPRISE EN MATIÈRE DE PLAN DE CONTINUITÉ D'ACTIVITÉ :

Ce tableau sera repris dans la synthèse globale de cartographie des risques en fin de première partie.

Le niveau de risque sera noté comme suit :

- 1 : Faible
- 2 : Moyen
- 3 : Elevé

Evaluation du risque	Niveau de risque	Commentaire
Incidence		
Probabilité d'occurrence		

EXEMPLES DE BONNES PRATIQUES :

- Définir une étude d'impact du métier (Business Impact Analysis : BIA) ;
- Définir et formaliser un plan de continuité d'activité ;
- Définir une stratégie de sauvegarde ;
- Effectuer des sauvegardes régulières (quotidiennes ou hebdomadaires) ;
- Effectuer des tests périodiques de restauration des sauvegardes ;
- En cas de sauvegardes sur bandes, ranger les supports utilisés pour la sauvegarde dans des endroits sécurisés (coffres ignifugés et antimagnétiques) ou suffisamment éloignés (domicile du responsable des sauvegardes) ;
- Nommer un responsable des sauvegardes afin qu'il s'assure du correct déroulement des sauvegardes.

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 via Internet, mais aussi l'atteinte à la confidentialité, l'intégrité et la disponibilité des systèmes d'information.

Une cyberattaque est donc un acte malveillant destiné à perturber le bon fonctionnement d'un système d'information.

LES DEUX CATÉGORIES DE CYBERATTQUES

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

- › **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. La cybercriminalité a toutes les caractéristiques de la fraude telles que définies par cette norme.
- › Doctrine de la CNCC relative aux prestations entrant dans le cadre des Services Autres que la Certification des Comptes (SACC)
- › **CobiT** dont les défaillances peuvent rendre l'entité vulnérable aux cyberattaques :

APO12	Gérer le risque
APO13	Gérer la sécurité
LSS04	Gérer la continuité
LSS05	Gérer les services de sécurité
SEM02	Surveiller, évaluer et mesurer le système de contrôles internes
SEM03	Surveiller, évaluer et mesurer la conformité aux exigences externes

FICHE 10 CYBERSÉCURITÉ

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. L'utilisation par les collaborateurs d'équipements personnels dans un contexte professionnel (BYOD : Bring Your Own Device ou AVEPC en français : Apportez Votre Equipement Personnel de Communication).
5. La complexité et la décentralisation des organisations
6. Le nomadisme professionnel et le télétravail
- 7 Le manque d'exemplarité des dirigeants
8. Et bien évidemment, le manque de contrôle interne et de formations associées.

QUELQUES EXEMPLES DE CYBERATTAQUE :

- **Hameçonnage (phishing) ou harponnage (spear phishing)**
- **Logiciel malveillant (malware)**
- **Cassage de mot de passe**
- **Attaques par déni de service (DoS) et par déni de service distribué (DDoS)**

QUELQUES EXEMPLES RÉCENTS

➤ **Wannacry**

Considéré comme l'une des plus importantes attaques informatiques de l'histoire, le wannacry (logiciel malveillant ou malware) a pris en otage plusieurs centaines de milliers d'ordinateurs dans le monde en s'attaquant aux données personnelles.

➤ **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

FICHE 10 CYBERSÉCURITÉ

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 ordinateurs de bureau 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

MATURITÉ DE L'ENTREPRISE EN MATIÈRE DE CYBERSÉCURITÉ :

Ce tableau sera repris dans la synthèse globale de cartographie des risques en fin de première partie.

Le niveau de risque sera noté comme suit :

- 1 : Faible
- 2 : Moyen
- 3 : Elevé

Evaluation du risque	Niveau de risque	Commentaire
Incidence		
Probabilité d'occurrence		

EXEMPLES DE BONNES PRATIQUES :

- Nommer un responsable de la sécurité du système d'information (RSSI) ;
- Définir des procédures d'autorisation de nouveaux matériels ou logiciels, d'accès aux informations par des tiers ;
- Avoir une politique de cryptage des données ;
- Choisir un mot de passe fort (longueur minimale de 8 caractères avec des caractères de types différents) et le mettre à jour de manière régulière (tous les 3 mois) ;
- Mettre à jour de manière régulière les logiciels, les anti-virus et configurer le pare-feu ;
- Sécuriser l'accès wifi de votre entreprise ;
- Différencier les usages personnels des usages professionnels ;
- Sensibiliser et former le personnel à la question de la cybersécurité.

MODE D'EMPLOI

La rosace ci-dessous a été constituée grâce à l'ensemble des différentes synthèses par fiche.

Le **niveau de risque inhérent** et la **probabilité d'occurrence** sont notés comme suit :

- 1 : Faible
- 2 : Moyen
- 3 : Elevé

Le **risque global** est une moyenne de ces 2 éléments.

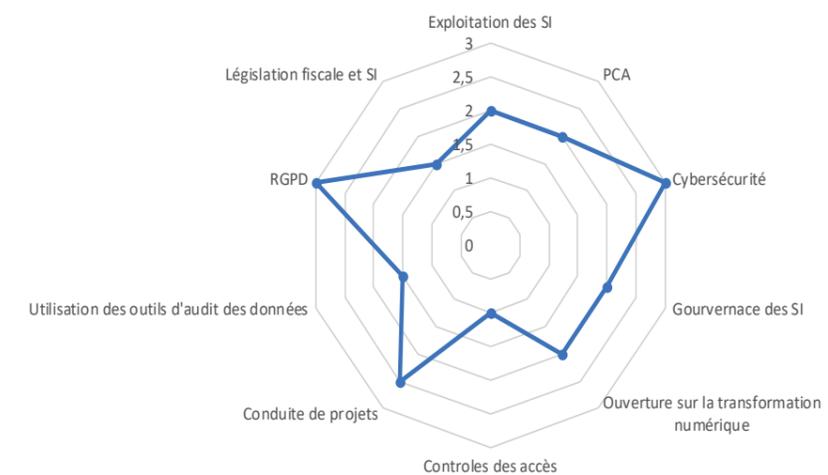
Le fichier de synthèse (téléchargeable ici) a été complété en guise d'exemple afin de montrer la **maturité d'une entreprise en matière de SI**.

Cette maturité peut être visualisée sous forme d'un radar avec 10 extrémités représentant l'ensemble des thématiques des fiches.

Thématique	N° Fiche	Nom de la fiche	Risque inhérent	Probabilité d'occurrence	Risque
Activités de contrôle	Fiche 5	Exploitation des SI	3	1	2
Activités de contrôle	Fiche 6	PCA	2	2	2
Activités de contrôle	Fiche 7	Cybersécurité	3	3	3
Gouvernance entreprise	Fiche 2	Gouvernance des SI	2	2	2
Gouvernance entreprise	Fiche 1	Ouverture sur la transformation numérique	2	2	2
Risques opérationnels	Fiche 3	Contrôles des accès	1	1	1
Risques opérationnels	Fiche 4	Conduite de projet	2	3	2,5
Risques opérationnels	Fiche 8	Utilisation des outils d'audit des données	2	1	1,5
Risques opérationnels	Fiche 9	RGPD	3	3	3
Risques opérationnels	Fiche 10	Législation fiscale et SI	1	2	1,5

SYNTHÈSE DE LA CARTOGRAPHIE DES RISQUES

Risques opérationnels



PARTIE 2

DES SACC POUR DÉVELOPPER VOTRE OFFRE DE MISSIONS AUDIT DES SI

INTRODUCTION

01. L'article L. 823-10-1 du Code de commerce énonce que la mission de certification des comptes du commissaire aux comptes ne consiste pas à garantir la viabilité ou la qualité de la gestion de la personne ou entité contrôlée. A ce titre, le commissaire aux comptes définit la nature et l'étendue des diligences qu'il juge nécessaires compte tenu des prescriptions légales et des normes d'exercice professionnel pour prendre en considération de façon transversale le risque d'anomalies significatives dans les comptes. Le présent document propose des travaux d'investigation complémentaire des éventuels risques d'anomalies significatives induits par le système d'information de l'entité.

02. Le commissaire aux comptes d'une entité peut être amené à réaliser, à la demande de cette dernière, des travaux en vue de délivrer des rapports pour répondre à des besoins spécifiques relatifs à la gouvernance et à la sécurité du système d'information de l'entité.

03. Le cadre déontologique implique le respect strict des interdictions prévues par l'article L822-11 du code de commerce ainsi que les principes d'intégrité, d'impartialité, d'indépendance et de scepticisme professionnel tels que définis par le code de déontologie. A cet égard, l'article 5 du code de déontologie précise que « l'indépendance du commissaire aux comptes s'apprécie en réalité et en apparence. Elle se caractérise par l'exercice en toute objectivité des pouvoirs et des compétences qui sont conférés par la loi. Elle garantit qu'il émet des conclusions exemptes de tout parti pris, conflit d'intérêts, risque d'autorévision ou influence liée à des liens personnels, financiers ou professionnels. »

04. L'entité, en dehors de ses obligations légales, peut avoir besoin de produire des informations ayant fait l'objet d'un contrôle externe, afin de renforcer la crédibilité de ces dernières. Elle demande un rapport dans lequel le commissaire aux comptes formule des constats ou une conclusion à l'issue de diligences lui ayant permis d'obtenir une « assurance modérée », c'est-à-dire une assurance moins élevée que celle obtenue dans le cadre d'un audit des comptes, que les informations fournies au commissaire aux comptes ne comportent pas d'anomalies significatives.

05. La mission confiée au commissaire aux comptes permet de donner un avis ou de fournir des éléments d'information. Il nécessite la mise en œuvre de travaux non requis pour la mission de certification. Les avis peuvent être assortis de recommandations qui contribuent à l'amélioration de la qualité et de la sécurité du système d'information de l'entité. Il est destiné à l'usage propre de l'entité.

06. Le présent document a pour objet de définir les conditions dans lesquelles le commissaire aux comptes peut réaliser la mission demandée, les travaux qu'il met en œuvre pour ce faire et la forme sous laquelle celui-ci sera communiqué à l'entité.

CONTEXTE DE LA DEMANDE

07. Le commissaire aux comptes se fait préciser le contexte de la demande pour s'assurer :
➤ que la mission demandée respecte les conditions requises par le présent document ;
➤ et que les conditions de son intervention et l'utilisation prévue de son rapport sont compatibles avec les dispositions du code de déontologie de la profession.

08. Le commissaire aux comptes s'assure que les conditions de son intervention, notamment les délais pour mettre en œuvre ses travaux, sont compatibles avec les ressources dont il dispose.

09. Dans tous les cas, le commissaire aux comptes peut refuser l'intervention.

TRAVAUX DU COMMISSAIRE AUX COMPTES

10. Le commissaire aux comptes applique les dispositions de la norme d'exercice professionnel relative à la lettre de mission pour définir les termes et conditions de cette intervention. Si nécessaire, il établit une nouvelle lettre ou une lettre complémentaire, conformément aux principes de la norme susmentionnée.

11. Le commissaire aux comptes utilise sa connaissance de l'entité concernée et de son environnement et les travaux qu'il a déjà réalisés pour les besoins de la certification des comptes, et met en œuvre les travaux complémentaires qu'il estime nécessaires pour obtenir l'assurance modérée que les informations fournies par l'entité, prises dans leur ensemble, ne comportent pas d'anomalies significatives.

12. Les travaux consistent à évaluer les risques en tenant compte de l'identification des risques potentiels et du système de contrôle interne mis en place par l'entreprise, et à en déduire la nature et l'étendue des contrôles substantifs à mener, afin de maintenir le risque d'audit à un niveau faible acceptable dans les domaines suivants :

- **la gouvernance du système d'information ;**
- **le contrôle des accès informatiques ;**
- **la conduite des projets informatiques ;**
- **la protection des données personnelles ;**
- **l'exploitation du système d'information ;**
- **le plan de continuité d'activité informatique ;**
- **la protection de la confidentialité, de l'intégrité et de la disponibilité des données, autrement dit la sécurité du système d'information.**

INTRO

Conformément au Règlement européen de l'audit, ces travaux constituent des services autres que la certification des comptes.

Pour mener ces travaux, le commissaire aux comptes définit le référentiel de travail sur lequel il va se fonder. Par exemple :

- les NEP ou les normes ISA pour la vérification des données informatisées ;
- le COSO pour l'audit du contrôle interne ;
- le COBIT pour l'audit du système d'information et de la gouvernance informatique.

La CNCC a publié une mise à jour de son guide sur les SACC en novembre 2018, précisant les normes ou doctrines auxquelles faire référence lors de la réalisation des services autres que la certification des comptes. Dans le cas des travaux évoqués ici, les prestations suivantes sont envisageables :

- des procédures convenues qui donneront lieu à des constats ;
- des travaux qui permettront d'émettre une attestation avec éventuellement des observations ;
- un examen limité qui permettra la formulation soit d'une conclusion sans observation, soit d'une conclusion avec observation(s), soit d'une impossibilité de conclure.

13. Le commissaire aux comptes, à partir des éléments vérifiés lors de l'évaluation des risques, se concentre sur les risques de niveau modéré ou élevé, afin de déterminer la nature et l'étendue des contrôles substantifs à mener et s'il est pertinent, pour ce faire, de recourir aux techniques d'audit assistées par ordinateur.

14. Après avoir effectué les contrôles substantifs nécessaires et disposant des éléments probants suffisants et appropriés recherchés, le commissaire aux comptes formule les résultats de ses travaux sur la qualité du système d'information de l'entreprise. La formulation des résultats est fonction notamment du caractère significatif des anomalies éventuellement relevées.

CONSTATS DE LA PROCÉDURE CONVENUE

15. Les constats du commissaire aux comptes doivent permettre à l'entité de tirer ses propres conclusions des procédures convenues. Pour mémoire, les procédures convenues ne conduisent pas à une opinion d'audit, à une conclusion d'examen limité ou à une attestation du commissaire aux comptes.

OBSERVATION DE L'ATTESTATION

16. Lorsqu'il émet une attestation, le commissaire aux comptes formule, s'il y a lieu, toutes observations utiles.

17. En formulant une observation, le commissaire aux comptes attire l'attention sur une information fournie dans une annexe ou dans des notes explicatives. Il ne peut pas dispenser d'informations dont la diffusion relève de la responsabilité des dirigeants.

18. Les observations sont formulées dans un paragraphe distinct.

19. Le commissaire aux comptes formule systématiquement une observation en cas d'incertitude sur la continuité de l'exploitation.

CONCLUSIONS DE L'EXAMEN LIMITÉ

20. Les conclusions de l'examen limité sont normées par la NEP 2410.

FORME DU RAPPORT DÉLIVRÉ

21. Le commissaire aux comptes établit un rapport qui comporte les informations suivantes :

- un titre qui indique la nature des prestations réalisées ;
- l'identité du destinataire du rapport au sein de l'entité ou l'indication de l'organe auquel le rapport est destiné ;
- le rappel de la qualité de commissaire aux comptes ;
- l'identification de l'entité concernée ;
- la nature des informations qui font l'objet du rapport et sont jointes à ce dernier ;
- la période concernée ;
- les rôles respectifs de la direction ou de l'organe compétent de l'entité concernée pour établir les informations et du commissaire aux comptes pour formuler ses résultats ;
- la nature et l'étendue des travaux mis en œuvre dans le cadre de l'audit ;
- les constats ou les conclusions du commissaire aux comptes ;
- le cas échéant, ses observations ;
- la date du rapport ;
- l'identification et la signature du commissaire aux comptes.

CO-COMMISSARIAT AUX COMPTES

22. Il appartient au commissaire aux comptes qui établit seul le rapport :

- d'informer préalablement les autres commissaires aux comptes de l'objet de la mission ;
- de leur communiquer une copie du rapport.

INTRO

TRANSFORMATION NUMÉRIQUE

AUDIT INFORMATIQUE : TOUS CONCERNÉS !
SERVICE AUTRE QUE LA CERTIFICATION DES COMPTES

FICHE 01

TRANSFORMATION NUMÉRIQUE

01

TRANSFORMATION NUMÉRIQUE

PROPOSITION D'UN PÉRIMÈTRE D'INTERVENTION

OBJECTIFS DE LA PRESTATION

Une entité peut souhaiter confier à son commissaire aux comptes une intervention sur la maturité numérique de son entreprise : où en est ma société au sujet de la transformation numérique ?

La transformation numérique que l'on appelle parfois aussi transformation digitale, désigne le processus qui permet aux entreprises d'intégrer les technologies numériques disponibles au sein de leur activité.

Toutes les entités sont concernées. Il s'agit d'un phénomène sociétal qui touche aussi bien notre vie privée que notre vie professionnelle. L'introduction de nouvelles technologies et l'apparition de nouveaux usages ont bouleversé notre monde d'un point de vue culturel, structurel et organisationnel.

Les travaux ont pour objet, à la demande de l'entité :

- de fournir un support permettant de comprendre ce qu'est la transformation numérique, la convergence entre le monde professionnel et le numérique, les enjeux et leurs impacts ;
- ou de fournir un support de formation concernant des textes, des projets de textes ou des pratiques contribuant à la bonne compréhension des obligations de l'entité en matière de transformation numérique ;
- ou de donner un avis sur la maturité numérique de l'entité ;
- ou de donner un avis sur la manière dont l'entité à engager sa transformation numérique ;
- ou donner un avis sur la prise en compte par l'entité des 4 axes fondamentaux de la transformation numérique (innovation, excellence opérationnelle, management et l'écosystème) ;

Les avis peuvent être assortis de recommandations portant sur des éléments du contrôle interne, objets de la consultation et contribuant à l'amélioration des traitements de l'information financière.

FICHE 01

TRANSFORMATION NUMÉRIQUE

Dans les Entités d'Intérêt Public, les travaux du commissaire aux comptes ne peuvent pas inclure la participation¹ :

- à la conception et la mise en œuvre de la transformation numérique ou de gestion des risques en rapport avec la préparation et/ou le contrôle de l'information financière ;
- au choix de la solution ;
- aux services liés à la fonction d'audit interne de l'entité contrôlée.

La prestation décrite dans le présent document est un Service Autre que la Certification des Comptes (SACC) : il ne s'agit pas d'une mission de certification des comptes.

Dans tous les cas, le commissaire aux comptes peut refuser l'intervention.

PÉRIMÈTRE D'INVESTIGATION

La CNCC a publié une mise à jour de son guide sur les SACC en novembre 2018 précisant les normes ou doctrines auxquelles faire référence lors de la réalisation des services autres que la certification des comptes. Dans le cas des travaux évoqués ici, les prestations suivantes sont envisageables :

- des procédures convenues qui donneront lieu à des constats ;
- des travaux qui permettront d'émettre une attestation avec éventuellement des observations ;
- un examen limité qui permettra la formulation soit d'une conclusion sans observation, soit d'une conclusion avec observation(s), soit d'une conclusion défavorable, soit d'une impossibilité de conclure.

Pour répondre aux demandes de l'entité, le commissaire aux comptes met en œuvre toutes les diligences possibles dans le cadre d'une obligation de moyens.

Les travaux du commissaire aux comptes portent sur :

- la planification de la transformation numérique,
- les tests mis en place,
- les déploiements et optimisations.

RAPPORT ET DOCUMENTATION

Le commissaire aux comptes consigne dans son dossier de travail :

- l'analyse de la maturité, des forces et des faiblesses de l'entité en matière transformation numérique ;
- l'identification des étapes de la transformation numérique de l'entité ;
 - un management de la transformation numérique,
 - une culture d'entreprise repensée,
 - une technologie mise à jour pour être agile,
 - la maîtrise des données,
 - les aspects marketing qui doivent répondre aux nouvelles attentes du client,
 - la mesure de la performance.
- le calendrier, les entretiens, les tests sur le management, les documents relatifs à la culture d'entreprise, la technologie, les données, le marketing et la mesure de la performance.

Le commissaire aux comptes émet un rapport avec les résultats des travaux qu'il a réalisés. Le rapport prend la forme d'un document daté et signé par le commissaire aux comptes et comporte selon les cas :

- son analyse de la situation et des faits avec, le cas échéant, les références aux textes légaux et réglementaires, à la doctrine, à la pratique ou à un référentiel international sur la transformation numérique ;
- son avis sur la maturité numérique ou ses recommandations éventuelles ;
- les éléments d'informations et commentaires sur les textes qui font l'objet de la demande de l'entité.

¹ Dans les entités non EIP, en vertu de la loi Pacte, ces services ne sont plus interdits mais doivent faire l'objet d'une approche « risques / sauvegarde »

FICHE 01

TRANSFORMATION NUMÉRIQUE

PROPOSITION D'UNE DÉMARCHE MÉTHODOLOGIQUE

IDENTIFICATION DES ZONES DE RISQUES

Suite à la revue du contrôle interne, il convient dans un premier temps d'identifier au sein de l'entité, les cycles et les processus les plus exposés ; puis, dans un second temps, d'évaluer les risques. Les investigations sont ensuite organisées en fonction des risques qui ont pu être identifiés.

- › la compréhension et vision du digital ;
- › la culture d'entreprise et les compétences ;
- › l'écosystème et l'architecture ;
- › le Big Data ;
- › la connaissance des clients ;
- › les bonnes pratiques.

CHOIX DES TESTS À RÉALISER

Le leadership et le management

- › La compréhension et la vision du nouveau monde du numérique ;
- › La planification d'une nouvelle stratégie : simplification des processus et diffusion des savoirs-faire digitaux ;
- › La mise en place d'un projet test ;
- › Le déploiement et les processus d'amélioration continue.

La culture et l'organisation

- › Le niveau d'acculturation au numérique ;
- › La planification des compétences en numérique ;
- › L'organisation mise en place pour digitaliser l'entité ;
- › L'efficacité du CDO (Chief Digital Officer ou manager de la transformation numérique) ;
- › L'agilité au sein de l'organisation ;
- › Le déploiement de la formation ;
- › Optimiser la collaboration.

Les technologies

- › L'écosystème et les architectures ;
- › La planification de l'intégration de la Direction des Systèmes d'Information ;
- › Le déploiement du Cloud, de l'approche SAAS ou API ;
- › L'optimisation de l'agilité.

Les données

- › Le volume de traitement des données ;
- › La maîtrise du client ;
- › La maîtrise des enjeux légaux ;
- › La maîtrise des enjeux de sécurité ;
- › La maîtrise des enjeux éthiques ;
- › Le déploiement des données à chaque niveau de l'organisation ;
- › L'optimisation Big Data et de l'Intelligence Artificielle.

L'expérience clients et le marketing 2.0

- › La connaissance du client ;
- › La manière dont est repensée l'approche marketing.

La mesure de la performance

- › Les bonnes pratiques de la mesure de la performance ;
- › La définition des indicateurs clés de la mesure ;
- › Le déploiement du Tableaux de bord ;
- › L'optimisation du benchmark.

ANALYSE DES RÉSULTATS

Les résultats des tests vont permettre de repérer les forces et faiblesses de la mise en place de la transformation numérique de l'entité.

L'analyse des faiblesses nécessite d'affiner encore les tests sur un périmètre plus restreint.

01

GOVERNANCE DES SYSTÈMES D'INFORMATION

AUDIT INFORMATIQUE : TOUS CONCERNÉS !
SERVICE AUTRE QUE LA CERTIFICATION DES COMPTES

FICHE 02

GOVERNANCE DES SYSTÈMES D'INFORMATION

02

PROPOSITION D'UN PÉRIMÈTRE D'INTERVENTION

OBJECTIFS DE LA PRESTATION

Une entité peut souhaiter confier à son commissaire aux comptes une intervention tendant à la qualité de la gouvernance de son système d'information. Les travaux ont pour objet, à la demande de l'entité :

- de donner un avis quant aux rôles et responsabilités vis-à-vis du système d'information ;
- de donner un avis sur la pertinence de la gouvernance des données ;
- de donner un avis sur le contrôle interne du système d'information ;
- de donner un avis sur la couverture et la cohérence du système d'information.

Les avis peuvent être assortis de recommandations qui visent à contribuer à l'amélioration des traitements de l'information financière et qui portent sur des éléments du contrôle interne objets de la consultation.

Dans les Entités d'Intérêt Public, les travaux du commissaire aux comptes ne peuvent pas inclure la participation¹ :

- à la conception et la mise en œuvre de procédures de contrôle interne ou de gestion des risques en rapport avec la préparation et/ou le contrôle de l'information financière ;
- à la conception et la mise en œuvre de systèmes techniques relatifs à l'information financière ;
- aux services liés à la fonction d'audit interne de l'entité contrôlée.

La prestation décrite dans le présent document est un Service autre que la certification des comptes (SACC) : il ne s'agit pas d'une mission de certification des comptes.

Dans tous les cas, le commissaire aux comptes peut refuser l'intervention.

¹ Dans les entités non EIP, en vertu de la loi Pacte, ces services ne sont plus interdits mais doivent faire l'objet d'une approche « risques/sauvegarde »

FICHE 02

GOVERNANCE DES SYSTÈMES D'INFORMATION

PÉRIMÈTRE D'INVESTIGATION

La CNCC a publié une mise à jour de son guide sur les SACC en novembre 2018, précisant les normes ou doctrines auxquelles faire référence lors de la réalisation des services autres que la certification des comptes. Dans le cas des travaux évoqués ici, les prestations suivantes sont envisageables :

- des procédures convenues qui donneront lieu à des constats ;
- des travaux qui permettront d'émettre une attestation avec éventuellement des observations ;
- un examen limité qui permettra la formulation soit d'une conclusion sans observation, soit d'une conclusion avec observation(s) soit d'une impossibilité de conclure.

Pour répondre aux demandes de l'entité, le commissaire aux comptes met en œuvre les diligences nécessaires à son jugement professionnel, dans le cadre d'une obligation de moyens.

Il se réfère notamment à COBIT qui est le référentiel international de gouvernance des SI.

Les travaux du commissaire aux comptes portent sur :

- la répartition des responsabilités au sein de la DSI et notamment sur la séparation des tâches entre développement et exploitation ;
- la répartition des responsabilités entre la DSI, le DAF, les « propriétaires » d'applications et les « propriétaires » de données ;
- les tâches principales de contrôle qui doivent être dûment attribuées afin d'assurer la surveillance et de sécurisation du SI dans un cycle d'amélioration continue ;
- le contrôle de la gouvernance des données et notamment pour les données « référentielles » ou données maître afin d'assurer leur intégrité et la traçabilité des modifications par des personnes dûment autorisées. Les données référentielles et les interfaces sont la base de la piste d'audit ;
- La maturité en matière de contrôle interne propre au SI dans ses 6 composantes :
 - 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 : réseaux, systèmes d'exploitation, bases de données, mise en production.
- La maturité en matière de RGPD ;
- La couverture fonctionnelle par rapport à la cartographie des processus métiers, en distinguant les applications gérées en interne et celles qui sont externalisées.

Le commissaire aux comptes utilise également sa connaissance du contexte et du tissu économique dans lesquels évolue l'entité.

RAPPORT ET DOCUMENTATION

Le commissaire aux comptes consigne dans son dossier de travail :

- l'analyse des forces et des faiblesses de l'organisation et des systèmes examinés en matière de gouvernance du SI ;
- l'analyse des forces et des faiblesses de la gouvernance des données ;
- l'analyse des forces et des faiblesses du contrôle interne du SI ;
- l'identification et l'analyse des zones de risques ;
- l'identification et l'analyse des processus peu ou mal couverts par le SI ;
- les conclusions des tests éventuels.

Le commissaire aux comptes émet un rapport avec les résultats des travaux qu'il a réalisés. Le rapport prend la forme d'un document daté et signé par le commissaire aux comptes et comporte selon les cas :

- son analyse de la situation et des faits avec, le cas échéant, les références aux textes légaux et réglementaires, à la doctrine, à la pratique ou à un référentiel international de gouvernance informatique ;
- son avis quant à la maturité de l'entreprise en matière de gouvernance du SI et ses recommandations éventuelles ;
- les éléments d'informations et commentaires sur les textes qui font l'objet de la demande de l'entité.

FICHE 02

GOVERNANCE DES SYSTÈMES D'INFORMATION

PROPOSITION D'UNE DÉMARCHE MÉTHODOLOGIQUE

IDENTIFICATION DES ZONES DE RISQUES

Suite à la revue du contrôle interne, il convient dans un premier temps d'identifier au sein de l'entité, les cycles et les processus les plus exposés puis, dans un second temps, d'évaluer les risques. Les investigations sont ensuite organisées en fonction des risques qui ont pu être identifiés.

Dans le cas spécifique de la gouvernance du SI, par définition tous les processus COBIT sont concernés, mais avec un focus particulier sur les processus « **EVALUER, DIRIGER, SURVEILLER** » et « **SURVEILLER, EVALUER, MESURER** »

Les tests de procédures et les contrôles de substance sont identiques à ceux mis en œuvre par un audit traditionnel.

CHOIX DES TESTS À RÉALISER

S'agissant d'organisation et de procédures, les tests sont principalement des tests de compréhension et de procédures. Seule des cartographies du SI en termes d'infrastructure, d'applications et de flux permettent d'évaluer les besoins de gouvernance. Sur la base de ces cartographies, les responsabilités sont identifiées et testées, les données et les traitements évalués et les flux mesurés en termes de traçabilité et intégrité.

En fonction du secteur d'activité de l'entité auditée, l'auditeur doit définir les types de tests à réaliser. Par exemple, dans le secteur de l'industrie, l'auditeur peut vérifier le bouclage du « bilan matière » et la cohérence des stocks avec les flux d'achats et ventes.

Concernant le contrôle interne, l'analyse doit identifier les domaines où la maturité est moindre et donc l'existence de risques qui peuvent faire l'objet d'extension de missions afin d'effectuer des tests plus détaillés des procédures concernées.

ANALYSE DES RÉSULTATS

Les résultats de la mission vont permettre :

- de parfaire la compréhension du SI par rapport aux processus de l'entreprise,
- de mesurer l'adéquation de l'organisation de la DSI mais aussi des rôles et responsabilités des utilisateurs métier,
- d'évaluer la sensibilité des données et de leur gouvernance,
- de mesurer la maturité en termes de contrôle interne du SI.



CONTRÔLE DES ACCÈS

FICHE 03 CONTRÔLE DES ACCÈS

03

PROPOSITION D'UN PÉRIMÈTRE D'INTERVENTION

OBJECTIFS DE LA PRESTATION

Une entité peut souhaiter confier à son commissaire aux comptes une intervention tendant à la revue des droits d'accès de son système d'information.

Les travaux peuvent avoir pour objet, à la demande de l'entité :

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

Les avis peuvent être assortis de recommandations visant à contribuer à l'amélioration des traitements de l'information financière et qui portent sur des éléments du contrôle interne objets de la consultation.

Dans les Entités d'Intérêt Public, les travaux du commissaire aux comptes ne peuvent pas inclure la participation¹ :

- › à la conception et la mise en œuvre de procédures de contrôle interne ou de gestion des risques en rapport avec la préparation et/ou le contrôle de l'information financière ;
- › à la conception et la mise en œuvre de systèmes techniques relatifs à l'information financière ;
- › aux services liés à la fonction d'audit interne de l'entité contrôlée.

La prestation décrite dans le présent document est un Service autre que la certification des comptes (SACC) : il ne s'agit pas d'une mission de certification des comptes.

Dans tous les cas, le commissaire aux comptes peut refuser l'intervention.

¹ Dans les entités non EIP, en vertu de la loi Pacte, ces services ne sont plus interdits mais doivent faire l'objet d'une approche « risques/sauvegarde »

FICHE 03 CONTRÔLE DES ACCÈS

PÉRIMÈTRE D'INVESTIGATION

La CNCC a publié une mise à jour de son guide sur les SACC en novembre 2018, précisant les normes ou doctrines auxquelles faire référence lors de la réalisation des services autres que la certification des comptes. Dans le cas des travaux évoqués ici, les prestations suivantes sont envisageables :

- › des procédures convenues qui donneront lieu à des constats ;
- › des travaux qui permettront d'émettre une attestation avec éventuellement des observations ;
- › un examen limité qui permettra la formulation soit d'une conclusion sans observation, soit d'une conclusion avec observation(s) soit d'une impossibilité de conclure.

Pour répondre aux demandes de l'entité, le commissaire aux comptes met en œuvre toutes les diligences possibles dans le cadre d'une obligation de moyens.

Les travaux du commissaire aux comptes portent sur :

- › les applications, infrastructures et couches basses ;
- › des éléments du contrôle interne relatifs au traitement des opérations de l'entité ;
- › le système d'information en général, et les traitements informatisés des données financières en particulier.

Le commissaire aux comptes utilise également sa connaissance du contexte et du tissu économique dans lesquels évolue l'entité.

RAPPORT ET DOCUMENTATION

Le commissaire aux comptes consigne dans son dossier de travail :

- › l'analyse des forces et des faiblesses de l'organisation et des systèmes évalués en matière de gestion des droits d'accès ;
- › l'identification et l'analyse des zones de risques de fraude ;
- › le calendrier et les tests de revues des droits et des utilisateurs, conçus et mis en œuvre en réponse à son évaluation des risques.

Le commissaire aux comptes émet un rapport avec les résultats des travaux qu'il a réalisés. Le rapport prendrait la forme d'un document daté et signé par le commissaire aux comptes et comporterait selon les cas :

- › son analyse de la situation et des faits avec, le cas échéant, les références aux textes légaux et réglementaires, à la doctrine, à la pratique ou à un référentiel international de gouvernance informatique ;
- › son avis quant à l'existence de failles de sécurité au sein des applications ou ses recommandations éventuelles ;
- › les éléments d'informations et commentaires sur les textes qui font l'objet de la demande de l'entité.

PROPOSITION D'UNE DÉMARCHÉ MÉTHODOLOGIQUE

IDENTIFICATION DES ZONES DE RISQUES

Suite à la revue du contrôle interne, il convient dans un premier temps d'identifier au sein de l'entité, les cycles et les processus les plus exposés puis, dans un second temps, d'évaluer ces risques. Les investigations seront ensuite organisées en fonction des risques qui auront pu être identifiés et appliqués au système d'information supportant ces cycles et processus.

Dans le cadre de la revue des droits d'accès, une attention particulière sera évidemment consacrée aux cycles « Ventes – Clients », « Achats – Fournisseurs », « Trésorerie », « Immobilisations » et « Comptabilité » qui pourront faire l'objet de tests de procédure et de contrôle de substance.

Dans le cas spécifique de la revue des droits d'accès, nous avons recensé les processus CobiT dont les défaillances peuvent rendre l'entité vulnérable aux cyber-attaques :

APO12	Gérer le risque
APO13	Gérer la sécurité
LSS05	Gérer les services de sécurité
SEM02	Surveiller, évaluer et mesurer le système de contrôles internes

Le cas échéant, ces processus feront l'objet de tests de procédure.

FICHE 03

CONTRÔLE DES ACCÈS

CHOIX DES TESTS À RÉALISER

Les travaux sont de différentes natures :

Processus de gestion des droits d'accès

- Analyse de politique des mots de passe et son application ;
- Analyse de la procédure de gestion des droits et de la matrice de séparation des fonctions intra et inter applications ;
- Réalisation de tests d'efficacité sur les contrôles opérés dans la procédure :
 - Validation d'une demande d'attribution des droits par une personne habilitée ;
 - Séparation des fonctions dans le processus entre celui qui demande, crée les utilisateurs et les droits et attribue les droits aux utilisateurs ;
 - Validation de la déconnexion des utilisateurs et des droits attachés lors du départ d'un collaborateur ;
 - Validation de la modification des droits d'un utilisateur lors d'un mouvement interne au sein de l'entreprise ;
 - Mise en place d'une revue périodique des utilisateurs et des droits attachés.

Revue des profils et des droits attachés aux utilisateurs

- Analyse du contenu des profils pour identifier la correcte conception du profil en fonction des besoins métiers et des risques intra-profils en termes de séparation des fonctions (cumul de fonctionnalités incompatibles les unes avec les autres – par exemple – saisir une facture – effectuer un règlement) ;
- Analyse de l'affectation des profils aux utilisateurs pour s'assurer de l'adéquation du profil avec la fiche de poste ;
- Analyse que le cumul de profils ne donne pas des cumuls de fonctionnalités incompatibles – risques inter-profils.

ANALYSE DES RÉSULTATS

Les résultats des tests vont permettre de repérer des anomalies dans les transactions opérationnelles, financières et comptables. L'analyse de ces anomalies nécessitera d'affiner encore les tests sur un périmètre plus restreint, après stratification ou requêtes spécifiques, afin de déterminer si les opérations passées par l'utilisateur (en cas de droits d'accès large ou supérieurs à la fiche de poste de l'utilisateur) sont légitimes.

Il faut en effet garder à l'esprit que toutes les opérations présentant des risques en terme de séparation des fonction peuvent être justifiées du fait de l'organisation, d'équipe réduite, d'événements exceptionnels (maladie, etc...) . Il est nécessaire de corroborer les données informatiques avec d'autres éléments de preuve, comme les justificatifs papier par exemple. Le jugement professionnel demeure primordial.

03

CONDUITE DE PROJETS

AUDIT INFORMATIQUE : TOUS CONCERNÉS !
SERVICE AUTRE QUE LA CERTIFICATION DES COMPTES

FICHE 04 CONDUITE DE PROJETS

04

PROPOSITION D'UN PÉRIMÈTRE D'INTERVENTION

OBJECTIFS DE LA PRESTATION

Une entité peut souhaiter confier à son commissaire aux comptes une intervention tendant à évaluer le dispositif de la conduite des projets informatiques.

Toutes les entités peuvent être concernées par l'évaluation de leur dispositif de conduite de projet, mais cette intervention s'inscrit en premier lieu dans un contexte de projet de migration¹.

Les travaux ont pour objet, à la demande de l'entité, de s'assurer de :

- › la conformité du nouvel environnement avec les exigences comptables et réglementaires françaises,
- › l'efficacité des procédures de contrôles mises en place pour la reprise des données,
- › l'exhaustivité et l'intégrité de la migration des données,
- › l'adéquation des nouveaux outils avec le processus d'arrêtés des comptes,
- › la validation de la persistance de la qualité des informations produites dans le cadre du processus d'arrêtés.

Les avis peuvent être assortis de recommandations visant à contribuer à l'amélioration des traitements de l'information financière et qui portent sur des éléments du contrôle interne, objets de la consultation.

Dans les Entités d'Intérêt Public, les travaux du commissaire aux comptes ne peuvent pas inclure la participation² :

- › à la conception et la mise en œuvre de procédures de contrôle interne ou de gestion des risques en rapport avec la préparation et/ou le contrôle de l'information financière ;
- › à la conception et la mise en œuvre de systèmes techniques relatifs à l'information financière ;
- › aux services liés à la fonction d'audit interne de l'entité contrôlée.

La prestation décrite dans le présent document est un Service autre que la certification des comptes (SACC) : il ne s'agit pas d'une mission de certification des comptes.

Dans tous les cas, le commissaire aux comptes peut refuser l'intervention.

¹ Par migration, il est sous-entendu projet de mise en place d'un nouvel outil ; montée de version d'un outil existant ; changement d'infrastructure technique.

² Dans les entités non EIP, en vertu de la loi Pacte, ces services ne sont plus interdits mais doivent faire l'objet d'une approche risques / sauvegarde »

FICHE 04

CONDUITE DE PROJETS

PÉRIMÈTRE D'INVESTIGATION

La CNCC a publié une mise à jour de son guide sur les SACC en novembre 2018, précisant les normes ou doctrines auxquelles faire référence lors de la réalisation des services autres que la certification des comptes. Dans le cas des travaux évoqués ici, les prestations suivantes sont envisageables :

- › des procédures convenues qui donneront lieu à des constats ;
- › des travaux qui permettront d'émettre une attestation avec éventuellement des observations ;
- › un examen limité qui permettra la formulation soit d'une conclusion sans observation, soit d'une conclusion avec observation(s), soit d'une conclusion défavorable, soit d'une impossibilité de conclure.

Pour répondre aux demandes de l'entité, le commissaire aux comptes met en œuvre toutes les diligences possibles dans le cadre d'une obligation de moyens.

En fonction de l'état d'avancement du projet, les travaux peuvent être scindés en deux phases :

Une phase de pré-migration au cours de laquelle les travaux du commissaire aux comptes portent sur :

- › La revue du dispositif de gouvernance et du pilotage du projet.
- › La revue du dispositif d'analyse des risques liés au projet.
- › La prise de connaissance des principaux processus impactés par les migrations.
- › La revue des principaux livrables liés à l'expression de besoins et aux spécifications fonctionnelles.
- › La revue de la stratégie de migration de données.
- › La revue de la stratégie de tests, de recette et de gestion des anomalies (critères de Go/ No-go).
- › La revue ciblée de l'impact de la migration sur les schémas comptables.
- › La revue du dispositif prévu en matière de séparation des tâches.
- › La revue ciblée de la conception des interfaces et de la supervision des flux, le cas échéant.
- › La revue du dispositif de formation des utilisateurs.

Une phase de post-migration au cours de laquelle les travaux du commissaire aux comptes portent sur :

- › La revue du processus de mise en production.
- › La revue ciblée des contrôles de reprises de données, permettant d'assurer l'exhaustivité et l'intégrité des données migrées.
- › La revue de la gestion des droits utilisateurs implémentés et le respect du principe de séparation des tâches.
- › La revue des tests réalisés sur la correcte implémentation des schémas comptables.
- › La revue des tests de bout en bout réalisés par l'équipe projet et les key-users.

Les comptes concernent un exercice complet ou une autre période définie, le recours à des techniques d'investigation assistées par ordinateur permet d'effectuer des tests exhaustifs notamment sur les reprises de données.

Le commissaire aux comptes utilise également sa connaissance du contexte et du tissu économique dans lesquels évolue l'entité.

RAPPORT ET DOCUMENTATION

Le commissaire aux comptes consigne dans son dossier de travail :

- › L'analyse des forces et des faiblesses de l'organisation et des systèmes évalués en matière de la gestion de projet ;
- › L'identification et l'analyse des zones de risques liées au projet ;
- › Le détail des tests conçus et mis en œuvre en réponse à son évaluation des risques.

Le commissaire aux comptes émet un rapport avec les résultats des travaux qu'il a réalisés. Le rapport prend la forme d'un document daté et signé par le commissaire aux comptes et comporte selon les cas :

- › Son analyse de la situation et des faits avec, le cas échéant, les références aux textes légaux et réglementaires, à la doctrine, à la pratique ou à un référentiel international de gestion des projets informatiques ;
- › Son avis quant à l'existence de failles dans le dispositif de gestion de projet ou ses recommandations éventuelles ;
- › Les éléments d'informations et commentaires sur les textes qui font l'objet de la demande de l'entité.

FICHE 04

CONDUITE DE PROJETS

04

PROPOSITION D'UNE DÉMARCHE MÉTHODOLOGIQUE

IDENTIFICATION DES ZONES DE RISQUES

Suite à la revue du contrôle interne, il convient dans un premier temps d'identifier au sein de l'entité, les cycles et les processus les plus exposés puis, dans un second temps, d'évaluer ces risques. Les investigations sont ensuite organisées en fonction des risques qui auront pu être identifiés.

Dans le cas spécifique de la conduite des projets informatiques, nous avons recensé les processus COBIT suivants :

BAI01	Gérer les programmes et les projets
BAI02	Gérer la définition des exigences
BAI03	Gérer l'identification et la conception des solutions
BAI04	Gérer la disponibilité et la capacité
BAI05	Gérer le changement organisationnel
BAI06	Gérer les changements
BAI07	Gérer l'acceptation du changement et de la transition
BAI08	Gérer la connaissance
BAI09	Gérer les actifs
BAI10	Gérer la configuration

CHOIX DES TESTS À RÉALISER

Les tests à réaliser peuvent varier en fonction du contexte et du périmètre des projets. Ceux-ci peuvent être réalisés par thématique :

Prise de connaissance du projet

- Evaluer le dispositif de gouvernance et de pilotage de projet (comitologie, suivi budgétaire, organisation de l'équipe projet, analyse des risques liés au projet, etc.) ;
- Evaluer le dispositif de conduite du changement (plan de communication, plan de formation).

Evaluation de la préparation de la reprise des données

- Analyser le périmètre des données à reprendre ;
- Analyser la méthodologie de reprise des données pour les différents types de données (règles métier, prérequis en matière de nettoyage et d'enrichissement, règles d'extraction et de formatage des données) ;
- En cas d'utilisation d'un outil de reprise (Interface Standard de Migration des données), fournie par l'éditeur ou développement spécifique, analyse des spécifications ou de la documentation des outils utilisés ;
- Analyse de la documentation des contrôles lors du nettoyage des données, le cas échéant ;
- Analyse des règles de conversion des données et des tables de Trans codification, le cas échéant.

Recette fonctionnelle

- S'assurer de l'existence d'un environnement dédié, différent de l'environnement de production pour la réalisation des tests ;
- Prendre connaissance du plan de recette et s'assurer d'un niveau de couverture suffisant (fonctionnalités / états de contrôle, interfaces) ;
- Analyse de la documentation des tests réalisés sur les schémas comptables ;
- S'assurer de la correcte implémentation des droits utilisateurs conformément à la matrice de séparation des rôles de l'entreprise.

Phase de migration

- Analyser l'état des anomalies rencontrées lors de la bascule réelle ;
- Analyser les critères de GO/NO GO ;
- Analyser les documents attestant la validation formelle de la reprise de données par les responsables appropriés.

Phase de post-implémentation

- Analyser le dispositif de recensement et remontée des anomalies (outils utilisés, procédures de correction, etc.) ;
- Examiner le tableau de bord de suivi des anomalies ;
- Analyser les PV de validation relatifs aux tests cibles réalisés sur les données migrées (afin de s'assurer de l'exhaustivité et exactitude de celles-ci).

ANALYSE DES RÉSULTATS

Les résultats de la mission vont permettre de :

- Parfaire la compréhension du dispositif de conduite de projet de l'entité ;
- Mesurer l'adéquation de ce dispositif aux bonnes pratiques en la matière ;
- Evaluer l'exhaustivité, la fiabilité et l'intégrité des données comptables et financières.

FICHE 05

UTILISATION DES OUTILS D'AUDIT DE DONNÉES

En cours de rédaction ...

UTILISATION DES OUTILS D'AUDIT DE DONNÉES

05

PROTECTION DES DONNÉES PERSONNELLES

AUDIT INFORMATIQUE : TOUS CONCERNÉS !
SERVICE AUTRE QUE LA CERTIFICATION DES COMPTES

FICHE 06

PROTECTION DES DONNÉES PERSONNELLES

06

PROPOSITION D'UN PÉRIMÈTRE D'INTERVENTION

OBJECTIFS DE LA PRESTATION

Une entité peut souhaiter confier à son commissaire aux comptes une intervention sur les obligations prévues par le Règlement Général sur la Protection des Données (RGPD).

Les travaux peuvent alors avoir pour objet, à la demande de l'entité :

- › de donner un avis sur sa conformité RGPD ;
- › de donner un avis sur la gouvernance des données ;
- › de donner un avis sur le contrôle interne du traitement des données ;
- › de donner un avis sur la sécurité des données.

Les avis peuvent être assortis de :

- › recommandations qui contribuent à répondre aux obligations de l'entité prévues par la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, plus connue sous le nom de loi informatique et libertés ainsi qu'aux obligations de l'entité prévues par le RGPD ;
- › recommandations visant à contribuer à l'amélioration des traitements et de la sécurité des données personnelles.

Dans les Entités d'Intérêt Public, les travaux du commissaire aux comptes ne peuvent pas inclure la participation¹ :

- › à la conception et la mise en œuvre de procédures de contrôle interne ou de gestion des risques en rapport avec la préparation et/ou le contrôle de l'information financière ;
- › à la conception et la mise en œuvre de systèmes techniques relatifs à l'information financière ;
- › aux services liés à la fonction d'audit interne de l'entité contrôlée.

La prestation décrite dans le présent document est un Service autre que la certification des comptes (SACC) : il ne s'agit pas d'une mission de certification des comptes.

Dans tous les cas, le commissaire aux comptes peut refuser l'intervention.

¹ Dans les entités non EIP, en vertu de la loi Pacte, ces services ne sont plus interdits mais doivent faire l'objet d'une approche risques / sauvegarde»

FICHE 06

PROTECTION DES DONNÉES PERSONNELLES

PÉRIMÈTRE D'INVESTIGATION

La CNCC a publié une mise à jour de son guide sur les SACC en novembre 2018, précisant les normes ou doctrines auxquelles faire référence lors de la réalisation des services autres que la certification des comptes. Dans le cas des travaux évoqués ici, les prestations suivantes sont envisageables :

- › des procédures convenues qui donneront lieu à des constats ;
- › des travaux qui permettront d'émettre une attestation avec éventuellement des observations ;
- › un examen limité qui permettra la formulation soit d'une conclusion sans observation, soit d'une conclusion avec observation(s), soit d'une conclusion défavorable, soit d'une impossibilité de conclure.

Pour répondre aux demandes de l'entité, le commissaire aux comptes met en œuvre les diligences nécessaires à son jugement professionnel, dans le cadre d'une obligation de moyens.

Il se réfère notamment :

- › Aux NEP ou aux normes ISA pour la vérification des données ;
- › Au COBIT qui est le référentiel international de gouvernance des systèmes d'information ;
- › Au COSO pour l'analyse du contrôle interne ;
- › À la norme ISAE 3000 (l'International Standard on Assurance Engagements 3000) qui détermine les principes de base et les procédures à mettre en œuvre lors de l'exécution d'une mission d'attestation autre qu'un audit ou une revue d'informations financières historiques.

Les travaux du commissaire aux comptes consistent à :

- › S'entretenir avec tous les interlocuteurs de la structure en lien avec la gestion et le traitement des données personnelles y compris le Délégué à la Protection des Données (DPO) ou le Référent si celui-ci a été nommé, afin d'identifier toutes les données et les traitements des données ;
- › Réaliser une analyse des systèmes d'information et des transferts de données hors de France ;
- › Réaliser une analyse de risques pour l'ensemble des données et l'ensemble des traitements ;
- › Réaliser une revue critique de l'analyse des risques effectuée par l'entité dans le cadre de ses obligations RGPD ;
- › Réaliser un examen des analyses d'impact éventuellement effectuée par l'entité ;
- › Réaliser une revue des clauses et mentions obligatoires d'information relative à la protection des données personnelles (site Internet, contrat de travail, règlement intérieur, charte informatique, formulaire de collecte de données personnelles, CGV et CGA ...);
- › Réaliser une revue critique du registre des traitements de données si celui-ci existe ;
- › Réaliser une revue des procédures internes de la structure afin de répondre aux droits des personnes (droit à l'information, droit d'opposition, droits d'accès et de rectification, droit à l'oubli, droit d'effacement, droit à la modification, droit à la limitation du traitement, droit à la portabilité, droit au déréférencement).
- › Réaliser une revue des procédures de notification de violation des données personnelles ;
- › Réaliser un examen des clauses prévues dans les contrats de prestation et de sous-traitance ;
- › Et enfin, réaliser une analyse de la sécurité des données.

Le commissaire aux comptes utilise également sa connaissance du contexte et du tissu économique dans lesquels évolue l'entité.

RAPPORT ET DOCUMENTATION

Le commissaire aux comptes consigne dans son dossier de travail :

- › l'analyse des forces et des faiblesses de gouvernance des données ;
- › l'analyse des données et des traitements de données ;
- › l'identification et l'analyse des zones de risques pour l'ensemble des données et l'ensemble des traitements ;
- › l'analyse des forces et des faiblesses des procédures internes pour répondre aux obligations RGPD ;
- › l'identification et l'analyse des zones de risques des systèmes d'information, des transferts de données et de la sécurité des données.
- › l'analyse du niveau de conformité RGPD ;
- › les conclusions des tests éventuels.

Le commissaire aux comptes émet un rapport avec les résultats des travaux qu'il a réalisés. Le rapport prend la forme d'un document daté et signé par le commissaire aux comptes et comporte selon les cas :

- › son analyse de la situation et des faits avec, le cas échéant, les références aux textes légaux et réglementaires, à la doctrine, à la pratique ou à un référentiel international ;
- › son avis quant au niveau de conformité RGPD de l'entreprise et de sa maturité en matière de gouvernance du système d'information et ses recommandations éventuelles, à la date de son rapport ;
- › les éléments d'informations et commentaires sur les textes qui font l'objet de la demande de l'entité.

06

FICHE 06

PROTECTION DES DONNÉES PERSONNELLES

PROPOSITION D'UNE DÉMARCHÉ MÉTHODOLOGIQUE

IDENTIFICATION DES ZONES DE RISQUES

Suite à la revue du contrôle interne, il convient dans un premier temps d'identifier au sein de l'entité, les données, les traitements ainsi que les processus les plus exposés puis, dans un second temps, d'évaluer ces risques. Les investigations sont ensuite organisées en fonction des risques qui auront pu être identifiés.

Dans le cas spécifique du RGPD, les processus COBIT : EDS01, EDS03, EDS05, AP012, AP013, BAI06, LSS02, LSS03, LSS04, LSS05 sont concernés, mais avec un focus particulier sur les processus de « **SURVEILLER, EVALUER, MESURER** » : SEM01, SEM02 et SEM03.

Les tests de procédures et les contrôles de substance sont identiques à ceux mis en œuvre par un audit traditionnel.

CHOIX DES TESTS À RÉALISER

S'agissant d'organisation et de procédures, les tests sont principalement des tests de compréhension et de procédures. Des cartographies du système d'information en termes d'infrastructure, d'applications, de flux de données et de traitements de données permettent d'évaluer la réponse aux obligations RGPD. Sur la base de ces cartographies, les responsabilités sont identifiées et testées, les données et les traitements évalués et les flux mesurés en termes de traçabilité et intégrité.

Les tests suivants peuvent être proposés :

Tests sur les données, processus et support

- › sur les données traitées
- › déroulement du cycle de vie (fonctionnement)
- › supports des données (réseau, logiciel...)

Tests sur la proportionnalité et nécessité

- › les finalités et légitimité des traitements des données
- › licéité des traitements
- › adéquations, pertinences des traitements et leurs limites
- › exactitudes des traitements et de leurs mises à jour
- › durée de conservation des données

Tests sur les mesures protectrices des droits

- › droit à l'information
- › droit d'accès à l'information
- › droit de rectification
- › droit d'effacement
- › droit de portabilité
- › droit d'opposition

Tests sur les risques

- › sur les mesures existantes ou prévues
- › contrat de sous-traitance
- › sensibilisation des collaborateurs

Accès illégitimes à des données

- › Impacts sur les personnes concernées
- › Principales menaces
- › Les sources de risques
- › Les mesures pour traiter les risques
- › Estimation de la gravité du risque
- › Vraisemblance des risques

Modifications non désirées de données

- › Impacts sur les personnes concernées
- › Principales menaces
- › Les sources de risques
- › Les mesures pour traiter les risques
- › Estimation de la gravité du risque
- › Vraisemblance des risques

06

FICHE 06

PROTECTION DES DONNÉES PERSONNELLES

Disparition des données

- › Impacts sur les personnes concernées
- › Principales menaces
- › Les sources de risques
- › Les mesures pour traiter les risques
- › Estimation de la gravité du risque
- › Vraisemblance des risques

Tests sur la sécurité des données

Tester l'impact du RGPD sur les différents services (RH, marketing, financier...)

- › Marketing
 - › Données personnelles
 - › Permissions
 - › Processus
 - › Technologie
 - › Indicateurs
 - › Personnes
- › RH
 - › Cartographie des données
 - › Collecte des données
 - › Informations des candidats et employés
 - › Stocker et sécuriser les données

Tests sur la confiance numérique (le CLOUD)

Tests sur le DPO

- › Choix d'un DPO : interne, externe, mutualisé
- › L'organisation de la mission

Tests sur les transferts de données hors UE

- › Compréhension de cette notion de transfert
- › Respect des conditions de la licéité d'un transfert de données hors de l'UE

Tester la gestion et l'anticipation des sanctions

En fonction du secteur d'activité de l'entité auditée, l'auditeur doit définir les types de tests à réaliser. Concernant le contrôle interne, l'analyse doit identifier les domaines où la maturité est moindre et donc l'existence de risques qui peuvent faire l'objet d'extension de missions afin d'effectuer des tests plus détaillés des procédures concernées.

ANALYSE DES RÉSULTATS

Les résultats de la mission vont permettre :

- › de parfaire la compréhension du système d'information par rapport aux processus de l'entreprise ;
 - › de mesurer l'adéquation de l'organisation de la DSI mais aussi des rôles et responsabilités des utilisateurs métier ;
 - › d'évaluer la sensibilité des données, des traitements et de leur gouvernance,
 - › de mesurer la maturité en termes de contrôle interne du système d'information et des obligations RGPD ;
 - › de mesurer le niveau de sécurité des données ;
- enfin et surtout, de mesurer le niveau de conformité RGPD de la structure.

06

LÉGISLATION FISCALE & SI

FICHE 07 LÉGISLATION FISCALE ET SI

07

PROPOSITION D'UN PÉRIMÈTRE D'INTERVENTION

OBJECTIFS DE LA PRESTATION

Une entité peut souhaiter confier à son commissaire aux comptes une intervention tendant à évaluer le dispositif relatif à la transmission à l'administration fiscale :

- › des éléments requis dans le cadre d'un contrôle fiscal des comptabilités informatisées (CFI),
- › du fichier des écritures comptables (FEC),
- › des éléments contribuant à la piste d'audit fiable.

Toutes les entités peuvent être concernées par l'évaluation de leur dispositif de conformité aux obligations fiscales mais cette intervention s'adresse en premier lieu aux entités soumises aux déclarations de TVA et soumises à l'IS. L'administration fiscale demeure toutefois souveraine dans ses demandes.

Les travaux ont pour objet, à la demande de l'entité de s'assurer de :

- › La conformité du corpus documentaire au regard des obligations requises par l'administration fiscale,
- › La mise à disposition d'un fichier des écritures comptables ou des données nécessaires dans le cadre d'un contrôle fiscal des comptabilités informatisées,
- › La conformité de ce fichier des écritures comptable au regard des spécifications requises par l'administration fiscale (format et contenu),
- › La capacité de l'organisation à prouver la piste d'audit fiable en matière de facturation pour garantir l'authenticité de l'origine, l'intégrité du contenu, la lisibilité de la facture.

Les avis peuvent être assortis de recommandations visant à contribuer à l'amélioration de la transmission, de la documentation et des traitements de l'information financière et fiscale.

Dans les Entités d'Intérêt Public, les travaux du commissaire aux comptes ne peuvent pas inclure la participation¹ :

- › à la conception et la mise en œuvre de procédures de contrôle interne ou de gestion des risques en rapport avec la préparation et/ou le contrôle de l'information financière ;
- › à la conception et la mise en œuvre de systèmes techniques relatifs à l'information financière ;
- › aux services liés à la fonction d'audit interne de l'entité contrôlée.

La prestation décrite dans le présent document est un Service autre que la certification des comptes (SACC) : il ne s'agit pas d'une mission de certification des comptes.

Dans tous les cas, le commissaire aux comptes peut refuser l'intervention.

¹ Dans les entités non EIP, en vertu de la loi Pacte, ces services ne sont plus interdits mais doivent faire l'objet d'une approche risques / sauvegarde »

FICHE 07

LÉGISLATION FISCALE ET SI

07

PÉRIMÈTRE D'INVESTIGATION

La CNCC a publié une mise à jour de son guide sur les SACC en novembre 2018, précisant les normes ou doctrines auxquelles faire référence lors de la réalisation des services autres que la certification des comptes. Dans le cas des travaux évoqués ici, les prestations suivantes sont envisageables :

- des procédures convenues qui donneront lieu à des constats ;
- des travaux qui permettront d'émettre une attestation avec éventuellement des observations ;
- un examen limité qui permettra la formulation soit d'une conclusion sans observation, soit d'une conclusion avec observation(s), soit d'une conclusion défavorable, soit d'une impossibilité de conclure

Pour répondre aux demandes de l'entité, le commissaire aux comptes met en œuvre toutes les diligences possibles dans le cadre d'une obligation de moyens.

Les travaux du commissaire aux comptes portent sur :

- La revue de la documentation relative à la piste d'audit fiable, à la constitution du FEC et aux autres données identifiées par l'entreprise dans le cadre d'un CFCI.
- La conformité du FEC, tant dans sa structure que dans son contenu et la capacité de l'organisation à fournir une piste d'audit fiable
- Pour ce faire, réalisation de tests afin d'identifier des risques d'anomalies sur les informations fiscales par des techniques d'investigation assistées par ordinateur.

Le commissaire aux comptes utilise également sa connaissance du contexte et du tissu économique dans lesquels évolue l'entité.

RAPPORT ET DOCUMENTATION

Le commissaire aux comptes consigne dans son dossier de travail :

- L'analyse des forces et des faiblesses de l'organisation et des systèmes évalués en matière d'obligations fiscales ;
- L'identification et l'analyse des zones de risques ;
- Le détail des tests conçus et mis en œuvre en réponse à son évaluation des risques.

Le commissaire aux comptes émet un rapport avec les résultats des travaux qu'il a réalisés. Le rapport prend la forme d'un document daté et signé par le commissaire aux comptes et comporte selon les cas :

- Son analyse de la situation et des faits avec, le cas échéant, les références aux textes légaux et réglementaires, à la doctrine, à la pratique du marché ;
- Son avis quant à l'existence de failles dans la mise en place d'un dispositif répondant aux exigences fiscales ou ses recommandations éventuelles ;
- Les éléments d'informations et commentaires sur les textes qui font l'objet de la demande de l'entité.

FICHE 07

LÉGISLATION FISCALE ET SI

07

PROPOSITION D'UNE DÉMARCHE MÉTHODOLOGIQUE

IDENTIFICATION DES ZONES DE RISQUES

Suite à la revue du contrôle interne, il convient dans un premier temps d'identifier au sein de l'entité, les cycles et les processus les plus exposés puis, dans un second temps, d'évaluer ces risques. Les investigations sont ensuite organisées en fonction des risques qui auront pu être identifiés.

Dans le cas spécifique des obligations aux exigences fiscales, nous avons recensé les processus COBIT suivants :

BAI01	Gérer les programmes et les projets
BAI02	Gérer la définition des exigences
BAI03	Gérer l'identification et la conception des solutions
BAI04	Gérer la disponibilité et la capacité
BAI05	Gérer le changement organisationnel
BAI08	Gérer la connaissance
BAI09	Gérer les actifs
BAI10	Gérer la configuration

CHOIX DES TESTS À RÉALISER

Les tests à réaliser seront de différentes natures. Ceux-ci peuvent être réalisés par thématique :

Gouvernance et revue de la documentation

- Évaluer le dispositif de gouvernance pour répondre aux exigences fiscales
- Analyser la documentation requise dans le cadre de contrôles fiscaux
 - Description de l'environnement informatique
 - Cartographie applicative et matérielle
 - Description du modèle de données
 - Dossier de conception générale et détaillée, fiche de paramétrage / développement
 - Dossier explicatif de la constitution du FEC (Annexe)
 - Documentation de la piste d'audit fiable
 - Dossier d'archivage
 - Etc.

Conformité du FEC

- Réalisation de contrôles sur la conformité du FEC
 - Structure du FEC
 - Valeurs renseignées dans les zones de l'écriture / analyse du contenu
 - Cohérence des données comptables

Tests de la piste d'audit fiable

- Analyse des processus par segmentation d'achats / ventes et de leur fiabilité
- Évaluation du niveau de conformité / caractérisation des cas de non-conformité sur la base d'échantillons de tests

ANALYSE DES RÉSULTATS

Les résultats de la mission vont permettre de :

- Comprendre le dispositif de mise en conformité aux exigences fiscales,
- Mesurer l'adéquation de ce dispositif aux bonnes pratiques en la matière et aux exigences requises,
- D'évaluer les zones de risques liées à un contrôle de l'administration fiscale.

EXPLOITATION DES SYSTÈMES D'INFORMATION

FICHE 08

EXPLOITATION DES SYSTÈMES D'INFORMATION

08

PROPOSITION D'UN PÉRIMÈTRE D'INTERVENTION

OBJECTIFS DE LA PRESTATION

Une entité peut souhaiter confier à son commissaire aux comptes une intervention visant à évaluer la fonction « exploitation des systèmes informatiques ». Cette fonction essentielle permet de maintenir l'efficacité, la confidentialité, l'intégrité, la disponibilité, la conformité, la fiabilité et la sécurité du système informatique.

Toutes les entités qui utilisent un système informatique sont concernées : le fonctionnement des entités et parfois même leur survie, dépendent de plus en plus du bon fonctionnement de leur système informatique.

Les travaux ont pour objet, à la demande de l'entité :

- › de donner un avis sur les forces et faiblesses dans les procédures en place, relatives à l'exploitation du système informatique de l'entité ;
- › d'identifier des vulnérabilités qui pourraient compromettre le bon fonctionnement du système informatique de l'entité ;
- › fournir un support de formation sur les bonnes pratiques en matière d'exploitation des systèmes informatiques.

Les avis peuvent être assortis de recommandations visant à contribuer à améliorer l'efficacité, la confidentialité, l'intégrité, la disponibilité, la conformité, la fiabilité et la sécurité du système informatique de l'entité.

Dans les Entités d'Intérêt Public, les travaux du commissaire aux comptes ne pourront pas inclure la participation¹ :

- › à la conception et la mise en œuvre de procédures d'exploitation.
- › à la conception et la mise en œuvre de systèmes d'information de gestion.
- › aux services liés à la fonction d'audit interne de l'entité contrôlée.

La prestation décrite dans le présent document est un Service Autre que la Certification des Comptes (SACC) : il ne s'agit pas d'une mission de certification des comptes.

Dans tous les cas, le commissaire aux comptes peut refuser l'intervention.

¹ Dans les entités non EIP, en vertu de la loi Pacte, ces services ne sont plus interdits mais doivent faire l'objet d'une approche risques / sauvegarde »

FICHE 08

EXPLOITATION DES SYSTÈMES D'INFORMATION

PÉRIMÈTRE D'INVESTIGATION

La CNCC a publié une mise à jour de son guide sur les SACC en novembre 2018, précisant les normes ou doctrines auxquelles faire référence lors de la réalisation des services autres que la certification des comptes. Dans le cas des travaux évoqués ici, les prestations suivantes sont envisageables :

- des procédures convenues qui donneront lieu à des constats ;
- des travaux qui permettront d'émettre une attestation avec éventuellement des observations ;
- un examen limité qui permettra la formulation soit d'une conclusion sans observation, soit d'une conclusion avec observation(s) soit d'une impossibilité de conclure.

Pour répondre aux demandes de l'entité, le commissaire aux comptes met en œuvre les diligences qu'il juge nécessaires dans le cadre d'une obligation de moyens.

Il se référera notamment à COBIT qui est le référentiel international de gouvernance des SI.

Les travaux du commissaire aux comptes portent sur :

- la documentation des procédures d'exploitation,
- les comptes rendus des tests de conformité réalisés sur les procédures existantes par l'entité et / ou des tests de conformité réalisés par le commissaire aux comptes lui-même,
- les comptes rendus des tests de restauration de données réalisés par l'entité,
- les comptes rendus des tests de reprise d'activité après sinistre réalisés par l'entité,
- les journaux (logs) produits automatiquement par les systèmes informatiques,
- les contrats conclus avec des tiers auprès de qui tout ou partie de l'exploitation du système informatique est sous-traitée,
- les comptes relatifs aux actifs immobilisés (investissements en infrastructure informatique) et aux charges liées au fonctionnement du système informatique,
- le système d'information en général, et les traitements informatisés des données de gestion en particulier.

Le commissaire aux comptes utilise également sa connaissance du contexte et le cas échéant, son expérience acquise en matière de gestion des risques informatiques.

RAPPORT ET DOCUMENTATION

Le commissaire aux comptes consigne dans son dossier de travail :

- l'analyse des forces et des faiblesses dans les procédures en place relatives à l'exploitation du système informatique ;
- l'identification de vulnérabilités et de zones de risques qui pourraient compromettre le bon fonctionnement du système informatique,
- les comptes rendus des tests de conformité réalisés sur les procédures d'exploitation existantes,
- les comptes rendus des tests de restauration de données et de reprise d'activité après sinistre,
- la synthèse sur les tests réalisés avec la mise en évidence des éléments de non-conformité et des vulnérabilités ou autres facteurs de risques qui pourraient compromettre le bon fonctionnement du système informatique.

Le commissaire aux comptes émet un rapport avec les résultats des travaux qu'il a réalisés. Le rapport prend la forme d'un document daté et signé par le commissaire aux comptes et comporte selon les cas :

- son analyse de la situation et des faits avec, le cas échéant, les références aux textes légaux et réglementaires, à la doctrine, à la pratique ou à un référentiel international de gouvernance informatique ;
- son avis quant à l'existence de vulnérabilités ou autres facteurs de risques et ses recommandations éventuelles ;
- les éléments d'informations et commentaires sur les textes qui font l'objet de la demande de l'entité.

08

FICHE 08

EXPLOITATION DES SYSTÈMES D'INFORMATION

08

PROPOSITION D'UNE DÉMARCHE MÉTHODOLOGIQUE

IDENTIFICATION DES ZONES DE RISQUES

Suite à la revue du contrôle interne, et en particulier suite aux tests de conformité réalisés sur les procédures d'exploitation existantes, il convient dans un premier temps d'identifier au sein de l'entité, les cycles et les processus les plus exposés puis, dans un second temps, d'évaluer les risques. Les investigations sont ensuite organisées en fonction des risques qui ont pu être identifiés.

Dans le cas spécifique de l'évaluation de la fonction «exploitation des systèmes informatiques», nous avons recensé les processus COBIT dont les défaillances pourraient rendre l'entité vulnérable en cas de défaillance de son système informatique.

A noter : L'exploitation des systèmes informatiques est une fonction transverse, pour autant nous avons délimité son domaine par rapport aux autres fiches :

BAI04	Gérer la disponibilité et la capacité
BAI10	Gérer la configuration
LSS01	Gérer les opérations
LSS02	Gérer les demandes de services et les incidents
LSS06	Gérer les contrôles des processus métier
SEM01	Surveiller, évaluer et mesurer la performance et la conformité

Le cas échéant, ces processus font l'objet de tests de procédure.

Les tests de procédures et les contrôles de substance sont identiques à ceux mis en œuvre par un audit traditionnel.

CHOIX DES TESTS À RÉALISER

L'évaluation de la fonction «exploitation des systèmes informatiques» s'appuie sur l'évaluation des procédures d'exploitation et l'identification des risques qui peuvent remettre en cause l'efficacité du système d'information, la confidentialité et l'intégrité des données, la disponibilité du système informatique et donc la continuité d'activité de l'entité, la conformité, la fiabilité et la sécurité du système d'information.

On peut citer :

Lecture et analyse critique des procédures d'exploitation existantes

Tests de conformité sur les procédures d'exploitation

Évaluation du contrôle interne de la fonction informatique et en particulier recherche des réponses aux questions suivantes :

- › Les fonctions de développement, de tests et d'exploitation sont-elles séparées ?
- › Les équipements de développement, de tests et d'exploitation sont-ils séparés ?

Analyse des contrats d'externalisation, de sous-traitance, d'hébergement, de Cloud... Évaluation des risques associés et des clauses de réversibilité.

Analyse des solutions de sécurité informatique (antivirus, pare feu, antispam, gestion centralisée des mises à jour et des alertes...). Évaluation de la pertinence et de l'exhaustivité des solutions de sécurité.

Évaluation des procédures de sauvegarde et de restauration. Lecture des comptes rendus des tests de restauration.

Évaluation de la procédure de reprise d'activité après sinistre. Lecture critique des comptes rendus rédigés à l'issue des tests de reprise d'activité.

Analyse des mesures de sécurité protégeant les connexions distantes au système d'information.

Analyse des procédures de gestion pour les supports et les équipements mobiles, pouvant contenir des données sensibles.

Évaluation de la procédure d'analyse et de surveillance des journaux (logs) produits automatiquement par les composants du système informatique (serveurs, pare feu, antivirus...)

ANALYSE DES RÉSULTATS

Les résultats de la mission vont permettre :

- › d'évaluer, sous l'angle des opérations de tous les jours, l'efficacité, la confidentialité, l'intégrité, la disponibilité, la conformité, la fiabilité et la sécurité du système informatique de l'entité
- › d'identifier des vulnérabilités qui pourraient compromettre le bon fonctionnement du système informatique de l'entité
- › de mesurer la maturité en termes de contrôle interne du SI.

PLAN DE CONTINUITÉ D'ACTIVITÉ

AUDIT INFORMATIQUE : TOUS CONCERNÉS !
SERVICE AUTRE QUE LA CERTIFICATION DES COMPTES

FICHE 09 PLAN DE CONTINUITÉ D'ACTIVITÉ

09

PROPOSITION D'UN PÉRIMÈTRE D'INTERVENTION

OBJECTIFS DE LA PRESTATION

Une entité peut souhaiter confier à son commissaire aux comptes une intervention tendant à la revue du Plan de Secours et/ou du Plan de la Continuité d'Activité.

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. Le Plan de Secours (PS) ne concerne que la reprise des actifs informatiques et informationnels alors que le Plan de Continuité d'Activité comprend les procédures dégradées (ou pas) mises en œuvre par le « métier » en cas de sinistre. 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.

Les travaux ont pour objet, à la demande de l'entité :

- De revoir le dispositif de reprise des actifs informatiques et informationnels ;
- De revoir les procédures pour s'assurer d'une reprise d'activité de l'entreprise suite à un sinistre majeur.

Les avis peuvent être assortis de recommandations qui visent à contribuer à l'amélioration des traitements de l'information financière et qui portent sur des éléments du contrôle interne objets de la consultation.

Dans les Entités d'Intérêt Public, les travaux du commissaire aux comptes ne peuvent pas inclure la participation¹ :

- à la conception et la mise en œuvre de procédures de contrôle interne ou de gestion des risques en rapport avec la préparation et/ou le contrôle de l'information financière ;
- à la conception et la mise en œuvre de systèmes techniques relatifs à l'information financière ;
- aux services liés à la fonction d'audit interne de l'entité contrôlée.

La prestation décrite dans le présent document est un Service autre que la certification des comptes (SACC) : il ne s'agit pas d'une mission de certification des comptes.

Dans tous les cas, le commissaire aux comptes peut refuser l'intervention.

¹ Dans les entités non EIP, en vertu de la loi Pacte, ces services ne sont plus interdits mais doivent faire l'objet d'une approche risques / sauvegarde »

FICHE 09

PLAN DE CONTINUITÉ D'ACTIVITÉ

PÉRIMÈTRE D'INVESTIGATION

La CNCC a publié une mise à jour de son guide sur les SACC en novembre 2018, précisant les normes ou doctrines auxquelles faire référence lors de la réalisation des services autres que la certification des comptes. Dans le cas des travaux évoqués ici, les prestations suivantes sont envisageables :

- des procédures convenues qui donneront lieu à des constats ;
- des travaux qui permettront d'émettre une attestation avec éventuellement des observations ;
- un examen limité qui permettra la formulation soit d'une conclusion sans observation, soit d'une conclusion avec observation(s), soit d'une conclusion défavorable, soit d'une impossibilité de conclure.

Pour répondre aux demandes de l'entité, le commissaire aux comptes met en œuvre toutes les diligences possibles dans le cadre d'une obligation de moyens.

Il se réfère notamment à COBIT qui est le référentiel international de gouvernance des SI.

Les travaux du commissaire aux comptes peuvent porter sur :

- les applications, infrastructures et couches basses ;
- des éléments du contrôle interne relatifs au traitement des opérations de l'entité ;
- le système d'information en général, et les traitements informatisés des données financières en particulier.

Le commissaire aux comptes utilise également sa connaissance du contexte et du tissu économique dans lesquels évolue l'entité.

RAPPORT ET DOCUMENTATION

Le commissaire aux comptes consigne dans son dossier de travail :

- L'analyse des forces et des faiblesses de l'organisation et des systèmes évalués en matière de plan de secours et de continuité d'activité ;
- L'identification et l'analyse des zones de risques liés à la continuité d'exploitation ;
- Les tests de Plan de Secours, conçus et mis en œuvre en réponse à son évaluation des risques.

Le commissaire aux comptes émet un rapport avec les résultats des travaux qu'il a réalisés. Le rapport prend la forme d'un document daté et signé par le commissaire aux comptes et comporte selon les cas :

- son analyse de la situation et des faits avec, le cas échéant, les références aux textes légaux et réglementaires, à la doctrine, à la pratique ou à un référentiel international de gouvernance informatique ;
- son avis quant à l'existence de failles de disponibilité du système d'information ou ses recommandations éventuelles ;
- les éléments d'informations et commentaires sur les textes qui font l'objet de la demande de l'entité.

FICHE 09

PLAN DE CONTINUITÉ D'ACTIVITÉ

PROPOSITION D'UNE DÉMARCHE MÉTHODOLOGIQUE

IDENTIFICATION DES ZONES DE RISQUES

Suite à la revue du contrôle interne, il convient dans un premier temps d'identifier au sein de l'entité, les cycles et les processus les plus exposés puis, dans un second temps, d'évaluer ces risques. Les investigations sont ensuite organisées en fonction des risques qui ont pu être identifiés et appliqués au système d'information supportant ces cycles et processus.

Dans le cadre de la revue du plan de continuité d'activité, une attention particulière est évidemment consacrée aux données et cycles ayant un impact fort sur la continuité d'exploitation de l'entité. Cela peut concerner dans le cadre d'une entreprise industrielle les systèmes et données de la chaîne de production.

Dans le cas spécifique de la revue de continuité d'activité, nous avons recensé les processus COBIT dont les défaillances peuvent rendre l'entité vulnérable :

EDS03	Assurer l'optimisation du risque
APO09	Gérer les accords de services
APO10	Gérer les fournisseurs
APO12	Gérer le risque
BAI10	Gérer la configuration
LSS04	Gérer la continuité
SEM02	Surveiller, évaluer et mesurer le système de contrôle interne

Le cas échéant, ces processus font l'objet de tests de procédure.

CHOIX DES TESTS À RÉALISER

Les travaux sont de différentes natures :

Revue de la « Business Impact Analysis » (Analyse d'Impact Métier) qui s'assure que les éléments critiques essentiels de l'entité ont bien été identifiés et qu'une classification / priorisation a bien été réalisée ;

Analyse des politiques de Sauvegarde et d'Archivage ;

Analyse du Plan de Secours pour les actifs informatiques et informationnels ;

Analyse du Plan de Continuité d'Activité

Dans les deux cas (PS et PCA), les analyses concernent :

- Identification des objectifs et les activités essentielles
- Identification du SI sous jacent
- Détermination et attentes de disponibilité / sécurité pour tenir des objectifs
- Identification, analyse, évaluation et traitement des risques
- Définition de la stratégie de continuité d'activité
- Mise en œuvre et appropriation
- Test périodique

Revue des tests périodiques du Plan de Secours et du Plan de Continuité d'Activité

Analyse des plans d'actions

ANALYSE DES RÉSULTATS

Les résultats des tests vont permettre de repérer des anomalies dans la disponibilité des transactions opérationnelles, financières et comptables.

Dans le cadre d'identification de zones de risques sur des données essentielles critiques, des plans d'actions sont recommandés.

FICHE 10 CYBERCRIMINALITÉ

10

PROPOSITION D'UN PÉRIMÈTRE D'INTERVENTION

OBJECTIFS DE LA PRESTATION

Une entité peut souhaiter confier à son commissaire aux comptes une intervention tendant à la détection de fraudes externes dans les comptes de l'entité.

Toutes les entités sont concernées par la détection de fraudes externes mais cette intervention s'adresse en premier lieu aux opérateurs visés par la loi de programmation militaire 2014-2019 et aux entreprises sous-traitantes de ces opérateurs.

Les travaux ont pour objet, à la demande de l'entité :

- › de donner un avis quant à la probabilité d'existence de fraudes externes dans les comptes et les informations financières dans le périmètre d'investigation ;
- › ou de fournir un support de formation concernant des textes, des projets de textes ou des pratiques contribuant à la bonne compréhension des obligations de l'entité en matière de lutte contre la fraude externe ;
- › ou de donner un avis sur les forces et faiblesses d'éléments du contrôle interne ou du système d'information en place.

Les avis peuvent être assortis de recommandations visant à contribuer à l'amélioration des traitements de l'information financière et qui portent sur des éléments du contrôle interne objets de la consultation.

Dans les Entités d'Intérêt Public, les travaux du commissaire aux comptes ne peuvent pas inclure la participation :

- › à la conception et la mise en œuvre de procédures de contrôle interne ou de gestion des risques en rapport avec la préparation et/ou le contrôle de l'information financière ;
- › à la conception et la mise en œuvre de systèmes techniques relatifs à l'information financière ;
- › aux services liés à la fonction d'audit interne de l'entité contrôlée.

La prestation décrite dans le présent document est un Service autre que la certification des comptes (SACC) : il ne s'agit pas d'une mission de certification des comptes.

Dans tous les cas, le commissaire aux comptes peut refuser l'intervention.

¹ Dans les entités non EIP, en vertu de la loi Pacte, ces services ne sont plus interdits mais doivent faire l'objet d'une approche risques / sauvegarde »

FICHE 10 CYBERCRIMINALITÉ

PÉRIMÈTRE D'INVESTIGATION

La CNCC a publié une mise à jour de son guide sur les SACC en novembre 2018, précisant les normes ou doctrines auxquelles faire référence lors de la réalisation des services autres que la certification des comptes. Dans le cas des travaux évoqués ici, les prestations suivantes sont envisageables :

- des procédures convenues qui donneront lieu à des constats ;
- des travaux qui permettront d'émettre une attestation avec éventuellement des observations ;
- un examen limité qui permettra la formulation soit d'une conclusion sans observation, soit d'une conclusion avec observation(s), soit d'une conclusion défavorable, soit d'une impossibilité de conclure.

Pour répondre aux demandes de l'entité, le commissaire aux comptes met en œuvre toutes les diligences qu'il juge nécessaires dans le cadre d'une obligation de moyens.

Les travaux du commissaire aux comptes portent sur :

- des comptes, états comptables ou éléments des comptes de l'entité ;
- l'exhaustivité des écritures comptables et des transactions de l'entité grâce à des outils d'analyse de gros volumes de données ;
- des informations, données ou documents de l'entité ayant un lien avec la comptabilité ou les données sous-tendant celle-ci ;
- des éléments du contrôle interne relatifs au traitement comptable et financier de l'entité ;
- le système d'information en général, et les traitements informatisés des données financières en particulier.

Les comptes concernent un exercice complet ou une autre période définie. Le recours à des techniques d'investigation assistées par ordinateur permet d'effectuer des tests exhaustifs sur des opérations traitées électroniquement ou des fichiers informatiques.

Le commissaire aux comptes utilise également sa connaissance du contexte et du tissu économique dans lesquels évolue l'entité.

RAPPORT ET DOCUMENTATION

Le commissaire aux comptes consigne dans son dossier de travail :

- l'analyse des forces et des faiblesses de l'organisation et des systèmes évalués en matière de lutte contre la fraude externe ;
- l'identification et l'analyse des risques de fraude externe ;
- le calendrier et les tests de détection de fraudes, conçus et mis en œuvre en réponse à son évaluation des risques de fraude externe ;
- les conclusions des tests de détection d'éventuelles fraudes externes.

Le commissaire aux comptes émet un rapport avec les résultats des travaux qu'il a réalisés. Le rapport prend la forme d'un document daté et signé par le commissaire aux comptes et comporte selon les cas :

- son analyse de la situation et des faits avec, le cas échéant, les références aux textes légaux et réglementaires, à la doctrine, à la pratique ou à un référentiel international de gouvernance informatique ;
- son avis quant à l'existence de fraudes externes ou ses recommandations éventuelles ;
- les éléments d'informations et commentaires sur les textes qui font l'objet de la demande de l'entité.

10

FICHE 10 CYBERCRIMINALITÉ

PROPOSITION D'UNE DÉMARCHE MÉTHODOLOGIQUE

IDENTIFICATION DES ZONES DE RISQUES

Suite à la revue du contrôle interne, il convient dans un premier temps d'identifier au sein de l'entité, les cycles et les processus les plus exposés puis, dans un second temps, d'évaluer les risques. Les investigations sont ensuite organisées en fonction des risques qui ont pu être identifiés. S'agissant de détection de fraudes, une attention particulière est évidemment consacrée aux cycles « Ventes - Clients », « Achats - Fournisseurs », « Trésorerie » et « Immobilisations » qui pourront faire l'objet de tests de procédures et de contrôle de substance.

Dans le cas spécifique des cyber-fraudes, nous recensons les processus COBITT dont les défaillances peuvent rendre l'entité vulnérable aux cyber-attaques :

APO12	Gérer le risque
APO13	Gérer la sécurité
LSS04	Gérer la continuité
LSS05	Gérer les services de sécurité
SEMO2	Surveiller, évaluer et mesurer le système de contrôles internes
SEMO3	Surveiller, évaluer et mesurer la conformité aux exigences externes

Le cas échéant, ces processus feront l'objet de tests de procédures.

Les tests de procédures et les contrôles de substance sont identiques à ceux mis en œuvre par un audit traditionnel. Néanmoins, pour permettre la détection de fraudes, ils doivent être exhaustifs plutôt qu'être réalisés par sondage.

CHOIX DES TESTS À RÉALISER

Seule l'exhaustivité des contrôles comptables est de nature à permettre l'identification des transactions atypiques qui, dans un deuxième temps, feront l'objet d'investigations plus approfondies. Les logiciels de fouille de données (« data mining ») proposent un large panel de tests utiles à la détection de fraudes :

- Analyse de corrélation pour déterminer la relation entre plusieurs variables parmi des données brutes. Des corrélations aberrantes ou absentes permettront de présumer d'une dissimulation de fraude.
- Analyse de la conformité des opérations aux seuils fixés par le contrôle interne.
- Stratification (par montant, par dates, etc.) pour connaître les caractéristiques des données analysées : montants les plus élevés, montants les plus petits, etc.
- Sélection des données spécifiques et des exceptions (montants légèrement en deçà des seuils, petits montants, montants ronds, etc.) pour investigations approfondies.
- Comparaison de fichiers pour identifier les données communes et les données différentes (listes de fournisseurs, listes d'assurés bénéficiant de remboursement, etc.)
- Rapprochement de données appartenant à des fichiers différents
- Recherche de doublons (redondance des petits prélèvements, unique fournisseur avec deux relevés différents de coordonnées bancaires) ou de «trous» dans les séquences (rupture sur les numéros de chèque, sur les numéros d'enregistrement, etc.)
- Test de la loi de Benford

En fonction du secteur d'activité de l'entité auditée et compte tenu des schémas de fraude à détecter, l'auditeur doit définir les types de tests à réaliser. Par exemple, dans le secteur du crédit à la consommation, des tests de corrélation sont mis en œuvre sur les incidents de remboursement de prêt.

Concernant le contrôle interne, la détection de fraudes doit privilégier la recherche des exceptions (montants légèrement en deçà des seuils, petits montants, montants ronds, etc.) et leur analyse, car ce sont elles qui favorisent la fraude en permettant de contourner les procédures en place. Là encore, ces exceptions doivent faire l'objet de tests exhaustifs de procédures.

FICHE 10 CYBERCRIMINALITÉ

L'audit technique doit permettre de fournir un avis sur le niveau de sécurité atteint par le système d'information.

Il pourra notamment intégrer les contrôles suivants :

Audit des choix d'architecture (authentification, échange de données, protection des données, sauvegarde, etc.) et des choix de configuration sur un échantillon d'équipements (système d'exploitation, système de gestion de bases de données relationnelles (SGBDR), serveur de messagerie, pare-feu etc.). Il s'agit notamment de s'assurer de l'application des derniers correctifs de sécurité, du respect de la politique des mots de passe, de l'absence de protocoles non sécurisés comme Telnet ou FTP ;

Audit de la gestion de l'authentification des utilisateurs pour s'assurer de l'existence de :

- › Sécurisation des connexions
- › Stockage chiffré des mots de passes (fonction de hachage)
- › Transmission des informations d'authentification (requête POST)
- › Protection contre les attaques de type « force brute » (CAPTCHA, mécanismes de blocage des accès en « force brute », avec verrouillage automatique des comptes après un nombre prédéfini d'erreurs dans le mot de passe)
- › Gestion du renouvellement de mots de passe
- › Contraintes sur le format des mots de passe
- › Gestion de traces lors des authentifications réussies / échouées.

Audit de la gestion des sessions applicatives pour s'assurer de la :

- › Sécurité horizontale des comptes utilisateurs (un utilisateur ne peut pas consulter les informations d'un autre utilisateur ayant le même profil au sein de l'application)
- › Sécurité verticale des comptes utilisateurs (un utilisateur ayant des droits restreints ne peut pas obtenir de droits d'administration sur l'application)
- › Prise en charge de la gestion des cookies et de leur durée de vie

Audit des pratiques cryptographiques pour s'assurer de l'existence de :

- › Choix et implémentation d'algorithmes cryptographiques
- › Contraintes sur la taille des clés
- › Stockage des clés de chiffrement

Audit de la protection des données des applications développées en interne pour s'assurer des points suivants :

- › Aucune information sensible au sein des commentaires du code de l'application
- › Séparation des fonctions entre utilisateurs et développeurs
- › Stockage des informations sensibles de manière chiffrée
- › Echange sécurisé des informations entre le client et le serveur (protocole TLS par exemple)

Tests d'intrusion pour évaluer la sécurité du système d'information de l'entreprise. Ils sont réalisables soit sans information préalable (« boîte noire ») ; soit en ayant des accès limités, une connaissance relative de la topologie du système d'information, ou en ayant un compte avec un accès limité (« boîte grise ») ; soit enfin, en ayant des accès étendus ou une connaissance documentée de la topologie réseau ou des applicatifs (« boîte blanche ») ;

Tests d'intrusion Wi-Fi en tentant de récupérer des clés Wi-Fi, d'usurper l'identité d'un utilisateur identifié, etc.

ANALYSES DES RÉSULTATS

Les résultats des tests permettent de repérer des anomalies dans les transactions financières et comptables. L'analyse de ces anomalies nécessite d'affiner encore les tests sur un périmètre plus restreint, après stratification ou requêtes spécifiques, afin de déterminer si le schéma de fraude recherché est avéré ou non.

Il faut en effet garder à l'esprit que tout ce qui ressemble à une fraude n'en est pas forcément une et qu'il est nécessaire de corroborer les données informatiques avec d'autres éléments de preuve, comme les justificatifs papier par exemple. Le jugement professionnel demeure primordial dans la détection de fraude.

AUDIT DE SERVICES EXTERNALISÉS

FICHE 11 AUDIT DE SERVICES EXTERNALISÉS

11

PROPOSITION D'UN PÉRIMÈTRE D'INTERVENTION

OBJECTIFS DE LA PRESTATION

Les clients d'un prestataire, auprès de qui ils ont externalisé des services impactant leurs états financiers, ont besoin d'obtenir des assurances et évaluations sur le contrôle interne des processus associés à ces prestations¹. Dans ce cas, le prestataire a, en pratique, la possibilité de confier une mission ISAE 3402² à un auditeur de son choix (c'est l'objet du présent SACC), ou de laisser l'auditeur du client effectuer lui-même cet audit.

Une entité peut souhaiter confier à son commissaire aux comptes une intervention tendant à la formalisation d'un rapport ISAE 3402 dans le cadre de prestations de services externalisés que l'entité opère pour ses clients. Ces prestations de services peuvent concerner des services informatiques (hébergement, exploitation informatique, développement informatique, etc.) ou des prestations intellectuelles (paie, comptabilité, etc.). Le rapport peut être décliné en deux types :

- › **Type 1** : seuls la revue de la conception et le test d'implémentation du dispositif de contrôle sont effectués.
- › **Type 2** : en plus de la revue de conception et du test d'implémentation du dispositif de contrôle, des tests d'efficacité opérationnelle sont effectués pour évaluer le caractère systématique du contrôle.

Les travaux ont alors pour objet, à la demande de l'entité :

De revoir le dispositif de contrôle interne relatif à ces prestations de services

- › Environnement de contrôle
- › Activités de contrôle sur les processus des prestations de services.

Évaluer la conception du dispositif de contrôle (test de Design & Implémentation).

Évaluer l'efficacité opérationnelle du dispositif de contrôles.

¹ Cette situation inclut également le cas d'un centre de services partagés (CSP) vis-à-vis des filiales du groupe (voir en ce sens la note d'information CNCC n°19)

² Les rapports ISAE 3402 concernent les contrôles qui ont un impact sur l'établissement des états financiers.

FICHE 11 AUDIT DE SERVICES EXTERNALISÉS

Les avis peuvent être assortis de plans d'actions émis par le prestataire qui visent à contribuer à l'amélioration des traitements de l'information financière et qui portent sur des éléments du contrôle interne objets de la présente mission.

Dans les Entités d'Intérêt Public, les travaux du commissaire aux comptes ne peuvent pas inclure la participation³ :

- à la conception et la mise en œuvre de procédures de contrôle interne ou de gestion des risques en rapport avec la préparation et/ou le contrôle de l'information financière ;
- à la conception et la mise en œuvre de systèmes techniques relatifs à l'information financière ;
- aux services liés à la fonction d'audit interne de l'entité contrôlée.

La prestation décrite dans le présent document est un Service autre que la certification des comptes (SACC) : il ne s'agit pas d'une mission de certification des comptes.

Dans tous les cas, le commissaire aux comptes peut refuser l'intervention.

PÉRIMÈTRE D'INVESTIGATION

La CNCC a publié une mise à jour de son guide sur les SACC en novembre 2018, précisant les normes ou doctrines auxquelles faire référence lors de la réalisation des services autres que la certification des comptes. Dans le cas des travaux évoqués ici, les prestations suivantes sont envisageables :

- des procédures convenues qui donneront lieu à des constats ;
- des travaux qui permettront d'émettre une attestation avec éventuellement des observations ;
- un examen limité qui permettra la formulation soit d'une conclusion sans observation, soit d'une conclusion avec observation(s) soit d'une impossibilité de conclure.

Pour répondre aux demandes de l'entité, le commissaire aux comptes met en œuvre les diligences nécessaires à son jugement professionnel, dans le cadre d'une obligation de moyens.

Il se réfère notamment à COBIT qui est le référentiel international de gouvernance des SI.

Les travaux du commissaire aux comptes portent sur :

- les processus en lien avec les prestations externalisées réalisées pour le compte des clients de l'entité ;
- des éléments du contrôle interne relatifs au traitement des opérations de l'entité incluant, le cas échéant, le système d'information et les traitements informatisés.

Le commissaire aux comptes utilise également sa connaissance du contexte et du tissu économique dans lesquels évolue l'entité.

RAPPORT ET DOCUMENTATION

Le commissaire aux comptes consigne dans son dossier de travail :

- le référentiel de contrôle mis en place par l'entité ;
- les preuves des contrôles testés ;
- l'analyse des forces et des faiblesses du dispositif de contrôle interne sur le périmètre de travail ;
- les plans d'actions ou les contrôles compensatoires pouvant couvrir les risques identifiés.

Le commissaire aux comptes émet un rapport avec les résultats des travaux qu'il a réalisés. Le rapport prend la forme d'un document daté et signé par le commissaire aux comptes et comporte selon les types de rapport (type 1 ou 2) :

- La lettre d'opinion de l'auditeur (Independent Service Auditor's report) ;
- La lettre du Management (Group Management Assertion) ;
- La description de l'entité et des services (type 1) ;
- La description des tests, des objectifs de contrôles et des résultats (type 2) ;
- Autres informations fournies par l'entité.

PROPOSITION D'UNE DÉMARCHÉ MÉTHODOLOGIQUE

IDENTIFICATION DES ZONES DE RISQUES

Il convient dans un premier temps d'identifier au sein de l'entité, les périmètre et critères d'évaluation qui sont inclus dans le cadre de la revue puis, dans un second temps, d'évaluer le dispositif de contrôle (conception et application).

De nombreux processus COBIT peuvent être revus. Nous avons recensé les processus COBIT les plus couramment testés :

EVALUER, DIRIGER, SURVEILLER		
EDS	EDS01	Assurer la définition et le suivi d'un référentiel de gouvernance
	EDS03	Assurer l'optimisation du risque
	EDS05	Assurer la transparence aux parties prenantes

³ Dans les entités non EIP, en vertu de loi "pacte", ces services ne sont plus interdits mais doivent faire l'objet d'une approche "risques/sauvegarde".

FICHE 11
AUDIT DE SERVICES EXTERNALISÉS

APO	ALIGNER, PLANIFIER, ORGANISER	
	APO01	Gérer le cadre de gestion des SI
	APO03	Gérer l'architecture d'entreprise
	APO06	Gérer les budgets et les coûts
	APO07	Gérer les ressources humaines
	APO08	Gérer les relations
	APO10	Gérer les fournisseurs
	APO11	Gérer la qualité
	APO12	Gérer le risque
	APO13	Gérer la sécurité

BAI	BATIR, ACQUERIR, IMPLEMENTER	
	BAI01	Gérer les programmes et les projets
	BAI02	Gérer la définition des exigences
	BAI03	Gérer l'identification et la conception des solutions
	BAI04	Gérer la disponibilité et la capacité
	BAI05	Gérer le changement organisationnel
	BAI06	Gérer les changements (SI)
	BAI07	Gérer l'acceptation du changement et de la transition
	BAI08	Gérer la connaissance
	BAI09	Gérer les actifs
BAI10	Gérer la configuration	

LSS	LIVRER, SERVIR, SOUTENIR	
	LSS01	Gérer les opérations
	LSS02	Gérer les demandes de services et les incidents
	LSS03	Gérer les problèmes
	LSS04	Gérer la continuité
	LSS05	Gérer les services de sécurité
	LSS06	Gérer les contrôles des processus métier

SEM	SURVEILLER, EVALUER, MESURER	
	SEM01	Surveiller, évaluer et mesurer la performance et la conformité
	SEM02	Surveiller, évaluer et mesurer le système de contrôle interne
	SEM03	Surveiller, évaluer et mesurer la conformité aux exigences externes

CHOIX DES TESTS À RÉALISER

Les travaux sont de différentes natures :

Revue du dispositif de contrôle interne relatif à ces prestations de services

- Environnement de contrôle (organisation, gouvernance, etc.)
- Activités de contrôle sur les processus des prestations de services.

Évaluation de la conception du dispositif de contrôle (test de Design & Implémentation) au travers d'une revue documentaire et d'un test de cheminement

Évaluation de l'efficacité opérationnelle du dispositif de contrôles au travers de tests par échantillonnage dépendant de la fréquence de réalisation du contrôle

Formalisation du rapport



GLOSSAIRE

TERME	DÉFINITION	FICHES AI**	SACC AI**	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	1	16, 96
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	1	16, 96, 97
BUREAU DYNAMIQUE	Des espaces où les salariés n'ont plus de poste de travail attribué ni d'espace personnel. On parle également de salariés « sans bureau fixe ».	1		16
Business Impact Analysis	Une analyse d'impact sur les entreprises (BIA) est un processus qui identifie et évalue les effets potentiels d'événements naturels ou provoqués par l'homme sur les opérations commerciales de l'entité.	9	9	77, 143
CAPTCHA	Test requis pour accéder à certains services sur Internet, qui consiste à saisir une courte séquence visible sur une image, afin de différencier les utilisateurs humains d'éventuels robots malveillants.		10	150
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, 3, 5 et 7	2, 5 et 6	27, 29, 31, 50, 102, 123
CDO	Pour « Chief Digital Officer ou manager de la transformation numérique ». Son rôle est de piloter et d'accélérer la transformation numérique d'une organisation.		1	96

TERME	DÉFINITION	FICHES AI	SACC AI	N° DE PAGE
CFCI	Contrôle fiscal des comptabilités informatisées	7	7	31, 64, 127, 128
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, 6 et 10	6	36, 57, 120
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		-
CIL	Correspondant Informatique et Libertés	6		56
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		15
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.	1, 2, 4 et 8	1, 6 et 8	13, 22, 23, 25, 42, 69, 71, 96, 124, 137
Conformité formelle du FEC	Le FEC doit répondre à un certain nombre de critères 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		62
CRM	Pour « Customer Relationship Management » ou Gestion de la Relation Client. 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		16
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		80
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	10	79, 81

TERME	DÉFINITION	FICHES AI	SACC AI	N° DE PAGE
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 faciliter la prise de décision.	1		17
Data center	Un data center ou centre de données, est une infrastructure composée d'un réseau d'ordinateurs et d'espaces de stockage. Cette infrastructure peut être utilisée par les entreprises pour organiser, traiter, stocker et entreposer de grandes quantités de données. Un data center est composé d'un centre de données basique qui regroupe des serveurs, des sous-systèmes de stockage, des commutateurs de réseau, des routeurs, des firewalls, et bien entendu des câbles et des racks physiques permettant d'organiser et d'interconnecter tout cet équipement informatique.	6 et 8	2	24, 56, 69, 100
Data mining	Ou fouille de données, est une technique informatique d'exploration de données à même de trouver des structures originales et des corrélations informelles entre les données. Elle permet de mieux comprendre les liens entre des phénomènes en apparence distincts, voire d'anticiper des tendances encore peu discernables. C'est pourquoi, elle est très utilisée dans la détection de fraudes.		10	149
Dématérialisation	Remplacement de formulaires imprimés, de documents matériels ou de processus utilisant du papier par des traitements numériques avec l'utilisation de fichiers et d'outils informatiques.		1	-
Digitalisation	Numérisation de documents afin de les sauvegarder sur un support informatique. Tous les types de documents peuvent être digitalisés, papiers, vidéos, photographiques ou bandes sonores.	1	1	17
DPO	Pour « Data Protection Officer ». Il s'agit généralement de l'individu en charge de la protection des données personnelles et du respect de la réglementation relative à ces données au sein d'une organisation.	6	6	53, 56, 124
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		27, 31, 35, 39, 48, 50, 63

TERME	DÉFINITION	FICHES AI	SACC AI	N° DE PAGE
Facture électronique	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		60, 62
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 doit respecter certaines normes sous peine d'amende ou de rejet de la comptabilité. Il sera bientôt à déposer en même temps que la liasse fiscale.	5 et 7	7	31, 62, 64, 127, 128, 131
FTP	Un serveur FTP (File Transfer Protocol) est un logiciel utilisé dans le transfert de fichiers entre deux ordinateurs. Il est, avec le client FTP, l'une des deux composantes d'un transfert de fichiers via le langage FTP.		10	150
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		55
Go / No go	La condition ou l'état d'opérabilité d'un composant ou d'un système : « go », se traduisant par un fonctionnement correct ; ou « no-go » comme ne fonctionnant pas correctement.		4	-
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		-
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		80
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	5	49
KEY USER	Ou super utilisateur. Dans la conduite d'un projet informatique, les super utilisateurs sont des ressources désignées dans l'organisation pour apprendre le fonctionnement du nouveau système et transférer ses connaissances aux utilisateurs finaux.		4	-
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	5	49
Logs	Journal des événements, enregistré automatiquement par un système informatique (serveur, équipement télécom...). Précieux pour le diagnostic des pannes et la détection des anomalies.	6 et 8	8	67, 68, 70, 134, 137
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		16

TERME	DÉFINITION	FICHES AI	SACC AI	N° DE PAGE
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		16
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		16
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		16
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	9	73, 74, 75, 76, 139, 143
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	7	59, 127, 128, 131
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		16
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		21
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. <ul style="list-style-type: none"> • R : Responsable, ou Réalisateur • A : Approbateur (« Accountable » en anglais). • C : Consulté • I : Informé <p>Il ne peut y avoir qu'un seul A par tâche.</p>	2 et 4		21, 23, 4, 41, 45

TERME	DÉFINITION	FICHES AI	SACC AI	N° DE PAGE
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		17
RGPD	Règlement général sur la protection des données du 27 avril 2016 (Règlement UE 2016/679).	1, 2, 4, 6 et 7	2 et 6	53, 54, 56, 65, 100, 119, 120, 121, 122, 123, 124, 125
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	9	25
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	9	25
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	1	22, 60, 96
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 « Segregation 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		23, 24, 25
TELNET	Protocole standard d'Internet autorisant les communications entre un client et un serveur. Celui-ci relie un système composé d'un clavier et d'un affichage à un interpréteur de commande. En pratique, le protocole Telnet permet à un utilisateur d'accéder à des données stockées sur Internet ou d'utiliser des applications depuis son propre ordinateur.		10	150
TLS	Protocole assurant la confidentialité des échanges entre les applications de communication et les utilisateurs sur Internet. Lorsqu'un serveur et un client communiquent, TLS s'assure qu'aucun tiers ne peut intercepter ni falsifier un message. TLS succède notamment au protocole SSL (Secure Sockets Layer).		10	150
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		15

TERME	DÉFINITION	FICHES AI	SACC AI	N° DE PAGE
Virus informatique	Un virus informatique est un automate autorépliquatif 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		68, 80
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.

** AI : Audit Informatique

FORMATIONS

- › Formation professionnelle spécialisée : **Master Systèmes d'Information de l'Entreprise Etendue à Dauphine**
- › Formation en ligne : **MOOC ANSSI** (Agence nationale de sécurité des systèmes d'information) et **MOOC CNIL, «L'Atelier RGPD»**
- › Formation CNCC (Compagnie nationale des commissaires aux comptes) : **CyberAudit - «Evaluer l'exposition aux risques cyber»**.

TRANSFORMATION NUMÉRIQUE

- › **L'Academie**, cahier 33 - Mesure globale de la performance durable
- › **La revue fiduciaire comptable**, La maturité « numérique » : signe de la performance de l'entreprise

GOVERNANCE DES SYSTÈMES D'INFORMATION

- › **AFAI** : Association Française de l'Audit et du conseil informatique
- › **COBIT 5**
- › **CIGREF** : Les référentiels de la DSI

CONTRÔLE DES ACCÈS ET CYBERSÉCURITÉ

- › **CYBERMALVEILLANCE**
- › **La Hack academy**
- › **AFAI**
- › **ANSSI** :
 - Entreprise - les bonnes pratiques
 - Particulier - formations : la Secnumacademie
- › **Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (Police nationale)**
- › **SISSE** : Service de l'information stratégique et de la sécurité économiques
- › **CERT-FR** : Centre gouvernemental de la veille, d'alerte et de réponse aux attaques informatiques
- › **CIGREF** : Association de grandes entreprises et d'administrations publiques françaises
- › **CLUSIF** : Club de la sécurité de l'information français
- › **CSOEC et CNCC** : Conseil supérieur de l'ordre des experts-comptables et Compagnie nationale des commissaires aux comptes, «10 commandements pour se prémunir de la cybercriminalité «
- › **CNCC** : CyberAudit

CONDUITE DE PROJETS

- › **Méthodologies et référentiels** :
 - PMBOK
 - PRINCE2
 - Méthodes AGILE

POUR ALLER PLUS LOIN ...

PROTECTION DES DONNÉES PERSONNELLES

- **AFAI** : Association Française de l'Audit et du conseil informatique - Modèle de maturité
- **CNIL** : Commission nationale de l'informatique et des libertés de France
 - Guide pratique de sensibilisation au RGPD
 - La sécurité des données personnelles
- **Académie des sciences et techniques comptables**, cahier 35 - Gouvernance des données personnelles et analyse d'impact

LÉGISLATION FISCALE ET SI

- **FEC : Fichiers des écritures comptables** - Extrait de l'article A 47A-1 du LPF qui détaille les dix-huit informations obligatoires fixée par l'administration.
- **Questions - réponses du groupe de travail entre l'Ordre des experts comptables et la DGFIP (direction générale des Finances publiques) 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 ?
- **ANSSI** - Signature électronique

PLAN DE CONTINUITÉ D'ACTIVITÉ

- **ANSSI** - Externalisation et sécurité des systèmes d'information : un guide pour maîtriser les risques

UTILISATION DES OUTILS D'AUDIT DES DONNÉES

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
 - Rapprochements 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-badges 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 / badges 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
- % 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
- Recalcul 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

Notre profession accompagne des entreprises de plus en plus informatisées, collectant et traitant des millions de données. Elle se doit donc d'évoluer pour conserver le contrôle des données financières analysées dans un contexte de cas de fraude en croissance permanente. Après une série de conférences sur le rôle du commissaire aux comptes dans la lutte anti- fraude organisées dès 2015, 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.



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