IT understanding

(MOVENPICK HOTEL GAMMARTH TUNIS)

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’équipe intervenante a réalisé un entretien en date du 13/10/2022 (cf. ABC) qui décrit la gouvernance IT. Ainsi, nous comprenons que Movenpick Gammarth comporte uniquement un intervenant IT qui est Bechir LANDOULSI (IT Manager). * 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 : l’entité utilise plusieurs applications informatiques qui interviennent pour fournir les données d’entrés dans le calcul comptable, mais, le résultat final est traité externalisé (sous-traitance) avec l’entreprise OPTIMA utilisant le logiciel SAGE PAIE pour fournir le résultat comptable final. * 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) : d’après Bechir LANDOULSI, ORACLE CLOUD est le cœur du système informatique de MOVENPICK administré par l’entreprise mère ACCOR et géré en cloud * La manière dont les systèmes s'interfacent / transfèrent les données entre eux : il n’existe aucun interfaçage automatique entre ces applications sauf pour les deux applications ORACLE CLOUD d’ACCOR et SUN de MOVENPICK qui sont autosynchronisés * Les types données utilisés pour le traitement de l’information financière ou la mise en œuvre/le fonctionnement des contrôles automatisés :il n’y a pas de contrôle automatique * Les projets informatiques récemment mis en œuvre et les projets nouveaux ou à venir : introduire le type d’authentification SSO pour toutes les applications * 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 : A la lecture de l’organigramme interne à Movenpick Gammarth (cf. Organisation chart …), nous apprenons que Bechir LANDOULSI (IT Manager) est directement rattaché au general Manager au niveau de Movenpick Gammarth et aussi attaché à Mohamed SLAMA jouant le rôle de Cluster Director of IT Tunisia du groupe Accor(cf.Tunisia IT Organisation). * Politiques et procédures IT : Movenpick Gammarth suit les politiques et les procédures décrites au niveau du groupe ACCOR qui documenté et bien détaillé(cf.Accor IMEAT-Livre des procédures et des politiques) * Cartographie des risques :D’après le document(cf.IT ESCALATION MATRIX), on obtient les procédures et démarches à suivre dans des différentes situations) * Procès-verbaux des réunions de la gouvernance et des comités informatique : toutes les équipes informatiques doivent maintenir quotidiennement des procédures de sécurité opérationnelles administratives et techniques qui sont conformes à la politique de sécurité informatique de Accor (cf. Accor General IT Security Policy, page 11) * Rapports d’audit interne relatifs aux contrôles IT : Accor insiste à mettre en place et maintenir des contrôles internes par le suivi et d’audits iternes.(cf. Accor General IT Security Policy, page 10) qui se manifeste dans le document (cf. Movenpick Hotel Gammarth IT Audit report) pour l’audit de l’année 2019 avec un score de 68,37% et un score de 73,35% pour l’année 2021 (cf. HB4I5-Movenpick-Gammarth 2021) |

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(cf. Organisation chart …),. 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 : Mr Bechir LANDOULSI IT Manager et seul responsable 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(cf. 2. Accor IMEAT - FR - Procedures Policies Book - 2021 - V1.2). et (cf. Accor General IT Security Policy) et (cf. Accor Cyber-attack Data Breach Response Plan v 1.8)  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(cf. Accor General IT Security Policy). Et aussi les étapes à suivre par ordre chronologique en cas de survenance de risque IT (cf. IT Escalation Matrix)  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 Bechir LANDOULSI IT Manager 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(cf. Movenpick Hotel Gammarth IT Audit report) pour l’année 2019 et (cf. HB4I5-Movenpick-Gammarth 2021) pour l’année 2021.  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** | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| **Nom du SI** | OPERA CLOUD v5&v9 | SUN | MATERIALS  CONTROL | SOBI | HOTIX | VINGCARD | SIMPHONY |
| **Objectifs du SI** | Permet la gestion des achats, budget, stock, comptabilité, chiffre d’affaire, règlements et immobilisations et le contrôle des autre applications dans le domaine ACCOR sur le cloud | Permet la gestion des achats, budget, stock, comptabilité, chiffre d’affaire, règlements et immobilisations | Gestion des achats | Pointage | Traitement des congès,  prets,etc | Gestion d’accès | Gestion  Des ventes |
| **Process Métier / Module** | PMS (Property Management Systems) | Comptabilité générale. | Achat | Pointage | RH | Gestion d’accès | Point de vente (POS) |
| **Interfaçage (Flux IN/ Flux OUT)** | SUN,VINGCARD,SIMPHONY POS | OPERA CLOUD |  |  |  |  |  |
| **Mise à jour, adaptation ou changement** | Obtenir le plan stratégique ou budget IT |  |  |  |  |  |  |
| **Niveau d'externalisation** | Basé sur le  cloud |  |  |  |  |  |  |
| **Type** | Logiciel | Logiciel | Logiciel | Logiciel | Logiciel | Logiciel | Logiciel + hardware |
| **Editeur** | ORACLE | HMS | OSBC | HOTIX | HOTIX | VINGCARD | ORACLE,  MICROS |
| **Integrateur** | ORACLE | HMS | OSBC | HOTIX | HOTIX | RSI | ORACLE,  MICROS |
| **Etat** | En production | En  production | En production | En production | En production | En  production | En  production |
| **Date Mise en Production** | 2010 | 2010 | 2010 | 2021 | 2021 | 2010 | 2018 |
| **Administrateur systéme** | ACCOR |  |  |  |  |  |  |
| **Administrateur métier** | N/A |  |  |  |  |  |  |
| **Version OS** | N/A | Windows Server® 2016 Standard | Windows Server® 2012 R2 x64 | Windows Server® 2012 R2 x64 | Windows Server® 2012 R2 x64 | Windows Server® 2012 R2 x64 | N/A |
| **Version BDD** | N/A | SQL Server 2016 v13.0.16000.28 | Oracle 11g | HyperFileSQL 15.0.1.48 | SQL Server 2012 v11.0.7507.2 | SQL Flat File Database | N/A |

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

D’après Bechir LANDOULSI , les mises à jour sont selon des planifications par ACCOR

Selon la politique d’ACCOR , les mise à jour des antivirus des serveurs et des ordinateurs sont hebdomadaire au minimum(chaque semaine)(cf. 2. Accor IMEAT - FR - Procedures Policies Book - 2021 - V1.2 page 187)

**IT System Diagram (ISD) :**

Comptabilité générale

Gestion d’accès

**Pointage**

**RH (paie,prêts,**

**congès)**

**Acaht**

**Process**

SUN

VINGCARD

SOBI

HOTIX

Materials

Control

**Couche Application**

SQL FLAT FILE

SQL SERVER

2016

HYPERFILE SQL

15 .0.1.48

SQL SERVER

2012

ORACLE

11g

**Couche**

**Base de données**

**Couche IT**

**Couche Système d’exploitation**

WINDOWS

SERVER 2012

WINDOWS

SERVER 2016

WINDOWS

SERVER 2012

WINDOWS

SERVER 2012

WINDOWS

SEVER 2012

LOCAL

LOCAL

LOCAL + CLOUD

LOCAL+CLOUD

LOCAL

**Couche**

**Réseau**

## Compréhension de l’organisation IT:

Les membres clés de l’organisation IT :

|  |  |  |
| --- | --- | --- |
| Nom | Poste | Localisation |
| Mohamed SLAMA | Directeur IT Tunisie | CASA ,MAROC |
| Bechir LANDOULSI | Manger IT | MOVENPICK GAMMARTH |
| Hassen CHAOUACH | General Manager MOVENPICK | MOVENPICK GAMMARTH |

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 Bechir LANDOULSI, IT Manager et responsable aux projets à réaliser au sein de Movenpick Gammarth (cf. organisation chart MOVENPICK Juin 2022)

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

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** |
| Direction informatique | -Budgétisation,planification et gestion du processus d’approbation des dépenses informatiques  -Conformité aux politiques et directives informatiques  -Management des projets IT  (cf.JD-IT Manger[Accor]) |
|  |  |
|  |  |

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

D’après Bechir LANDOULSI, il n’y a pas de changements apportés au département informatique 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]

D’après le document communiqué de la part de Bechir LANDOULSI (cf.Tunisia IT organisation), il décrit les principaux rôles de chacun membre de l’organisation IT .

**Les éléments externalisés :**

Nous avons rencontré Bechir LANDOULSI IT Manager de l’IT dans Movenpick le 18/10/2022 dans le but de comprendre les activités de sous-traitance en place.

Participants à l'entretien :

- Equipe d’audit IT: - Mohamed Riyadh EL YOUNSI (IT Audit Manager)

- Firas KAROUI (IT Audit Junior)

La société a un 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** |
| OPTIMA SARL | -La saisie des éléments variables de la paie pour les périodes préfixés(jours de présence, heures supplimentaires, congès, avances sur salaire,etc…  -La saisie et la mise à jour des éléments fixes prévus par la loi et par la société(récrutement,départ,etc…)  -traitement des salaires SIVP et stagiaire  -La saisie des divers retenues sur salaire  -La préparation de soldes de tout compte en cas de départ  -Traitement des virement bancaires  -L’édition du journal de contrôle  -L’édition des OD comptables  -L’édition des journaux de paie sous format PDF  -L’édition des fiche de paie sous forme PDF  -L’édition des ordres de virements bancaires sous forme PDF  -Traitement et édition des déclarations trimestrielles de CNSS et Assurance groupe  -Traitement et édition des déclarations de l’employeur  -édition des certificats de retenue à la source annuels | Traitement de la paie |
|  |  |  |
|  |  |  |

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 OPTIMA SARL précisant notamment que Movenpick confie à la société OPTIMA SARL a mission pour le traitement de la paie objet d’un cahier de charge fixé.

IL n’existe pas dans le contrat (cf. Contrat optima 2021) des clauses d’audits ou de contrôles

[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 | OUI |
| Définition des SLA | OUI |
| Clause de confidentialité (protection des données personnelles si c’est le cas) | OUI |
| Clause d’audit | NON |
| Présence d’un Escrow agreement (si nécessaire) | NON |

[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]

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]

NON

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

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.

On a demandé à Movenpick de nous fournir le rapport SOC d’ACCOR concernant le domaine d’ACCOR constitué principalement des application OPERA CLOUD,VINGCARD et SIMPHONY POS

## 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 l’IT Manager de Movenpick Bechir LANDOULSI le 25/10/2022 dans le but de comprendre les processus d'accès aux programmes et données.

Participants à l'entretien :

- Equipe d’audit IT: Firas KAROUI [IT Audit Associate]

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

*-SUN : accès via SSO (Windows authentification) vérifié [OK]*

*-MC : accès via login et mot de passe vérifié [OK] (cf.* *Utilisateurs MC)*

*-SOBI : accès via login et mot de passe vérifié [OK] (cf.* *SOBI-HOTIX)*

*-HOTIX : accès via login et mot de passe vérifié [OK] (cf.* *SOBI-HOTIX)*

*-OPERA CLOUD : accès via SSO (Windows authentification) vérifié [OK]*

*- Obtenir et inspecter la procédure de gestion des accès : (cf.* *2. Accor IMEAT - FR - Procedures Policies Book - 2021 - V1.2 page 187)*

*Les pc doivent être en mode de veille automatique qui sera verrouillé au bout de 15min d’inactivité*

*Les revues d’accès des utilisateurs au réseau et aux applications doivent être effectuées tous les trimestres*

*- 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 : (cf.* *2. Accor IMEAT - FR - Procedures Policies Book - 2021 - V1.2 page 190)*

Les mots de passe des applications et de l’active directory doivent être changés tous les trois mois

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]

OUI , Pour les applications SUN et ORACLE CLOUD

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]

OUI

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

OUI, …………………..

Nous avons obtenu la procédure de gestion des accès de l’entité datée du 25/10/2022.

[à fournir cf. User Profile and IT! System Access Request OSM]

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

Formulaire

Décrire le process d’attribution des accès

D’après Bechir LANDOULSI, Les accès aux programmes suit une procedure comme suit: remplissage d’un forrmulaire nommé “User Profile and IT! System Access Request OSM) qui fourni plusieurs informations sur le type d’accès , quand,quelle application, etc qui sera validé par le directeur general Mr.Hassen CHAOUACH ou la directrice RH Mme.Olfa MEDDEB, après confirmation , Bechir LANDOULSI est le seul à donner les accès aux applications.

Pour les applications MC,SOBI,HOTIX sont gérés par Bechir LANDOULSI et les intégrateurs de ces applications alors que pour les applications SUN et ORACLE CLOUD , les utilisateurs sont ajouté par ACCOR après l’envoie d’une demande d’accès par Bechir LANDOULSI à ACCOR via E-mail

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

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]

OUI

Décrire le process de révocation des accès

La revocation d’accès suit la meme démarche que la procedure d’accès en remplissant le meme formulaire (cf. User Profile and IT! System Access Request OSM) avec l’option “sortie”

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

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

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

*OUI*

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

Les revues d’accès des utilisateurs au réseau et aux applications doivent être effectuées tous les trimestres (d’après la politique d’ACCOR) (cf. 2. Accor IMEAT - FR - Procedures Policies Book - 2021 - V1.2 page 187)

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

OUI

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]

OUI

Si oui :

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

Il existe une politique de mot de passe stricte détaillée dans l’exigence 8 de la norme PCI DSS qui doit être appliquée selon la politique d’ACCOR pour les cartes de paiement (cf. Accor General IT Security Policy page 14)

Les mots de passe des applications et de l’active directory doivent être changés tous les trois mois (cf. 2. Accor IMEAT - FR - Procedures Policies Book - 2021 - V1.2 page 190)

[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]

OUI, pour les comptes utilisateurs des systèmes d’exploitations windows

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

90 jour pour l’AD et trimestrielle pour les applications du domaine ACCOR (cf. 2. Accor IMEAT - FR - Procedures Policies Book - 2021 - V1.2 page 190)

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

Les accès physiques aux sites sont garantis par les cartes VINGCARD gérés par Bechir LANDOULSI et une autre personne (à verifier) et doit etre documenté selon la politique d’ACCOR. (cf. 2. Accor IMEAT - FR - Procedures Policies Book - 2021 - V1.2 page 184)

[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 l’IT Manager Bechir LANDOULSI de la société MOVENPICK GAMMARTH le 26/10/2022 dans le but de comprendre les processus de gestion des changements.

**Participants à l'entretien :**

- Equipe d'audit financier : xxx

- Equipe d’audit IT: Firas KAROUI [IT Audit Associate]

- 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]

OUI

Si oui,

[Ajouter la procédure de gestion des changements]

Dans le périmètre PCI DSS, un processus strict de gestion des changements doit être en place, y compris une documentation et un processus d'approbation formel.(cf. Accor General IT Security Policy page 14)

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

Les changements majeurs (changement d’applications et systèmes) sont gérés par ACCOR

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

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

D’apprès l’IT Manager Bechir LANDOULSI tous les changements IT sont recommandés par ACCOR et commuiqués vie e-mail

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]

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 l’IT Manager Bechir LANDOULSI de la société MOVENPICK GAMMARTH le 25/10/2022 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: Firas KAROUI [IT Audit Associate]

- Co-CAC: xxx

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

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

OUI, d’après Bechir LANDOULSI, mais , les responsables au développement ou acquisition des nouveaux systèmes sont l’organisation mère ACCOR ou le propriétaire de l’hôtel CTKD (Equity Capital) dont MOVENPICK participe dans le coté applicatif de l’intégration de ces technologies

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

OUI

Si oui,

[Décrire la méthodologie de développement de programme]

Le processus d'adoption et d’intégrant de nouvelle technologie améliorée et des solutions pour accompagner les objectifs organisationnels se manifeste dans la compréhension de l’environnement IT et le dégagement des potentielles améliorations est la responsabilité de l’IT Coordinator ,aussi, l’IT Cluster Director a pour responsabilité de diriger la mise en œuvre des mises à niveau technologiques /améliorations ainsi que la veille à appliquer ces transformations avec efficacité.(cf. IT\_Technical\_Competency\_Framework\_2021v01 page 9)

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

D’après Bechir LANDOULSI, cette méthodologie est communiquée via des réunions de travail

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 l’IT Manager Bechir LANDOULSI de MOVENPCK GAMMARTH le 26/10/2022 dans le but de comprendre les traitements IT en place.

**Participants à l'entretien :**

- Equipe d'audit financier : xxx

- Equipe d’audit IT: Firas KAROUI [IT Audit Associate]

- 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]

D’après Bechir LANDOULSI ,il existe une supervision de l’exploitation IT chaque 3, 6 mois à une fois par un (à vérifier / documentation )

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]

OUI

Si oui,

[Ajouter les procédures de gestion des incidents] (cf. 2. Accor IMEAT - FR - Procedures Policies Book - 2021 - V1.2 page 178)

-Tous les problèmes, incidents et demandes concernant les accès utilisateurs doivent être

soumis et suivis dans l’outil de suivi d’incidents du service d’assistance. Les équipes du

service d’assistance et les responsables de système doivent surveiller les tickets ouverts

tous les jours pour garantir leur résolution rapide. Pour les hôtels où l’accès au service

d’assistance est limité à un responsable IT, un mécanisme de suivi local doit être maintenu.

-L’hôtel doit également effectuer un suivi pour s’assurer que tous les tickets sont traités en

temps voulu

-Contacter le service MyIT pour les examiner en cas de besoin (envoie par e-mail)

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

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

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

D’après Bechir LANDOULSI , Jusqu’à ce moment , il n y a pas d’incidents informatique

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]

OUI

Si oui,

[Ajouter la stratégie de sauvegarde] (cf. 2. Accor IMEAT - FR - Procedures Policies Book - 2021 - V1.2 page 191)

ET

(cf. ITSOP\_Plan de Reprise Anti-Sinistre Informatique\_V01-01 page 7)

[Ajouter un commentaire concernant la stratégie de sauvegarde]

Pour la sauvegarde en cloud, il est recommandé de mettre en œuvre la solution régionale de sauvegarde en cloud (Barracuda) et de la configurer conformément aux standards Accor..

Quelles sont les applications concernées par les sauvegardes ?

OPERA CLOUD sur BARRACUDA CLOUD

SUN,MICROS,MC, File Server sont sauvegardés sur site (cf.Applications backup checklist.xlsx)

Quel est la nature des données sauvegardées ?

En cas d'un désastre, la clé de la reprise est de disposer d'une sauvegarde intégrale (full backup / total)

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

Tous les systèmes sont sauvegardés au moins quotidiennement (cf. ITSOP\_Plan de Reprise Anti-Sinistre Informatique\_V01-01 page 7)

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

OUI

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

-Sur le cloud en utilisant Barracuda Cloud

-Sur site :

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

OUI : Les supports de sauvegarde hebdomadaires, mensuels et annuels doivent être stockés dans un lieu sécurisé hors site, à quatre (04) heures maximums de l'hôtel

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]

• Une maintenance adéquate des équipements et des supports de sauvegarde doit être assurée, y compris le cycle de vie des supports de sauvegarde, l'utilisation de supports de nettoyage, etc…

• Des supports de sauvegarde primaires et secondaires sont utilisés

[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]

OUI

Si oui,

[Ajouter la procédure de restauration]

[Ajouter un commentaire concernant la procédure de restauration]

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

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

OUI

Si oui, quelle est la fréquence de ces tests ?

• Un test de restauration des fichiers de sauvegarde de tous les systèmes critiques est effectué une fois par trimestre.

• Un test de restauration des fichiers de sauvegarde pour tous les systèmes non critiques est effectué une fois tous les six mois.

[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.)

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]

OUI

Si oui,

[Ajouter le plan de reprise d’activité]

(cf. ITSOP\_Plan de Reprise Anti-Sinistre Informatique\_V01-01)

[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]

OUI

Si oui, en quoi consiste ces mécanismes ?

(cf. ITSOP\_PMS\_Plan\_d'urgence\_V01-00)

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.)

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 ;

Bechir LANDOULSI, IT Manager et responsable en sécurité de système d’information

L'entité dispose d'un seul responsable de gestion des risques de cybersécurité dédié qui est encore Bechir LANDOULSI.

Ses responsabilités comprennent :

Contacter ACCOR en cas de survenance de risque

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

NON…………………………………………………………………………………………………………………………..

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

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]

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]

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]

Le document (cf. Accor Cyber-attack Data Breach Response Plan v 1.8) définit la procédure à suivre en cas de cyber attaque avéré ou suspecté ou perte de données détenue ou contrôlé par Accor SA ou une entité du groupe Accor

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]

Movenpick utilise des logiciels de sécurité recommandé par ACCOR (firewall Forcepoint)

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

OUI , recommandé et géré par ACCOR

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]

Recommandation ACCOR

**Formation, sensibilisation et communication**

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

Pour les cartes de crédit : E-Learning (s’inscrire et s’assurer que tous les collègues qui traitent des

informations relatives aux cartes de crédit assistent au cours annuel en ligne et

obtiennent le certificat).(cf. 2. Accor IMEAT - FR - Procedures Policies Book - 2021 - V1.2 page 177)

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

il existe des notes de sensibilisation pour la sécurité IT à la fin du formulaire « User Profile and IT systems Access Request » lors de la demande d’accès aux applications et aux sites IT

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 ?

oui

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.]

Firewall ForcePoint

**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]

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