QUESTIONNAIRES PAR ASSERTIONS CYCLE : Système d'information

Validé le 02/05/2023

Question	*Réponse*	*Commentaire*	*Risque*
1 - Risques en termes d'organisation et de responsabilité			Faible
Existe-t-il un organigramme de la fonction et de la sécurité informatique régulièrement mis à jour ? (On entend par Fonction Informatique l'ensemble des serveurs/postes/imprimantes... composant le réseau informatique On entend par Sécurité informatique les stratégies de sécurité des comptes utilisateurs, de sauvegardes, accès aux ressources depuis l'extérieur, paramétrage des pare-feu)			
Une personne a-t-elle été désignée pour piloter la ""fonction informatique"" ?			
- En interne, préciser sa place hiérarchique au sein de la société			
- En externe			
Un responsable de la sécurité informatique a-t-il été désigné ?			
- En interne, préciser sa place hiérarchique au sein de la société			
- En externe			
Dans le cas de prestataires externes, le(s) contrat(s) liant l'entité auditée au prestataire sont-ils adaptés aux besoins de l'entité ?			
Une politique de sécurité est-elle définie par l'entité et est-elle soutenue, comprise et évaluée par la direction ?			
Une charte ou politique d'entreprise sur l'utilisation du Système d'Information a-t-elle été définie ?			
La politique de sécurité est-elle régulièrement revue et mise à jour (changements technologiques, historique des incidents...) ?			
Les acteurs de la sécurité sont-ils formés de manière appropriée ?			
Le directeur administratif et financier (ou la personne occupant ces fonctions) est-il sensibilisé à la sécurité des systèmes d'information sur les données comptables et financières ?			
Un responsable a-t-il été désigné pour chaque application ? (Dans le cas d'utilisation d'applications complexes)			
Les règles de contrôle d'accès sont-elles formalisées dans un format ""tout est interdit sauf"" plutôt que ""tout est permis sauf"" ?			

QUESTIONNAIRES PAR ASSERTIONS CYCLE : Système d'information

Validé le 02/05/2023

Question	*Réponse*	*Commentaire*	*Risque*
Une personne a-t-elle été désignée pour décider de l'attribution, retrait, modifications des ressources du SI et des contrôles sont-ils effectués ?			
- pour chaque utilisateur (ou groupe) en interne ?			
- pour des tiers ?			
L'ensemble des responsables et des employés sont-ils sensibilisés aux problématiques de sécurité ?			
Existe-t-il une supervision des comptes d'administration du Système d'Information par la direction ?			
La séparation des tâches est-elle maintenue et assurée lors de la rotation des équipes, des vacances et du départ d'un personnel ?			
Le système d'information est-il basé sur un ERP ? (Le terme « ERP » est l'acronyme de « Entreprise Resource Planning » dont la traduction littérale est « Planification des ressources de l'entreprise ».)			
En cas de conduite de projets, un RACI est-il mis en place ? (L'acronyme RACI signifie : R : Responsible, A : Accountable, C : Consulted, I : Informed. Le RACI est un outil de formalisation des rôles et responsabilités pour chaque partie prenante au projet.)			
Existe-t-il des développements en interne ?			
Si oui, les fonctions de développement informatique, de tests et d'exploitation sont-elles séparées et menées par du personnel différent ?			
----------			
2 - Risques liés à la protection des données			
2.1 - Concernant les données généraiales (autres que données personnelles)			
Les données sont-elles référencées et classifiées ? (clients, fournisseurs, plan compable, etc.)			
Les données référentielles (données référencées et classifiées vues ci-dessus) apparaissent-elles sur une unique base de données ? (pas de doublon)			
Un nombre limité d'utilisateur a-t-il été défini pour créer, supprimer, mettre à jour les données référentielles (création d'un nouveau fournisseur, modification d'une fiche client, etc.) ?			
Le logiciel comptable utilisé est-il hébergé en interne			

QUESTIONNAIRES PAR ASSERTIONS CYCLE : Système d'information

Validé le 02/05/2023

Question	*Réponse*	*Commentaire*	*Risque*
?			
Si non, les conditions de mises à disposition des données sont-elles prévues contractuellement ?			
Les logiciels utilisés par l'entité auditée interdisent-ils des exports de données vers des fichiers non sécurisés (fichier excel, fichier texte...) ?			
Les études, tests sont effectués sur des données différentes que celles servant à l'exploitation de l'entité auditée ? (Important pour la garantie de l'intégrité des données)			
Existe-t-il des mesures de sécurisation des échanges de données ? (sécurité du courrier électronique, échange entre applications internes et externes			
2.2 - Concernant le traitement des données à caractère personnel (Définition : Une donnée à caractère personnel est toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement.)			
L'entité auditée s'est-elle enquérie de la réglementation européeenne sur la protection des données à caractère personnel ?			
L'entité a-t-elle engagé un processus de mise en conformité ?			
L'entité auditée sensibilise-t-elle son personnel à la nouvelle réglementation ? (Exemple : Mise en place d'une charte informatique, formations, etc…)			
L'entité auditée tient-elle une documentation destinée à prouver sa conformité au RGPD ?			
Un DPO est-il obligatoire et/ou a-t-il été désigné par l'entité auditée ? (Art. 37 RGPD - DPO = Data Protection Officer ou délégué à la protection des données personnelles / Un DPO est obligatoire lorsqu'il s'agit d'un traitement effectué par un organisme public ou une autorité public, lorsque l'entité traite de données sensibles ou lorsque l'entité traite de données à grande échelle)			
L'entité a-t-elle mis à jour sa politique de confidentialité ? (Permet de respecter les obligations d'information de l'intéressé sur le sort de ses données)			
Une politique de cookie a-t-elle été définie ? (Par exemple : En cas d'utilisation de cookies			

QUESTIONNAIRES PAR ASSERTIONS CYCLE : Système d'information

Validé le 02/05/2023

Question	*Réponse*	*Commentaire*	*Risque*
publicitaires, de mesure d'audience ou de traceur de réseaux sociaux, un bandeau est présent en page d'accueil du site et permet à l'internaut de paramétrer ces cookies)			
En cas de recours à un système de vidéo-surveillance, une information des personnes est-elle visible ?			
L'entité a-t-elle mis à jour ses contrats ?			
L'entité a-t-elle déterminé si elle était responsable de traitement, co-responsable ou sous-traitant de chaque traitement identifié ? (Art. 24, 26, 28 RGPD - Définition : Le responsable de traitement est celui qui fixe les finalités du traitement de la donnée récoltée)			
2.2.1 - En tant que responsable de traitement / co-responsable			
L'entité a-t-elle défini et/ou identifié les différentes nature de données à caractère personnel récoltées par elle ? (Exemple : Nom, prénom, adresse, image, adresse IP, données bancaires, données fiscales, données sensibles, logs, données relatives à la vie familiale)			
L'entité auditée traite-t-elle de données sensibles, de données concernant des mineurs ou effectue-t-elle un traitement à grand échelle et a-t-elle mis en place des mesures particulières de récolte de ces données ? (Art. 8,9,10 RGPD - Définition : """""""""""""""""""""à grande échelle""""""""""""""""""" : traitements « qui visent à traiter un volume considérable de données à caractère personnel au niveau régional, national ou supranational, qui peuvent affecter un nombre important de personnes concernées »)			
L'entité a-t-elle identifié les différents traitements de données à caractère personnel qu'elle utilise ?			
L'entité a-t-elle identifié la finalité de chacun de ces traitements ?			
Les données collectées sont-elles pertinentes et nécessaires au regard de la finalité du traitement ?			
Les transferts internes/externes ou les interconnexions entre les différents traitements ont-ils été repérés ? (Remarque : L'objectif étant d'éviter que les bases de données aux mêmes finalités se multiplient.)			
La base légale du traitement a-t-elle été identifiée ? (Consentement, contrat, obligation légale, intérêt légitime…)			
La preuve des consentements est-elle disponible ?			

QUESTIONNAIRES PAR ASSERTIONS CYCLE : Système d'information

Validé le 02/05/2023

Question	*Réponse*	*Commentaire*	*Risque*
Une durée de conservation des données à caractère personnel a-t-elle été définie ?			
Une procédure de suppression des données ou d'anonymisation est-elle prévue ? (Anonymisation = procédure visant à rendre inexploitable la donnée (cryptage...))			
L'entité auditée doit-elle et a-t-elle mis en place une Etude d'Impact sur la vie privée (DPIA) ? (Art.35 RGPD)			
Les droits de l'intéressé d'accès, de rectification et d'opposition lui ont-ils été communiqués et sont-ils réellement mis en place au sein de l'entité ?			
Le responsable de traitement peut-il être sollicité en cas de demande du propriétaire de la donnée récoltée ?			
Un registre des données personnelles traitées par l'entité auditée est-il tenu et régulièrement mis à jour ? (Art. 30 RGPD - NB : pas obligatoire pour entreprise de moins de 250 salariés mais fortement recommandé.)			
Les données sont-elles accessibles en dehors de l'UE ?			
Si oui, les partenaires respectent-ils le RGPD ? (RGPD = """""""""""""""""""Règlement Général sur la Protection des Données""""""""""""""""""" ou GDPR en anglais pour """""""""""""""""""General Data Protection Regulation""""""""""""""""""")			
Les violations sont-elles notifiées à la CNIL ?			
2.2.2 - En tant que sous-traitant (Art. 28 RGPD)			
L'entité auditée est-elle sous-traitante en terme de données à caractère personnel ?			
Si oui, tient-elle un registre des données sous-traitées et répond-elle aux exigences du RGPD en tant que sous-traitant ? (Conformément au RGPD, le sous-traitant doit tenir un registre des traitements qu'il effectue sur instructions du responsable du traitement)			
2.2.3 - L'entité auditée fait appel à un sous-taitant			
L'entité auditée fait-elle appel à des sous-traitants ? (Au sens du RGPD un sous-traitant est toute personne qui traite des données à caractère personnel pour le compte du responsable de traitement sur instruction documentée de ce dernier)			

QUESTIONNAIRES PAR ASSERTIONS CYCLE : Système d'information

Validé le 02/05/2023

Question	*Réponse*	*Commentaire*	*Risque*
Si oui, l'entité a-t-elle défini contractuellement les exigences en termes de protection des données avec son partenaire ? Le contrat avec le prestataire comprend-il les différentes clauses exigées par le règlement ?			
----------			
3 - Risques liés à la continuité d'activité pour l'entité auditée			
Les procédures de sauvegarde sont-elles mises en place ? (Plans de sauvegarde, délai de rétention, cryptage des données…)			
Existe-t-il un plan d'urgence approprié en matière de système d'information pour assurer la poursuite du fonctionnement de l'entité auditée en cas de sinistre ?			
Existe-t-il une copie externe à l'infrastructure pour les données critiques ? (Sauvegarde dans un espace """""""""""""""""""Cloud""""""""""""""""""" sécurisé ou autre…)			
Des tests de restauration sont-ils régulièrement effectués ?			
Les outils cloud repondent-ils aux besoins de l'entreprise en matière de procédure de sauvegarde des données ?			
Pour chaque ressource informatique mise en place (infrastructure, système d'information, ressource humaine intellectuelle), l'entreprise auditée a-t-elle défini leur degrès de criticité en observant ?			
- un niveau de service minimum,			
- un niveau d'indisponibilité minimum,			
- les ressources indispensables. (Ressources humaines et/ou matérielles)			
Dans le cadre d'un nouveau projet, l'entité auditée a-t-elle pris en compte les dépendances inhérentes au projet en termes de technologie, d'infrastructure et de période d'intégration pour son implantation au sein de l'entitée ?			
Le système d'information est-il compatible avec les évolutions de l'activité de l'entité auditée ?			
Les sécurités mises en place contre les risques de dégats des eaux, d'incendie et de vol sont-elles suffisantes ? (Contrôle d'accès (par badge par exemple), lieu du local/salle informatique, détection incendie…)			

QUESTIONNAIRES PAR ASSERTIONS CYCLE : Système d'information

Validé le 02/05/2023

Question	*Réponse*	*Commentaire*	*Risque*
Le système d'alimentation électrique permet-il d'assurer la continuité de l'activité ? (Présence d'onduleurs, de groupe électrogène ou autres)			
Les systèmes d'exploitation de l'ensemble du parc informatique (serveurs, postes...) sont-ils maintenus à jour par leurs éditeurs ?			
Les logiciels utilisés par l'entité sont-ils maintenus à jour par leurs éditeurs ?			
Des contrats sont-ils définis pour la maintenance des matériels et logiciels ? (extension de garantie, contrat de dépannage...)			
L'entité utilise-t-elle des applications spécialisées (en matière de production, gestion...) ?			
Si oui, existe-t-il un support utilisateur suffisant pour ne pas bloquer la continuité d'activité de l'entité auditée ?			
----------			
4 - Risques quant à l'exploitation informatique			
Existe-t-il un inventaire du système d'information ?			
Existe-t-il une cartographie du système d'information ? (Liens entre les différents éléments du SI)			
Les procédures d'exploitation sont-elles documentées ? (Procédure d'arrêt, démarrage, sauvegardes…)			
Les changements (Achats, Remplacements) apportés aux matériels, logiciels, systèmes d'exploitation sont-ils anticipés, contrôlés et approuvés ? (Etudier les modalités d'installation et de validation des nouveaux systèmes informatiques pour déterminer leur incidence sur le risque inhérent. L'entreprise doit avoir mis en place des procédures de gestion de projet pour permettre une mise en place sans risque d'un nouvel outil ou d'une nouvelle application.)			
Les prestations de services par des tiers sont-elles encadrées et gérées ?			
Existe-t-il une cohérence et une homogénéité des technologies utilisées par l'entité (Système d'exploitation, base de données, postes de travail, standardisation des configurations des matériels et logiciels) ? (La multiplication des technologies peut engendrer des coûts de formations, de maintenance, des			

QUESTIONNAIRES PAR ASSERTIONS CYCLE : Système d'information

Validé le 02/05/2023

Question	*Réponse*	*Commentaire*	*Risque*
problèmes d'adaptabilité entre les systèmes...)			
L'intégrité des systèmes et la confidentialité des données sont-elles préservées par une protection appropriée contre les codes informatiques non autorisés et/ou malveillants, présents : (Système Anti-virus, anti-ransomware par exemple)			
- sur les équipements de l'entreprise			
- sur les équipements personnels des utilisateurs connectés au système d'information.			
Existe-t-il un antivirus sur tous les équipements de l'entité auditée ?			
Si oui, sont-ils mis à jour ?			
Existe-t-il une politique de déploiement des mises à jour concernant :			
- les systèmes d'exploitation			
- les logiciels et/ou applications			
- les micrologiciels embarqués sur les matériels actifs (firmware) (définition """""""""matériels actifs""""""""" : tout le matériel comportant un équipement électronique chargé d'assurer la répartition des signaux entre les différentes branches d'un réseau informatique. (ex : hubs ou des switches, convertisseurs, bornes wifi...))			
Existe-t-il une gestion centralisée et remontée automatique d'alertes concernant : (Remontées par mail par exemple)			
- les antivirus			
- les systèmes de sauvegarde			
- les équipements de l'infrastructure informatique (serveurs, routeurs, parefeu...)			
Existe-t-il un filtrage d'URL pour les utilisateurs ayant accès au système d'information ? (définition """"URL""""" : de l'anglais Uniform Resource Locator, littéralement « localisateur uniforme de ressource ») c'est ce que l'on appelle l'adresse web. Filtrage rendant inaccessible des sites à caractères illicites)			
Existe-t-il des mesures de sécurisation des échanges de données ? (sécurité du courrier électronique, échange entre applications internes et externes, prise de contôle à distance) (Utilisation d'un système de cryptage, connexion VPN, SSH, utilisation d'API sécurisée, ...)			

QUESTIONNAIRES PAR ASSERTIONS CYCLE : Système d'information

Validé le 02/05/2023

Question	*Réponse*	*Commentaire*	*Risque*
Les ressources de l'entreprise accessibles en ligne par le public, font-elle l'objet de mesure de sécurité spécifiques, régulièrement auditées ? (Dans le cas ou l'entité auditée héberge des sites internet dans son infrastructure)			
Les fonctions essentielles de l'entreprise ont-elles été sécurisées pour préserver la résilience de l'entreprise en cas d'attaque ? (Mise en place de pare-feu…)			
Existe-t-il un contrôle des équipements autorisés à se connecter au système d'information ? (Intégration des équipements dans un Active Directory par un administrateur par exemple)			
Les supports amovibles font-ils l'objet d'une procédure d'autorisation, d'utilisation, de suivi et de destruction pour préserver la confidentialité des données ? (Supports amovibles : Clés USB, diques durs portables…)			
Existe-t-il une politique de sensibilisation du personnel quant à la confidentialité du travail dans les lieux publics ou moyens de transport ? (Vérification que les connexions soient en https…)			
Existe-t-il une politique de sensibilisation du personnel quant à la protection des données critiques de l'entité (ex : chiffrement) et à l'espionnage industriel ? (Cryptage des données sensibles)			
Existe-t-il des procédures liées aux incidents de sécurité et aux défauts de fonctionnement ?			
- signalement rapide des incidents de sécurité,			
- signalement de dysfonctionnements de logiciels,			
- capitalisation sur la résolution d'incidents,			
- mise en place d'un processus disciplinaire.			
Chaque année, l'endité définit-elle ses besoins en termes de système d'information et lui consacre-t-elle un budget ? (Etudier les modalités d'achat ou de développement des solutions informatiques pour déterminer leur incidence sur le risque inhérent. L'entreprise doit avoir mis en place des procédures permettant d'identifier les besoins informatiques et de mener à terme les projets d'achats ou de développement de solutions.)			
----------			
5 - Risques en matière de fraude, accès non			

QUESTIONNAIRES PAR ASSERTIONS CYCLE : Système d'information

Validé le 02/05/2023

Question	*Réponse*	*Commentaire*	*Risque*
autorisé, vol de données (conséquences d'un détournement des règles d'exploitation)			
Concernant la gestion des droits d'accès appliquée à l'ensemble du système informatique (applications, serveurs, matériels réseaux...), l'entité autidée a-t-elle défini :			
- une politique de contrôle des accès (autorisation qualitativement et quantitativement définies, étendue des droits avec autorisation spécifique, un utilisateur par identifiant),			
- une matrice de suivi des autorisations, (Organigramme des personnes habilitées à créer, modifier, supprimer des accès utilisateurs)			
- une personne en charge de la création, suppression ou blocage des droits d'accès, (En général un administrateur système, ou un délégué à l'administrateur)			
- une procédure formelle d'attribution/retrait avec informations entre les services concernés, (Comment est faite la demande d'accès pour un utilisateur à l'administrateur ou la personne déléguée (par mail, demande écrite...))			
- une politique de sensibilisation interne quant à la confidentialité, complexité et renouvellement des mots de passe,			
- une documentation de sa politique de gestion des droits d'accès. (Document indiquant pour l'ensemble des ressources les accès utilisateurs par ressource)			
L'entité auditée fait-elle appel à des ressources externes (serveur hébergé, application hébergée) :			
Si oui,			
- la gestion des accès est-elle assurée par un système de double authentification ? (Système de connexion avec Nom Utilsateur/Mot de passe + une confirmation par un code (envoyé par sms, par mail...))			
- la gestion des accès est-elle assurée par une clé d'authentification physique ? (Certificat SSL, connexion SSH…)			
Les postes de travail se verrouillent-ils automatiquement après quelques minutes d'inactivité sur le poste ? Necessitent-ils un mot de passe pour sortir de la veille ?			
Un réseau wifi est-il connecté au réseau de production ?			

QUESTIONNAIRES PAR ASSERTIONS CYCLE : Système d'information

Validé le 02/05/2023

Question	*Réponse*	*Commentaire*	*Risque*
Si oui, la méthode d'authentification respecte-t-elle la politique de contrôle des accès ?			
La connexion à Internet est-elle sécurisée par un pare feu suivi et administré ?			
Les points d'accès au système d'information font-ils l'objet d'une sécurité appropriée tels que porte avec verrou, badge d'entrée, caméra ? (Protection des locaux informatiques)			
Existe-t-il des journaux de connexions et sont-ils régulièrement examinés ?			
L'entité auditée est-elle sensibilisée aux risques de cybercriminalité ?			
- a-t-elle mis en place une cartographie des risques ?			
- a-t-elle identifié les scénarios possibles en fonction des types d'attaque ?			
- des plans d'action en cas de crise sont-ils actualisés en fonction des évolutions technologiques ou opérationnelles ?			
----------			
6 - Risques liés à la législation fiscale / conformité			
L'entité auditée est-elle dans un processus de mise en conformité avec le RGPD ?			
L'entité auditée utilise-t-elle un système de comptabilité informatisé ?			
- La dernière mise à jour du logiciel est-elle antérieure à 1 an ?			
- La conformité formelle du FEC a-t-elle été vérifiée ?			
- La concordance du FEC avec la déclaration fiscale annuelle a-t-elle été vérifiée ?			
- L'entité auditée peut-elle extraire les données opérationnelles en cas de contrôle fiscal des comptabilités informatisées ?			
- La piste d'audit peut-elle être clairement identifiée ? (cartographie et mise en lumière des liens entre les fichiers)			
La cohérence des dates (notamment date de validation, calendrier des jours fériés) peut-elle être vérifiée ?			
Une numérotation continue et chronologique des			

QUESTIONNAIRES PAR ASSERTIONS CYCLE : Système d'information

Validé le 02/05/2023

Question	*Réponse*	*Commentaire*	*Risque*
écritures comptables est-elle vérifiable ?			
La saisie des écritures fait-elle référence aux pièces justificatives ?			
L'impossibilité de modifier ou supprimer les écritures comptables est-elle effective ?			
La recherche de doublons de factures ou de paiements est-elle disponible ?			
Le délais de paiement fournisseurs/clients sont-ils respectés ?			
Les contrats des informaticiens contiennent-ils des clauses spécifiques de confidentialité et de non concurrence ?			
L'entité auditée a-t-elle conscience des enjeux liés à l'utilisation de moyens de chiffrement (certificats, signature électronique, https) ?			
L'entité auditée est-elle conforme aux exigences légales et réglementaires en matière de respect de la propriété intellectuelle ?			
Existe-t-il un archivage spécifique pour répondre aux obligations de la loi de 1990 sur les comptabilités informatisées ?			