****

Fiche 01 [OUVERTURE SUR LA TRANSFORMATION NUMÉRIQUE 2](#_Toc496193561)

Fiche 02 [GOUVERNANCE DES SYSTÈMES D’INFORMATION 4](#_Toc496193562)

Fiche 03 [CONTRÔLE DES ACCÈS 9](#_Toc496193563)

fiche 04 [CONDUITE DE PROJETS 11](#_Toc496193564)

fiche 05 [UTILISATION DES OUTILS D’AUDIT DE DONNÉES 14](#_Toc496193565)

fiche 06 [PROTECTION DES DONNÉES PERSONNELLES 16](#_Toc496193567)

fiche 07 [LÉGISLATION FISCALE ET SI 18](#_Toc496193569)

fiche 08 [EXPLOITATION DES SYSTÈMES D’INFORMATION 21](#_Toc496193570)

fiche 09 [PLAN DE CONTINUITÉ D’ACTIVITÉ 23](#_Toc496193572)

fiche 10 [CYBERSÉCURITÉ 25](#_Toc496193573)

**FICHE 01**

OUVERTURE SUR LA TRANSFORMATION NUMÉRIQUE

**QUESTIONNAIRE**

|  |  |  |  |
| --- | --- | --- | --- |
| **Thème / Question** | **Enjeu /**  **Risque associé** | **Interlocuteur**  **concerné** | **Réponse attendue** |
| L’entreprise a-t-elle mis en place un projet de transformation numérique dans les deux dernières années ? | Continuité  d’exploitation | Le DG,  le marketing,  la DSI, la DRH, la DAF | OUI  - Mobilité  - Vente multi canal (clic and collect) |
| Est-ce que l’entreprise a étudié les opportunités en matière de marketing, de connaissance de ses clients, de création de nouveaux services, de changement de Business Model, d’amélioration des processus de production et de logistique ? | Continuité  d’exploitation | Le DG,  le marketing,  la DSI, la DRH, la DAF | OUI  - Objets connectés  - Réseaux sociaux |
| L’entreprise est-elle accompagnée dans ses projets de transformation par des experts/consultants ? | Fiabilité des données  Conformité | DG | OUI |
| Les responsables opérationnels ont-ils compris les enjeux et les contraintes du numérique ? (nouveautés, changements de 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 maitrise de l’agilité et des interactions, d’équipes; | Continuité d’activité | Le DG, la DSI,  Chief Digital Officer | OUI   * Méthodes agiles * Budget d’inves- tissement   - 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 dyna- mique  - Innovation favorisée |



|  |  |  |  |
| --- | --- | --- | --- |
| **Thème / Question** | **Enjeu /**  **Risque associé** | **Interlocuteur**  **concerné** | **Réponse attendue** |
| 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 par- cours 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 |
| 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 |

**FICHE 02**

GOUVERNANCE DES SYSTÈMES D’INFORMATION

**RÔLES & RESPONSABILITÉS**

**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 fonctionne- ment 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 |

**GOUVERNANCE DES DONNÉES**

**QUESTIONNAIRE**

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

**CONTRÔLE INTERNE DES SI**

**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 contrac- tuelles sont-elles conformes aux besoins de l’entreprise (RPO, RTO) ? | Garantie de reprise et de continuité d’activité | DSI et DAF | OUI |
| Des tests de restauration sont-ils menés ? Sur quel périmètre, avec quelles parties prenantes et avec quelle fréquence ? | Garantie de reprise et de continuité d’activité | DSI et DAF | OUI |

**COUVERTURE ET COHERENCE DU SYSTEME D’INFORMATION**

**QUESTIONNAIRE**

|  |  |  |  |
| --- | --- | --- | --- |
| **Thème / Question** | **Enjeu /**  **Risque associé** | **Interlocuteur**  **cible** | **Réponse attendue** |
| **A. Composantes du SI**  Le système d’information est-il basé sur un ERP ? | * Niveau d’intégration du système d’information * Nombre important 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 ? | 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 ? | * 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 ? | * Connaissance des applications sources et des traitements * Maitrise 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 ? | * Connaissance des applications sources et des traitements   Maitrise 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 ? | * Connaissance des applications sources et des traitements   Maitrise des risques liés aux évolutions du SI | DSI et/ou DAF | OUI |

|  |  |  |  |
| --- | --- | --- | --- |
| **C. Cohérence et évolution du SI**  Si certains processus ne sont pas couverts par le système d’information, il est envisagé de l’informatiser à court ou moyen terme | • Mise en place de contrôles automatiques et sécurisation des calculs et de l’accès aux données | DSI et/ou DAF | OUI |
| **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 aux 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 |

**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 |
| Les utilisateurs ont-ils l’interdiction de divulguer, communiquer, partager leur mot de passe ? | Accès non autorisés, fraudes | DG | OUI, règle- ment 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, régulière- ment auditées ? | Accès non autorisés, vol de données, sabotage, fraude | DSI | OUI |
| Les journaux de connexions sont-ils examinés : régulièrement ?  Les échecs de connexion sont-ils analysés ? | Détection des tentatives de piratages. | DSI | Analyses régulières, alertes automatiques |
| Existe-t-il une politique de chiffrement des données sensibles (mots de passe, supports nomades…) ? | Vol de données, accès non autorisé, fraude | DSI | Politique de chiffrement définie et respectée |
| Dans la liste des utilisateurs du SI, les comptes d’administration ont tous les droits. Comment ces comptes sont-ils supervisés ?  Leurs actions sont-elles enregistrées et surveillées ? | Accès non autorisé, fraude | DSI | Supervision des comptes d’administra- tion |
| Les fonctions de développement informatique, de tests et d’exploitation sont-elles séparées, avec du personnel différent ? | Fraude | DSI | OUI |

**FICHE 04**

CONDUITE DE PROJETS

**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 |

|  |  |  |  |
| --- | --- | --- | --- |
| La mise en production du nouveau logiciel comptable a-t-elle lieu au démarrage du nouvel exercice ou bien en cours d’exercice ? | Cut-off  Reprise des encours en cours d’exercice | Equipe projet | Démarrage si possible |
| Le DAF participe-t-il effectivement au comité de pilotage ? | 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) ? | Conformité Délai d’accès aux données sur demande du CAC. | Equipe projet DAF  Juridique | OUI |
| Phase : Cadrage  Le planning est-il réaliste ? | Retard du projet. Complexité d’un démarrage en cours d’exercice. | DAF, DSI | OUI |
| Phase : Cadrage  Un Plan d’Asurrance Qualité a-t-il été écrit et validé par les parties prenantes ? | Détection et communication des risques projet. Rôles et responsabilités des parties prenantes.  Arbitrage.  Gestion des litiges. | Equipe projet DAF  DSI | OUI |
| Phase : Spécifications  La définition des processus est-elle conforme au besoin ? | Non respect des règles de gestion, des procédures et des principes de séparation des fonctions. Non conformité | Equipe projet Utilisateurs | OUI +  demander l’accès aux spécifications fonctionnelles |
| Phase : Paramétrage   * La solution est-elle utilisée dans sa version standard ? * Sinon, quelle est la proportion de développements spécifiques ? | Non respect des règles de gestion.  Difficulté de maintenance de migration future. | DAF DSI | Proportion de customisations |
| Phase : Paramétrage   * Combien y a-t-il d’interfaces entrantes et sortantes autour de la nouvelle solution ? * Quel est le niveau d’intégration global ? | Exhaustivité et fiabilité des données : risque de déficience des mécanismes d’alimentation et de déversement des données en entrée et en sortie de la nouvelle application. | DSI  Equipe projet technique | Cartographie des interfaces |
| Phase : Tests   * Quelle est la stratégie de tests ? * Sur quel volume de données sont-ils réalisés ? * Qui a rédigé les scénarios ? | Exhaustivité  Fiabilité des données Régression fonctionnelle | Chef de projet DSI, responsable informatique | Stratégie de tests  Scénarios de tests |

|  |  |  |  |
| --- | --- | --- | --- |
| Phase : Reprise de données   * Nettoyage des données à reprendre * Transcodification des règles et référentiels comptables | Risque d’exhaustivité et d’intégrité des données reprises dans le nouveau système  Exactitude des schémas comptables, exhaustivité, auditabilité | Equipe projet DAF/DC  Equipe SI | Documentation Conservation des éléments techniques temporaires (base pivot, fichiers intermédiaires) |
| Phase : Recette  Quelle est l’organisation de la recette en termes de :   * 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   * Quelles sont les actions de communication et d’accompagnement ? * Quelle est la répartition de ces actions sur le planning projet ? | Absence de sponsor Implication insuffisante des utilisateurs.  Echec du projet Inadéquation de la solution. | DG | Démarche |
| Phase : Mise en production   * Quelle est la politique d’archivage de l’historique ? | 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  Quelle est l’organisation en place pour traiter les anomalies et répondre aux questions des utilisateurs pendant et après la mise en production (n.b. : sujet concernant également la recette et la conduite du changement) | Sécurité de l’environ- nement 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  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 |
| **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 TMA | DG, DAF | Détail de la comptabilisation des dépenses liées au projet |
| **Subventions**  Le projet fait-il l’objet d’un CIR ? | Correcte imputation des subventions | DG, DAF | En fonction de la réponse |

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

**FICHE 06**

PROTECTION DES DONNÉES

PERSONNELLES

**QUESTIONNAIRE**

|  |  |  |  |
| --- | --- | --- | --- |
| **Thématique** | **Question** | **Interlocuteurs** | **Réponse  et** **niveau de risque** |
| RGPD applicabilité | La société effectue-t-elle des traitements sur des données sensibles ou des traitements à grande échelle ? | DPO DSI | OUI |
| Gouvernance / déontologie | Les données personnelles ont été collectées de manière loyale, licite et transparente ?  L’objectif de la collecte et du traitement de la donnée est-il légitime ?  Les données sont-elles accessibles en dehors de l’Union européenne ? | DPO DSI  Directions métiers | Demande d’accord expresse sur les sites  Enquête de satisfaction  Localisation des Data Center en Union Européenne, sinon accord de respect du RGPD |
| Information | Le(s) responsable(s) des traitements ont-ils été identifiés et peuvent être sollicités en cas de demande par l’intéressé ?  La finalité du traitement, les catégories et sources de données ont-elles été portées à la connaissance de l’intéressé ?  Les droits attribués à l’intéressé lui-ont-ils été communiqués (accès, rectification, opposition, effacement, portabilité) ? | 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 reçue le consentement de son intéressé ? | DPO DSI | Demande d’accord express |
| Management | Les modalités du droit à l’information sont-elles établies et appliquées ?  Un registre des données et des traitements par finalité est formalisé et tenu à jour ?  Les responsabilités en termes de gestion des données personnelles dans l’entreprise et par les sous-traitants sont-elles établies ?  En cas d’incidents, un processus de recensement et de communication est-il prévu ? | 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. |

**FICHE 07**

LÉGISLATION FISCALE ET SI

**QUESTIONNAIRE**

QUESTIONS SUR LE CONTROLE DU SI – INDISPENSABLE

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

QUESTIONS SUR LE CONTROLE 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 |
| Existent-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 |

**FICHE 08**

EXPLOITATION DES SYSTÈMES

D’INFORMATION

**QUESTIONNAIRE**

L’audit de la fonction « exploitation des systèmes d’information » peut être réalisé en phase d’intérim.

Il faut commencer par identifier la ou les personnes en charge de l’exploitation. Dans les petites structures, les responsabilités et les tâches liées à l’exploitation des systèmes d’information sont peu ou mal définies.   
Par commodité, la personne en charge de l’exploitation est désignée “DSI” dans le questionnaire ci-dessous.

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

**FICHE 09**

PLAN DE CONTINUITÉ D’ACTIVITÉ

****

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

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

**2. Déterminer les attentes de sécurité pour tenir les objectifs**

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

**3. Identifier, analyser, évaluer et traiter les risques**

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



**4. Définir la stratégie de continuité d’activité**

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

**5. Mettre en œuvre 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 œuvre du PCA ont-elles été prévues ? | Opérationnel | DG/DSI | OUI |
| Les mesures à mettre en œuvre et les procédures associées sont-elles simples et accessibles ? | Opérationnel | DG | OUI |
| Les personnels responsables sont-ils désignés, informés et formés aux procédures prévues dans le PCA ? | Opérationnel  Réglementaire | DG | OUI |
| Les procédures de sauvegarde/récupération et moyens critiques du PCA sont-ils contrôlés périodiquement ? | Opérationnel  Réglementaire | DSI | OUI |

**FICHE 10**

CYBERSÉCURITÉ



|  |  |  |  |
| --- | --- | --- | --- |
| **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 |



|  |  |  |  |
| --- | --- | --- | --- |
| **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 |