IT understanding

XXXX

SOMMAIRE

[I. Les systèmes IT utilisés par l'entité pour le reporting financier et métiers : 3](#_Toc117066022)

[II. Compréhension des systèmes IT de l’entité : 7](#_Toc117066023)

[III. Compréhension de l’organisation IT: 10](#_Toc117066024)

[IV. Compréhension des process IT de l’entité 14](#_Toc117066025)

[V. Cybersecurity: 31](#_Toc117066026)

## Les systèmes IT utilisés par l'entité pour le reporting financier et métiers :

Les procédures d’évaluation des risques effectuées pour comprendre comment l’entité utilise l’IT dans le cadre de l’information financière (c.-à-d. compréhension des systèmes IT, de l’organisation IT et des processus IT).

|  |  |
| --- | --- |
| Procédures réalisées | |
| Entretiens | * La structure de la gouvernance IT * L'environnement IT de l'entité, y compris la manière dont IT est utilisée pour soutenir l'information financière / les processus opérationnels qui ont un impact sur l'information financière. * Les systèmes informatiques pertinents utilisés pour les opérations financières et commerciales, y compris les différentes couches de technologie qui composent le système informatique (applications, bases de données, systèmes d'exploitation et réseaux) * La manière dont les systèmes s'interfacent / transfèrent les données entre eux. * Les types données utilisés pour le traitement de l’information financière ou la mise en œuvre/le fonctionnement des contrôles automatisés * Les projets informatiques récemment mis en œuvre et les projets nouveaux ou à venir * Les mises à niveau ou les changements significatifs des couches technologiques pertinentes * L'étendue de la dépendance à l'égard des fournisseurs de services tiers * Politiques et procédures IT ; * L'évaluation par la direction des risques IT ; * L'évaluation par la direction des incidents TI au cours de la période couverte par l'audit. |
| Observations |  |
| Inspections | * Organigramme détaillée de l’IT ; * Politiques et procédures IT ; * Cartographie des risques ; * Procès-verbaux des réunions de la gouvernance et des comités informatique ; * Rapports d’audit interne relatifs aux contrôles IT |

Est-ce-que l’information utilisée dans nos procédures d’évaluation des risques est-elle utilisée pour comprendre comment l’entité utilise l’IT dans le cadre de l’information financière ?

|  |  |  |
| --- | --- | --- |
| **OUI** | **NON** | **Not selected** |

**Si OUI**:

|  |  |  |
| --- | --- | --- |
| Description de l’information | Source de l’information | Evaluation de la pertinence et de la fiabilité de l’information |
| Organigramme détaillée de l’IT | Interne | L'organigramme informatique est obtenu directement du département informatique par le DSI et partagé avec nous sans aucune modification. L'information est pertinente pour notre compréhension de : - la structure organisationnelle informatique et la ligne hiérarchique en place, et  - les rôles et responsabilités de chaque fonction informatique et du personnel informatique. Les informations sont fiables car elles sont préparées/éditées par le département informatique et approuvées par le DSI. Elles sont ensuite publiées sur l'intranet du département afin d'être accessibles à l'ensemble du personnel informatique. |
| Politiques et procédures IT | Interne | Les politiques et procédures informatiques sont obtenues directement sur l'intranet du département par le responsable informatique et nous ont été communiquées sans aucune modification.  L'information est pertinente pour notre compréhension des processus informatiques établis par le département informatique pour gérer :  - l'accès aux programmes et aux données,  - les changements applicatifs,  - l'acquisition / développement de nouveaux systèmes,  - L’exploitation informatique.  L'information est fiable car elle est préparée/éditée par le service informatique et approuvée par le DSI. Elle est ensuite publiée sur l'intranet du département afin d'être accessible à l'ensemble du personnel informatique. |
| Cartographie des risques IT | Interne | La cartographie des risques IT est obtenu directement du département par le DSI et nous est communiqué sans aucune modification.  L'information est pertinente pour notre compréhension de : - du cadre de gestion des risques informatiques établi par le département informatique, et - du mécanisme de contrôle établi par le département informatique pour suivre l'évolution des mesures de gestion des risques informatiques mises en œuvre et contrôlées par le département informatique. L'information est fiable car elle est préparée/éditée par le département informatique et approuvée par le DSI. Elles sont ensuite publiées sur l'intranet du département afin d'être accessibles à l'ensemble du personnel informatique. |
| Procès-verbaux des réunions de la gouvernance et des comités informatique | Interne | Le PV de la réunion du groupe de gouvernance et de pilotage des TI est obtenu directement du département par le DSI et nous est communiqué sans aucune modification. L'information est pertinente pour notre compréhension du canal de communication établi entre l'IT et la direction de l'entreprise pour :  - planifier et discuter de la stratégie informatique, du budget, des projets et des questions opérationnelles importantes, et  - discuter des mises à jour et du statut des projets avec les parties prenantes concernées. L'information est fiable car elle est préparée/éditée par le département informatique et approuvée par le DSI. Elles sont ensuite publiées sur l'intranet du département. |
| Rapports d’audit interne relatifs aux contrôles IT | Interne | Les rapports d'audit interne concernant les contrôles informatiques sont obtenus directement auprès du responsable de l'audit interne et nous sont communiqués sans aucune modification. L'information est pertinente pour notre compréhension de : - de la fonction d'audit interne, et  - de l'étendue et des résultats des audits informatiques réalisés au cours de la période d'audit.  Les informations sont fiables car elles sont préparées/éditées par le service d'audit interne et approuvées par le responsable de l'audit interne.  Tous les rapports d'audit interne de l'informatique, ainsi que les recommandations, ont été communiqués au DPI et au département informatique pour qu'ils en assurent le suivi. |

## Compréhension des systèmes IT de l’entité :

Les systèmes IT utilisés par l’entité dans le cadre de ses rapports financiers et de ses processus opérationnels, y compris l’objectif de chaque système informatique, le ou les processus utilisant chaque système IT, les composants utilisant le système IT, les couches technologiques qui composent chaque système IT (y compris le titre et la version), l’indication de la personnalisation et / ou les changements, l’étendue de l’externalisation et toute autre information pertinente.

|  |  |
| --- | --- |
| **ID** |  |
| **Nom du SI** |  |
| **Objectifs du SI** |  |
| **Process Métier / Module** |  |
| **Interfaçage (Flux IN/ Flux OUT)** |  |
| **Mise à jour, adaptation ou changement** |  |
| **Niveau d'externalisation** |  |
| **Type** |  |
| **Editeur** |  |
| **Integrateur** |  |
| **Etat** |  |
| **Date Mise en Production** |  |
| **Administrateur systéme** |  |
| **Administrateur métier** |  |
| **Version OS** |  |
| **Version BDD** |  |

Les Informations concernant les mises à jour ou changements important si existants :

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

**IT System Diagram (ISD) :**

**Process**

General Ledger, A/R, & A/P

**Couche Application**

**Couche**

**Base de données**

**Couche IT**

**Couche Système d’exploitation**

**Couche**

**Réseau**

## Compréhension de l’organisation IT:

Les membres clés de l’organisation IT :

|  |  |  |
| --- | --- | --- |
| Nom | Poste | Localisation |
|  |  |  |
|  |  |  |
|  |  |  |

Documenter les fonctions clés de l’organisation IT, y compris les éléments externalisés, l’utilisation de centres de services partagé et d’emplacements physiques.

**Fonctions clés de l'organisation IT :**

Le département informatique de l'entité est dirigé par [Mouna HAMROUNI / DSI ] et dispose d'un effectif de [insérer le nombre] personnes localisées à [insérer les sites].

…………………………………………………………………………………………………………………………..

Le département informatique est organisé selon les domaines fonctionnels suivants :

[Insérer dans le tableau ci-dessous les services et leurs activités principales]

|  |  |
| --- | --- |
| **Services** | **Activités principales** |
|  |  |
|  |  |
|  |  |
|  |  |

Les évolutions suivantes ont été apportées au département informatique [au cours des douze derniers mois / depuis le dernier audit] :

…………………………………………………………………………………………………………………………

**Membres clés de l’équipe de l’organisation IT :**

[Ajouter un commentaire concernant l’organisation IT au regard des bonnes pratiques et des règles de séparation des fonctions]

…………………………………………………………………………………………………………………………..

**Les éléments externalisés :**

Nous avons rencontré le [insérer le nom du Responsable IT / Titre] de la société le JJ/MM/AAAA dans le but de comprendre les activités de sous-traitance en place.

Participants à l'entretien :

- Equipe d'audit financier : xxx

- Equipe d’audit IT: xxx

- Co-CAC: xxx

La société a [nombre] fournisseur de services externalisés ;

[Indiquer dans le tableau ci-dessous le(s) fournisseur(s) de services externalisés et le(s) process supporté(s) par ce dernier]

|  |  |  |
| --- | --- | --- |
| **Fournisseur de service externalisé** | **Service externalisé** | **Process supporté** |
|  |  |  |
|  |  |  |
|  |  |  |

Si les contrôles ne sont pas correctement effectués par les prestataires de services, le risque que l'entité ne soit pas informée est couvert par :

[Exemple :

- Des contrôles mis en œuvre sur les activités du prestataire,

- Des audits du prestataire,

- La communication régulière des résultats de l'évaluation de l'efficacité des contrôles chez le prestaire via l'obtention d'un SOC (Service Organization Control) Report préparé par un auditeur indépendant,

- La supervision des niveaux de service du prestataire effectuée par l'entité.]

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

***- Inspecter les contrats de prestations IT : Vérifier le contenu (domaines d'intervention, compétences exigées, objectifs, méthode de supervision, clause d'audit),***

***- Obtenir et inspecter des preuves de la supervision des prestataires par l'entité / résultats des audits chez les prestataires.***

Nous avons obtenu le contrat de prestation de [Nom du prestataire], précisant notamment :

[Insérer ce qu’indique le contrat de prestation]

[Exemple : Périmètre d'intervention du prestataire, le niveau de service attendu (SLA), ainsi que les responsables de la prestation]

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

Dans le contrat de prestation, on doit trouver les clauses contractuelles qui ont pour objet comme indiqué dans le tableau suivant :

|  |  |
| --- | --- |
| **Objet des clauses contractuelles** | **Existant dans le contrat (Oui / Non)** |
| Documentation fonctionnelle et technique du service externalisé |  |
| Définition des SLA |  |
| Clause de confidentialité (protection des données personnelles si c’est le cas) |  |
| Clause d’audit |  |
| Présence d’un Escrow agreement (si nécessaire) |  |

[Ajouter un commentaire concernant le contrat de prestation]

…………………………………………………………………………………………………………………………..

Existe-t-il des comptes rendus des réunions régulières entre le client et le prestataire visant à évaluer le respect des termes du contrat et les éventuelles obligations de performance par le prestataire ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Existe-t-il un audit mandaté par le client auprès du prestataire ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Si oui :

Quelle est date de réalisation de l’audit mandaté par le client auprès du prestataire ?

…………………………………………………………………………………………………………………………..

Quels ont été les objectifs de l’audit réalisé ?

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

Existe-t-il un rapport de l’audit réalisé ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Existe-t-il un plan d’action en cours / finalisé / suivi par le client avec le prestataire ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Si oui, en quoi consiste ce plan d’action ?

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

[Ajouter un commentaire concernant la sous-traitance]

…………………………………………………………………………………………………………………………..

Y a-t-il des organisations de services ont été utilisées pour soutenir l’organisation informatique de l’entité ?   
OUI / NON

Si OUI ajouter le rapport SOC.

## Compréhension des process IT de l’entité

1. **L’accès aux programmes et aux données**

Notre compréhension de l’environnement du process IT qui gère l’accès aux programmes et aux données :

Nous avons rencontré le [insérer le nom du Responsable IT / Titre] de la société le JJ/MM/AAAA dans le but de comprendre les processus d'accès aux programmes et données.

Participants à l'entretien :

- Equipe d'audit financier : xxx

- Equipe d’audit IT: xxx

- Co-CAC: xxx

*- Vérifier que l'accès aux applications se fait via un identifiant unique et requiert un mot de passe.*

*- Obtenir et inspecter la procédure de gestion des accès.*

*- S'assurer de l'existence d'une liste des profils applicatifs / d'une matrice de séparation de tâches.*

*- Inspecter la politique de mot de passe définie au sein de l'entreprise et vérifier la cohérence des critères avec les meilleures pratiques.*

Existe-t-il un mécanisme d’identification unique des utilisateurs (identifiant de l’utilisateur) pour contrôler l’accès aux applications financières / métiers clés et aux bases de données sous-jacentes ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Si oui, existe-t-il une nomenclature spécifique utilisée lors de la création des identifiants afin de garantir l’unicité des comptes ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Si oui, décrire la nomenclature utilisée par application / OS / BDD.

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

Existe-t-il des comptes génériques ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Si oui, les comptes génériques sont-ils limités et justifiés ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Nous avons obtenu la procédure de gestion des accès de l’entité datée du JJ/MM/AAAA.

[Ajouter la documentation]

[Ajouter un commentaire concernant la procédure de gestion des accès de l’entité]

…………………………………………………………………………………………………………………………..

Décrire le process d’attribution des accès

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

Les accès au SI sont-ils autorisés ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Si oui, comment le risque d’accès non autorisé ou non approprié aux applications et aux bases de données sous-jacentes est couvert ?

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

Les accès du personnel sortant sont-ils révoqués ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Décrire le process de révocation des accès

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

Les accès du personnel sortant sont-ils suspendus / désactivés ? [Suspendus / Désactivés]

…………………………………………………………………………………………………………………………..

Les accès des utilisateurs sont-ils revus ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Si oui, quelle est la fréquence de revue des accès utilisateurs ? Comment est-elle réalisée ?

…………………………………………………………………………………………………………………………..

L'administration de l'application est-t-elle répartie entre les différentes équipes support ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Existe-t-il des comptes avec droits étendus ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Si oui, les comptes avec droits étendus sont-ils limités et justifiés ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Existe-t-il une politique de mot de passe chez l’entité ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Si oui :

[Ajouter la politique de mot de passe de l’entité]

[Ajouter un commentaire concernant la politique de mot de passe obtenue]

…………………………………………………………………………………………………………………………..

Le paramétrage des mots de passe chez l’entité est comme suit :

|  |  |  |
| --- | --- | --- |
| Paramètres | Bonnes pratiques  Réf. ISO/IEC 27002 : 2013 | [Nom Application] |
| Longueur minimale du mot de passe | 8 |  |
| Complexité : Au moins 3 types de caractère : Majuscule / minuscule / nombres / caractères spéciaux | ¾ |  |
| Fréquence obligatoire pour le renouvellement du mot de passe | 90 jours |  |
| Verrouillage du compte après des tentatives de connexion infructueuses | Au-delà de 3 tentatives infructueuses |  |
| Historisation des mots de passe | 6 |  |
| Renouvellement obligatoire du mot de passe d'initialisation | Activé |  |

Les collaborateurs sont-ils invités automatiquement à modifier leurs mots de passe avec les critères de complexité minimaux appliqués ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Si oui, quelle est la fréquence de modification des mots de passe ?

…………………………………………………………………………………………………………………………..

Décrire comment les membres de la société accède aux différents sites, ainsi que le process d’obtention des accès physiques aux différentes sites.

…………………………………………………………………………………………………………………………..

[Ajouter un commentaire concernant la gestion des accès aux programmes et données]

…………………………………………………………………………………………………………………………..

1. **Les changements applicatifs**

Notre compréhension de l’environnement du process IT qui gère les changements applicatifs :

Nous avons rencontré le [insérer le nom du Responsable IT / Titre] de la société le JJ/MM/AAAA dans le but de comprendre les processus de gestion des changements.

**Participants à l'entretien :**

- Equipe d'audit financier : xxx

- Equipe d’audit IT: xxx

- Co-CAC: xxx

***- Obtenir et inspecter la procédure de gestion des changements : Vérifier qu'elle est appropriée à la taille et complexité de l'environnement et des processus IT de la société.***

Existe-t-il une procédure de gestion des changements chez l’entité ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Si oui,

[Ajouter la procédure de gestion des changements]

[Ajouter un commentaire concernant la procédure de gestion des changements]

…………………………………………………………………………………………………………………………..

Comment la procédure de gestion des changements est-elle communiquée ?

[Indiquer les moyens de communications, exemple : Document écrit, intranet, etc.]

…………………………………………………………………………………………………………………………..

Existe-t-il des changements initier par le fournisseur ?

…………………………………………………………………………………………………………………………..

Si oui,

[Ajouter le processus de gestion des changements]

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

[Ajouter un commentaire concernant la gestion des changements initier par le fournisseur]

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

Quels sont les sujets couverts par la procédure de gestion des changements ?

[Exemple : Initiation des changements, autorisation des changements, tests unitaires et techniques en environnement de test, recette utilisateur et validation formelle, migration en production.]

…………………………………………………………………………………………………………………………..

Existe-t-il des changements réalisés au cours de l’exercice ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Si oui, remplir le tableau ci-dessous :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Changement** | **Nature du changement (Mineur & Majeur & Urgent)** | **Périmètre du changement** | **Process suivi pour le changement** | **Risque identifié dans le process** | **Contrôle mis en place** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

[Ajouter un commentaire concernant la gestion des changements]

…………………………………………………………………………………………………………………………..

1. **Acquisitions / développements de nouveaux systèmes**

Notre compréhension de l’environnement du process IT qui gère les acquisitions et les développements de nouveaux systèmes :

Nous avons rencontré le [insérer le nom du Responsable IT / Titre] de la société le JJ/MM/AAAA dans le but de comprendre les processus de développement de nouveaux systèmes .

**Participants à l'entretien :**

- Equipe d'audit financier : xxx

- Equipe d’audit IT: xxx

- Co-CAC: xxx

***- Obtenir et inspecter la méthodologie de développement de nouveaux systèmes.***

L’entité développe-t-elle de nouveaux systèmes ?

…………………………………………………………………………………………………………………………..

Existe-t-il une méthodologie de développement de programme chez l’entité ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Si oui,

[Décrire la méthodologie de développement de programme]

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

[Ajouter un commentaire concernant la méthodologie de développement de programme]

…………………………………………………………………………………………………………………………..

Comment est communiquée la méthodologie de développement de programme? [Ajouter moyens de communication]

…………………………………………………………………………………………………………………………..

Quels sont les sujets couverts par la méthodologie ?

[Exemple : Initiation et autorisation des projets IT / Priorisation des projets / Expression des besoins et spécifications / Test des applications / Recette utilisateur et validation formelle / Migration de l'environnement de test vers environnement de production / Réconciliation des données migrées vers les nouvelles applications.]

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

[Ajouter un commentaire concernant le développement de programme]

…………………………………………………………………………………………………………………………..

1. **Les opérations informatiques**

Notre compréhension de l’environnement du process IT qui gère les opérations informatiques :

Nous avons rencontré le [insérer le nom du Responsable IT / Titre] de la société le JJ/MM/AAAA dans le but de comprendre les traitements IT en place.

**Participants à l'entretien :**

- Equipe d'audit financier : xxx

- Equipe d’audit IT: xxx

- Co-CAC: xxx

***- Identifier les outils de supervision des traitements IT existant et leur périmètre.***

***- Obtenir et inspecter les procédures de supervision de l'exploitation IT.***

Existe-t-il des procédures de supervision de l’exploitation IT chez l’entité ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Si oui,

[Ajouter les procédures de supervision de l’exploitation IT]

[Ajouter un commentaire concernant les procédures de supervision de l’exploitation IT]

…………………………………………………………………………………………………………………………..

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Processus** | **Nature du traitement IT**  **(Calculs / Manipulation de données ou formules / Traitement automatique d’interface / Autre à préciser)** | **Description du traitement IT** | **Risque concernant le traitement IT** | **Contrôle mis en place** |
|  |  |  |  |  |
|  |  |  |  |  |

[Ajouter un commentaire concernant la supervision de l’exploitation IT]

…………………………………………………………………………………………………………………………..

* 1. **Gestion des incidents utilisateurs et des problèmes**

Nous avons rencontré le [insérer le nom du Responsable IT / Titre] de la société le JJ/MM/AAAA dans le but de comprendre le processus de gestion des incidents en place.

**Participants à l'entretien :**

- Equipe d'audit financier : xxx

- Equipe d’audit IT : xxx

- Co-CAC : xxx

***- Obtenir et inspecter les procédures de gestion des incidents et des problèmes.***

***- Obtenir et inspecter un exemple d'incident et de son suivi.***

***- Obtenir et inspecter un exemple de suivi périodique des incidents (backlog) et s'assurer qu'ils sont résolus au fil de l'eau.***

Existe-t-il des procédures de gestion des incidents chez l’entité ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Si oui,

[Ajouter les procédures de gestion des incidents]

[Ajouter un commentaire concernant les procédures de gestion des incidents]

…………………………………………………………………………………………………………………………..

Est-ce que les incidents sont tracés ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Si oui, comment les incidents sont-ils tracés ?

…………………………………………………………………………………………………………………………..

Est-ce que les incidents sont suivis ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Si oui, comment les incidents sont-ils suivis ?

…………………………………………………………………………………………………………………………..

[Ajouter un commentaire concernant la gestion des incidents]

…………………………………………………………………………………………………………………………..

Existe-t-il des procédures de gestion des problèmes chez l’entité ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Si oui, voici décrit ci-dessous les procédures de gestion des problèmes.

[Décrire les procédures de gestion des problèmes]

[Ajouter un commentaire concernant les procédures de gestion des problèmes]

…………………………………………………………………………………………………………………………..

Est-ce que les problèmes sont tracés ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Si oui, comment les problèmes sont-ils tracés ?

…………………………………………………………………………………………………………………………..

Est-ce que les problèmes sont suivis ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Si oui, comment les problèmes sont-ils suivis ?

…………………………………………………………………………………………………………………………..

Ci-dessous le tableau lié aux incidents survenus lors de l’exercice.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Ref. Incident survenu** | **Date de survenance de l’incident** | **Date de clôture de l’incident** | **Durée de l’incident** | **Nature de l’incident (Mineur / Majeur)** | **Périmètre de l’incident** | **Root cause de l’incident** | **Action corrective** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

[Ajouter un commentaire concernant les incidents survenus lors de l’exercice.]

…………………………………………………………………………………………………………………………………………………………………………..

[Ajouter un commentaire concernant l’action corrective mise en place par l’entité]

…………………………………………………………………………………………………………………………………………………………………………..

[Ajouter un commentaire concernant la fiabilité des contrôles concernée par l’incident et, le cas échéant, s’il est nécessaire de tester des contrôles supplémentaires au niveau des processus ou des contrôles informatiques généraux.]

…………………………………………………………………………………………………………………………………………………………………………..

Les incidents observés sont-ils de nature à remettre en cause la fiabilité de l’établissement des états financiers ? [Oui / Non]

…………………………………………………………………………………………………………………………………………………………………………..

[Ajouter un commentaire concernant la gestion des incidents]

…………………………………………………………………………………………………………………………………………………………………………..

Ci-dessous le tableau lié aux problèmes survenus lors de l’exercice.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Ref. Problème survenu** | **Date de survenance du problème** | **Date de clôture du problème** | **Durée du problème** | **Nature du problème (Mineur / Majeur)** | **Périmètre du problème** | **Root cause du problème** | **Action corrective** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

[Ajouter un commentaire concernant les problèmes survenus lors de l’exercice.]

…………………………………………………………………………………………………………………………………………………………………………..

[Ajouter un commentaire concernant l’action corrective mise en place par l’entité]

…………………………………………………………………………………………………………………………………………………………………………..

[Ajouter un commentaire concernant la fiabilité des contrôles concernée par le problème et, le cas échéant, s’il est nécessaire de tester des contrôles supplémentaires au niveau des processus ou des contrôles informatiques généraux.]

…………………………………………………………………………………………………………………………………………………………………………..

Les problèmes observés sont-ils de nature à remettre en cause la fiabilité de l’établissement des états financiers ? [Oui / Non]

…………………………………………………………………………………………………………………………………………………………………………..

[Ajouter un commentaire concernant la gestion des problèmes]

* 1. **Sauvegarde et restauration des données**

Nous avons rencontré le [insérer le nom du Responsable IT / Titre] de la société le JJ/MM/AAAA dans le but de comprendre les processus de sauvegarde et restauration des données.

**Participants à l'entretien :**

- Equipe d'audit financier : xxx

- Equipe d’audit IT: xxx

- Co-CAC: xxx

***- Obtenir et inspecter la stratégie de sauvegarde.***

***- Vérifier que le document définit les besoins en sauvegarde, ainsi que les périodes de rétention des données.***

***- Vérifier que les sauvegardes sont effectuées en conformité avec les besoins définis.***

***- Vérifier les mesures utilisées permettant de protéger les supports de sauvegardes sur site ou hors site.***

***- Obtenir et inspecter la procédure de restauration des données permettant de vérifier l’intégrité des sauvegardes. Vérifier qu'elle inclut des tests techniques et utilisateurs.***

***- Vérifier que la réalisation du test de restauration est au minimum annuel.***

***- Obtenir et inspecter les résultats du dernier test de restauration effectué (PV des tests techniques et PV des tests métiers / utilisateurs). Vérifier que les résultats des tests sont satisfaisants, sinon investiguer sur le plan d'actions mis en œuvre.***

Existe-t-il une stratégie de sauvegarde chez l’entité ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Si oui,

[Ajouter la stratégie de sauvegarde]

[Ajouter un commentaire concernant la stratégie de sauvegarde]

…………………………………………………………………………………………………………………………..

Quelles sont les applications concernées par les sauvegardes ?

…………………………………………………………………………………………………………………………..

Quel est la nature des données sauvegardées ?

…………………………………………………………………………………………………………………………..

Comment sont-elles sauvegardées ? (Régulièrement / En temps réel / etc)

…………………………………………………………………………………………………………………………..

Existe-t-il des supports de sauvegarde ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Si oui, les supports de sauvegarde se trouvent-ils dans des sites internes ou externes ?

…………………………………………………………………………………………………………………………..

Existe-t-il des mesures utilisées permettant de protéger les supports de sauvegardes sur site ou hors site ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Comment est couvert le risque lié à la perte / altération de données ?

[Exemple : Des tests réguliers sur le processus de restauration des données / Infrastructure de bascule / Utilisation de services virtuels ou dans le cloud / etc]

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

[Ajouter un commentaire concernant la couverture du risque lié à la perte de données.]

…………………………………………………………………………………………………………………………..

Existe-t-il une procédure de restauration des données chez l’entité ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Si oui,

[Ajouter la procédure de restauration]

[Ajouter un commentaire concernant la procédure de restauration]

…………………………………………………………………………………………………………………………..

Existe-t-il des tests de restauration ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Si oui, quelle est la fréquence de ces tests ?

…………………………………………………………………………………………………………………………..

[Ajouter un commentaire concernant les tests de restaurations si existants]

…………………………………………………………………………………………………………………………..

Est-ce qu’un incident nécessitant une restauration des données a eu lieu au cours de l’exercice ? [Oui / Non] (Si oui, expliquer si la restauration a bien fonctionné ou non.)

…………………………………………………………………………………………………………………………..

[Ajouter un commentaire concernant la sauvegarde et restauration des données]

…………………………………………………………………………………………………………………………..

* 1. **Plan de reprise d’activité**

Nous avons rencontré le [insérer le nom du Responsable IT / Titre] de la société le JJ/MM/AAAA dans le but de comprendre le plan de reprise d'activité.

**Participants à l'entretien :**

- Equipe d'audit financier : xxx

- Equipe d’audit IT : xxx

- Co-CAC : xxx

***- Obtenir et inspecter le PRA (ou description du plan de réplication des données / bascule).***

***- Obtenir et inspecter le compte rendu du test annuel du PRA (ou test du fonctionnement correct des bascules).***

Existe-t-il un plan de reprise d’activité chez l’entité ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Si oui,

[Ajouter le plan de reprise d’activité]

[Ajouter un commentaire concernant le plan de reprise d’activité]

…………………………………………………………………………………………………………………………..

Existe-t-il des mécanismes mis en place pour assurer la reprise des opérations critiques ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Si oui, en quoi consiste ces mécanismes ?

…………………………………………………………………………………………………………………………..

Est-ce qu’un incident déclenchant un plan de reprise d’activité a eu lieu au cours de l’exercice ? [Oui / Non] (Si oui, expliquer si le plan a bien fonctionné ou non.)

…………………………………………………………………………………………………………………………..

Y-a-t ’il une stratégie de benchmarking adoptée pour tester les contrôles automatisés ? OUI / NON

**Si OUI** :

Les facteurs pertinents pris en compte pour établir ou rétablir la ou les données de référence pour tester les contrôles automatisés, y compris notre approche sur l’échelonnement de nos procédures entre les périodes d’audit.  
………………………………………………………………………………………………………………………….

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

Utiliserons-nous des fonctionnalités pour regrouper les couches informatiques afin de faciliter la gestion et la documentation de nos tests des contrôles informatiques généraux, le cas échéant ? OUI / NON

## Cybersecurity:

Documenter les personnes principalement responsables et bien informées sur les questions et les risques de cybersécurité que nous avons rencontrés et les résultats des enquêtes sur la façon dont le processus d’évaluation des risques de la direction a évalué les risques de cybersécurité dans l’ensemble de l’entité, y compris les risques de cybersécurité dans les organisations de services pertinentes pour l’audit, comment ils ont analysé et évalué l’importance des risques pour l’information financière et comment ils gèrent les risques.

Les personnes responsables en sécurité de système d’information ;

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

L'entité dispose d'un [département / responsable de gestion des risques de cybersécurité] dédié.

Ses responsabilités comprennent :

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

L'entité réalise une évaluation [périodique / ponctuelle] des vulnérabilités et met en place des dispositifs visant à mitiger les éventuels risques identifiés.

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

L'entité a-t-elle réalisé une analyse de risques lié à la cybersécurité au regard des éventuels impacts sur le business et sur les états financiers ? [Oui / Non]

…………………………………………………………………………………………………………………………..

L'entité a-t-elle identifié des risques liés à la cybersécurité pouvant avoir un impact significatif sur le business ou sur les états financiers ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Si oui, le business et/ou les états financiers concerné(s) sont :

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

L’entreprise a-t-elle mis en place des dispositifs visant à mitiger les risques liés à la cybersécurité ? [Oui / Non]

…………………………………………………………………………………………………………………………..

Si oui, les dispositifs mis en place sont : [NB : supprimer les dispositifs non existant chez le client]

Documenter les résultats des demandes de renseignements visant à savoir qui dans l’entité serait au courant en temps opportun de l’application, de la base de données, des systèmes d’exploitation et/ou du réseau IT qui a fait l’objet d’un incident de cybersécurité qui pourrait avoir une incidence sur l’intégrité de l’information utilisée dans le processus d’information financière.

**Logiciels de sécurité**

L'entité installe des logiciels de sécurité pour la protéger contre les menaces provenant du web, notamment les logiciels espions, les virus et les attaques de phishing, à savoir : [Préciser]

…………………………………………………………………………………………………………………………..

L'entité utilise un réseau privé virtuel (VPN) et le cryptage des courriels pour empêcher la divulgation non autorisée d'informations : [Préciser]

…………………………………………………………………………………………………………………………..

Des projets d'amélioration de la sécurité informatique sont également en cours, tels que l'amélioration du proxy cloud d'authentification multi-facteurs pour appliquer le filtrage de contenu afin de renforcer les utilisateurs distants. Ces projets devraient permettre d'atténuer le risque lié aux cyberattaques internes et externes, y compris les menaces liées aux informations comptables internes. [Préciser]

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

**Formation, sensibilisation et communication**

Des actions de formation [obligatoires / facultatives] sont réalisées sur les sujets suivants : [Préciser]

…………………………………………………………………………………………………………………………..

Des actions de sensibilisation sont également réalisées, à savoir : [Préciser]

…………………………………………………………………………………………………………………………..

De plus, l'entité réalise des communications [ponctuelles / régulières] auprès des collaborateurs sur les sujets suivants : [Préciser]

…………………………………………………………………………………………………………………………..

**Contrôle du réseau**

L'entité utilise-t-elle des outils logiciels au sein de l'organisation pour surveiller l'accès au réseau ?

…………………………………………………………………………………………………………………………..

Si oui, les dispositifs mis en place sont : [NB : supprimer les dispositifs non existant chez le client]

[Exemple : il s'agit notamment de scanners de vulnérabilité, de renifleurs de paquets, de systèmes de détection d'intrusion (IDS), de dispositifs d'exploitation des vulnérabilités, d'outils de création de paquets et de dispositifs de surveillance des pares-feux.]

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

**Contrôle de vérification**

L'entité dispose-t-elle des contrôles qui vérifient les modifications apportées aux informations relatives aux comptes bancaires ou aux paiements des fournisseurs afin d'authentifier la validité des modifications ? (Par exemple, les membres de l'acheminement, les noms des fournisseurs, etc.).

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

Documenter les résultats de nos enquêtes sur la façon dont l’entité :

- Identifier, évalue et répond aux risques liés aux attaques perpétrées par le biais de la compromission des e-mails professionnels (BEC)escroqueries, usurpation d’identité ou hameçonnage

- Evaluer les contrôles comptables internes liée aux risques découlant des cyberfraudes (par exemple, escroqueries BEC, usurpation d’identité).

|  |  |  |
| --- | --- | --- |
| **Menaces** | **Exemple de contre-mesure** | **Réponse Client** |
| Un utilisateur a divulgué ses identifiants suite à une attaque de type « phishing » (mail, téléphone) | Les utilisateurs sont sensibilisés. |  |
| Un utilisateur ouvre un mail contenant un malware ou visite un site web contaminé | Un système antivirus est en place. |  |
| Un utilisateur connecte un media contenant un malware | Les utilisateurs sont sensibilisés et un système antivirus est en place. |  |
| Une faille de sécurité est dévoilée pour les applications utilisées | Il y a une veille sur les patchs de sécurité fournis par les éditeurs. |  |
| Un tiers ayant accès à votre système est victime d’une cyberattaque | Système de régulation des accès des tiers. |  |
| Une personne mal intentionnée a obtenu des identifiants de connexion et accède à des ressources sensibles | Logger toutes les activités sur le réseau (lieu et horaires des connexions, échec de connexion, accès aux ressources) pour détecter les activités anormales. |  |

Nous avons fait des demandes supplémentaires ? OUI / NON

D’après les résultats des demandes de renseignements, l’entité a-t-elle subi des incidents de cybersécurité au cours de la période faisant l’objet de l’audit à ce jour ou au cours de périodes antérieures qui ont une incidence sur la période en cours ? OUI / NON

SI OUI :

Ci-dessous le tableau lié aux incidents cybers survenus lors de l’exercice.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Ref. Incident cyber survenu** | **Date de survenance de l’incident cyber** | **Date de clôture de l’incident cyber** | **Durée de l’incident cyber** | **Nature de l’incident cyber (Mineur / Majeur)** | **Périmètre de l’incident cyber** | **Root cause de l’incident cyber** | **Action corrective** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**Équipe de réponse aux incidents de cybersécurité de l'entreprise**

L'entité a-t-elle mis en place une équipe de réponse aux incidents de cybersécurité dans le cadre de son programme de protection contre les cyber-intrusions.

[Ajouter un commentaire concernant l’équipe de réponse aux incidents de cybersécurité]

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………..

[Par exemple : une équipe de réponse aux incidents de cybersécurité qui surveille les menaces et/ou les violations de données en temps réel. En particulier, cette équipe identifie, évalue et prend des mesures pour atténuer les violations de données ou d'autres types de cyberintrusion non autorisée. Souvent, la direction organise ses activités de cybersécurité dans un centre des opérations de sécurité.

[Ajouter un commentaire concernant les incidents cybers survenus lors de l’exercice.]

…………………………………………………………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………………………………………………………..

[Ajouter un commentaire concernant l’action corrective mise en place par l’entité]

…………………………………………………………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………………………………………………………..

[Ajouter un commentaire concernant la fiabilité des contrôles concernée par l’incident cyber et, le cas échéant, s’il est nécessaire de tester des contrôles supplémentaires au niveau des processus ou des contrôles informatiques généraux.]

…………………………………………………………………………………………………………………………………………………………………………..

…………………………………………………………………………………………………………………………………………………………………………..

Les incidents observés sont-ils de nature à remettre en cause la fiabilité de l’établissement des états financiers ? [Oui / Non]

………………………………………………………………………………………………………………………………………………………………………