Vincent Draghi 25/04/2020 -26/04/2020

Etudes de Cas : EXIN Information Security Management Professional based on ISO/IEC 27001

Mission pratique PA-A1

Objectif :

• Réaliser une évaluation des risques liés à la situation de traitement des données de la société Doco.

• Rédiger la partie de l'entreprise Motco de la politique de sécurité de l'information qui couvre les activités de la société Doco.

Le livrable final de cette mission est :

- A) 1 feuille de Politique de sécurité de l'information
- B) 5 menaces pertinentes liées à la situation
- C) 25 contrôles pertinents (pour chaque menace)

A) **PSSI résumée sur une seule feuille (***l'énoncé ne précise pas s'il s'agit du sommaire de la PSSI ou de réaliser une partie de la PSSI sur une seule page)*

5 Politiques de sécurité de l'information

5.1 Orientations de la direction en matière de sécurité de l'information

6 Organisation de la sécurité de l'information

6.1 Organisation interne

6.2 Appareils mobiles et télétravail

7 La sécurité des ressources humaines

7.1 Avant l'embauche

7.2 Pendant la durée du contrat

7.3 Rupture, terme ou modification du contrat de travail

8 Gestion des actifs

8.1 Responsabilités relatives aux actifs

8.2 Classification de l'information

8.3 Manipulation des supports

9 Contrôle d'accès

9.1 Exigences métier en matière de contrôle d'accès

9.2 Gestion de l'accès utilisateur

9.3 Responsabilités des utilisateurs

9.4 Contrôle de l'accès au système et aux applications

10 Cryptographie

10.1 Mesures cryptographiques

11 Sécurité physique et environnementale

11.1 Zones sécurisées

11.2 Matériels

12 Sécurité liée à l'exploitation

12.1 Procédures et responsabilités liées à l'exploitation

12.2 Protection contre les logiciels malveillants

12.3 Sauvegarde

12.4 Journalisation et surveillance 12.5 Maîtrise des logiciels en exploitation

12.6 Gestion des vulnérabilités techniques

12.7 Considérations sur l'audit du système d'information

13 Sécurité des communications

13.1 Management de la sécurité des réseaux

13.2 Transfert de l'information

14 Acquisition, développement et maintenance des systèmes d'information

14.1 Exigences de sécurité applicables aux systèmes d'information

14.2 Sécurité des processus de développement et d'assistance technique

14.3 Données de test

15 Relations avec les fournisseurs

15.1 Sécurité de l'information dans les relations avec les fournisseurs

15.2 Gestion de la prestation du service

16 Gestion des incidents liés à la sécurité de l'information

16.1 Gestion des incidents liés à la sécurité de l'information et améliorations

17 Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité

17.1 Continuité de la sécurité de l'information

17.2 Redondances

18 Conformité

18.1 Conformité aux obligations légales et réglementaires

18.2 Revue de la sécurité de l'information

B) 5 menaces pertinentes (traitement des données Doco)

Catégorie de menace	Scénario de risque	Profil	Positionnement	Nature	Moyens techniques des attaquants
Interception et espionnage	Interception des données lors des transferts	Concurrence, pirates, hacktivistes, mafias, gouvernements…	Externe	Malveillance	Moyens
Vol	Infraction et vol des	Concurrence, pirates,	Externe	Malveillance	N/A

	disques dur des serveurs de données	hacktivistes, mafias, gouvernements…			
Sabotage ou vandalisme	Modification malveillante des données clients par un employé interne	Employé (par intérêt personnel ou financier)	Interne	Malveillance	Moyens
Attaques applicatives	Malware type virus qui modifie ou supprime les données clients	Pirates	Externe	Malveillance	Importants
Pannes et interruptions applicatives	Bugs du CRM qui n'enregistre pas voire supprime les données clients	Sous-traitant	Externe	Accident	N/A

Vincent Draghi 25/04/2020 -26/04/2020

Identification du risque

Scénario de risque	Vulnérabilité	Vraisemblance (Peu vraisemblable, Vraisemblable, Très vraisemblable, Quasi Certain)	Gravité de l'impact (Mineure, Significative, Grave, Critique)	Conséquences	Acceptabilité du risque (Acceptable en l'état, Tolérable sous contrôle, Innaceptable
A. Interception des données lors des transferts	Transfert des données en clair. Faible application de la procédure d'envoi des données via le VPN	Quasi Certain	Critique	Cout important. Perte de confiance clients, défiance des actionnaires et des partenaires, risques pénales (violation RGPD…)	Innaceptable
B. Infraction et vol des disques dur des serveurs de données	Surveillance inexistante des locaux	Très vraisemblable	Critique	Cout important. Perte de confiance clients, défiance des actionnaires et des partenaires, risques pénales	Innaceptable

				(violation RGPD…)	
C. Modification malveillante des données clients par un employé interne	Pas de mise en place de règles de confidentialité	Vraisemblable	Grave	Impact sur l'intégrité des données : clauses de contrats clients truqués, données clients non fiables, informations maquillées…	Innaceptable
D. Malware type virus qui modifie ou supprime les données clients	Anti-malware Bitdefender pas à jour	Très vraisemblable	Critique	Impact sur l'intégrité et la disponibilité des données : données clients non fiables	Innaceptable
E. Bugs du CRM qui n'enregistre pas voire supprime les données clients	Peu de tests ni de recettes réalisées	Vraisemblable	Critique	Impact sur l'intégrité et la disponibilité des données : données clients non fiables	Innaceptable

Evaluation du risque

Vraisemblance	Quasi certain				**A**
	Très vraisemblable				**B, D**
	Vraisemblable			**C**	**E**
	Peu vraisemblable				
		Mineure	Significative	Grave	Critique
		Gravité			

C) 25 contrôles pertinents (pour chaque menace)

Menace visée	Clause ISO 27001	Catégorie de contrôle / Mesure	Contrôle / Mesure
Interception des données lors des transferts	A.10.1.1	Politique d'utilisation des mesures crypto-graphiques	Il convient d'élaborer et de mettre en œuvre une politique d'utilisation de mesures cryptographiques en vue de protéger l'information.
	A.13.2.1	Politiques et procédures de transfert de l'information	Des politiques, des procédures et des mesures de transfert formelles doivent être mises en place pour protéger les transferts d'information transitant par tous types d'équipements de communication.
	A.9.4.2	Sécuriser les procédures de connexion	Lorsque la politique de contrôle d'accès l'exige, l'accès aux systèmes et aux applications doit être contrôlé par une procédure de connexion sécurisée.
	A.9.3.1	Utilisation d'informations secrètes d'authentification	Les utilisateurs doivent suivre les pratiques de l'organisation pour l'utilisation des informations secrètes d'authentification.
	A.13.1.2	Sécurité des services de réseau	Pour tous les services de réseau, les mécanismes de sécurité, les niveaux de service et les exigences de gestion, doivent être identifiés et intégrés dans les accords de services de réseau, que ces services soient fournis en interne ou externalisés.

Infraction et vol des disques dur des serveurs de données	A.11.2.1	Emplacement et protection des matériels	Les matériels doivent être localisés et protégés de manière à réduire les risques liés à des menaces et des dangers environnementaux et les possibilités d'accès non autorisé.
	A.11.2.8	Matériels utilisateur laissés sans surveillance	Les utilisateurs doivent s'assurer que les matériels non surveillés sont dotés d'une protection appropriée.
	A.11.1.1	Périmètre de sécurité physique	Des périmètres de sécurité doivent être définis et utilisés pour protéger les zones contenant l'information sensible ou critique et les moyens de traitement de l'information.
	A.11.1.2	Contrôle d'accès physique	Les zones sécurisées doivent être protégées par des contrôles adéquats à l'entrée pour s'assurer que seul le personnel autorisé est admis.
	A.11.1.3	Sécurisation des bureaux, des salles et des équipements	Des mesures de sécurité physique aux bureaux, aux salles et aux équipements doivent être conçues et appliquées.
Modification malveillante des données clients par un employé interne	A.8.1.3	Utilisation correcte des actifs	Les règles d'utilisation correcte de l'information, les actifs associés à l'information et les moyens de traitement de l'information doivent être identifiés, documentés et mis en œuvre.
	A.9.1.1	Politique de contrôle d'accès	Une politique de contrôle d'accès doit être établie, documentée et revue sur la base des exigences métier et de sécurité de l'information.
	A.12.4.1	Journalisation des événements	Des journaux d'événements enregistrant les activités de l'utilisateur, les exceptions, les défaillances et les

			événements liés à la sécurité de l'information doivent être créés, tenus à jour et vérifiés régulièrement.
	A.9.4.1	Restriction d'accès à l'information	L'accès à l'information et aux fonctions d'application système doit être restreint conformément à la politique de contrôle d'accès.
	A.7.2.3	Processus disciplinaire	Un processus disciplinaire formel et connu de tous doit exister pour prendre des mesures à l'encontre des salariés ayant enfreint les règles liées à la sécurité de l'information.
Malware type virus qui modifie ou supprime les données clients	A.12.2.1	Mesures contre les logiciels malveillants	Des mesures de détection, de prévention et de récupération conjuguées à une sensibilisation des utilisateurs adaptée, doivent être mises en œuvre pour se protéger contre les logiciels malveillants.
	A.12.3.1	Sauvegarde des informations	Des copies de sauvegarde de l'information, des logiciels et des images systèmes doivent être réalisés et testés régulièrement conformément à une politique de sauvegarde convenue.
	A.12.5.1	Installation de logiciels sur des systèmes en exploitation	Des procédures doivent être mises en œuvre pour contrôler l'installation de logiciel sur des systèmes en exploitation.
	A.12.6.1	Gestion des vulnérabilités techniques	Des informations sur les vulnérabilités techniques des systèmes d'information en exploitation doivent être obtenues en temps opportun, l'exposition de l'organisation à ces vulnérabilités doit être évaluée et les mesures

			appropriées doivent être prises pour traiter le risque associé.
	A.17.2.1	Disponibilité des moyens de traitement de l'information	Des moyens de traitement de l'information doivent être mis en œuvre avec suffisamment de redondances pour répondre aux exigences de disponibilité.
Bugs du CRM qui n'enregistre pas voire supprime les données clients	A.14.2.7	Développement externalisé	L'organisation doit superviser et contrôler l'activité de développement du système externalisée.
	A.14.2.8	Test de la sécurité du système	Les tests de fonctionnalité de la sécurité doivent être réalisés pendant le développement.
	A.15.1.2	La sécurité dans les accords conclus avec les fournisseurs	Les exigences applicables liées à la sécurité de l'information doivent être établies et convenues avec chaque fournisseur pouvant accéder, traiter, stocker, communiquer ou fournir des composants de l'infrastructure informatique destinés à l'information de l'organisation.
	A.15.2.1	Surveillance et revue des services des fournisseurs	Les organisations doivent surveiller, vérifier et auditer à intervalles réguliers la prestation des services assurés par les fournisseurs.
	A.15.2.2	Gestion des changements apportés dans les services des fournisseurs	Les changements effectués dans les prestations de service des fournisseurs, comprenant le maintien et l'amélioration des politiques, procédures et mesures existant en matière de sécurité de l'information, doivent être gérés en tenant compte du caractère critique de l'information, des systèmes et des processus concernés et de la réappréciation des risques.

Vincent Draghi 25/04/2020 -26/04/2020

Mission pratique PA-A2

Objectifs :

• Clarifier la discussion sur la propriété et aborder les questions de contrôle physique et de contrôle du personnel

• Définir les menaces, les contrôles appropriés et les risques résiduels.

Le livrable final de cette mission est un rapport d'analyse de risque dans lequel vous devez :

- A) Clarifier la discussion sur la propriété : qui possède quelle partie de quoi ?
- B) Définir **5 contrôles** appropriés au niveau de détail ISO/IEC 27001 pour traiter les questions de **sécurité physique** et du **personnel**.
- C) Définir **3 menaces** à chacune des actifs suivants : **serveurs locaux, système de commande local, information client**.
- D) Définir **3 risques résiduels** après la mise en place des contrôles, en supposant qu'ils sont efficaces.

A) Propriété : qui possède quelle partie de quoi ?

Un propriétaire est identifié pour chaque actif : il est responsable et redevable.

Selon la Norme ISO 27001 (section 8.1.2, Propriété des actifs) et après identification des actifs :

Une personne ou une entité qui a accepté la responsabilité d'assurer la gestion du cycle de vie d'un actif remplit les conditions pour être désignée propriétaire de l'actif.

Il convient que le propriétaire de l'actif soit responsable de la bonne gestion de cet actif tout au long de son cycle de vie.

Il convient que le propriétaire de l'actif :

a) s'assure que les actifs sont inventoriés;

b) s'assure que les actifs sont correctement classés et protégés;

c) définisse et revoit périodiquement les classifications et les restrictions d'accès aux actifs importants, en tenant compte des politiques de contrôle d'accès applicables;

Le propriétaire identifié peut être soit une personne, soit une entité qui a accepté la responsabilité d'assurer la gestion liée au contrôle du cycle de vie global d'un actif. Le propriétaire identifié ne possède pas nécessairement de droits de propriété sur l'actif.

On peut utiliser un tableau du type RACI, classer les types de bien (support, métiers…) et attribuer un propriétaire à chaque bien (personne ou entité par exemple)

B) 5 contrôles appropriés concernant la sécurité physique et du personnel

Problématique	Clause ISO 27001	Catégorie de contrôle / Mesure	Contrôle / Mesure	Mise en place	Coût / Complexité
Sécurité physique et personnelle	A.9.1.1	Politique de contrôle d'accès	Une politique de contrôle d'accès doit être établie, documentée et revue sur la base des exigences métier et de sécurité de l'information.	Formaliser et détailler les contrôles d'accès à la fois logiques et physiques : usage de badges avec photo et puce RFID pour accéder aux locaux + Accès au compte utilisateur sur les postes de travail selon les règles GPO mises en place.	++

				Les habilitations seront en cohérence avec la politique de classification de l'information (allant de public à secret défense). Deny by default (« Tout est généralement interdit sauf autorisation expresse »), sauf pour le personnel autorisé selon les principes de besoin de connaître et d'utiliser justifiés par le besoin métier. Les droits seront revus périodiquement (tous les 3 mois) avec archivage des historiques des accès données/retirés.	
Sécurité physique et personnelle	A.9.2.2	Distribution des accès aux utilisateurs	Un processus formel de distribution des accès aux utilisateurs doit être mis en œuvre pour attribuer et retirer des droits d'accès à tous	Dresser des profils d'utilisateurs types afin de gérer plus facilement les requêtes et les revues d'accès.	++

			types d'utilisateurs sur l'ensemble des services et des systèmes.	Préciser dans les contrats de travail et les SLA, les sanctions en cas de en cas de tentative d'accès non autorisé par un salarié ou un contractant. Adapter les droits d'accès des utilisateurs qui ont changé de fonction ou de poste et la suppression ou le blocage immédiat des droits d'accès des utilisateurs qui ont quitté l'organisation	
Sécurité physique et personnelle	A.11.2.8	Matériels utilisateur laissés sans surveillance	Les utilisateurs doivent s'assurer que les matériels non surveillés sont dotés d'une protection appropriée.	Mettre en place des campagnes de sensibilisation vis-à-vis de la protection des matériels laissés sans surveillance (campagne annuelle avec des ateliers, mailing, intranet, e-learning).	+

				Mesures à appliquer : Verrouillage systématique des sessions (postes de travail et mobiles) en cas d'absence et mise en place d'un économiseur d'écran protégé par mot de passe.	
Sécurité physique et personnelle	A.11.1.3	Sécurisation des bureaux, des salles et des équipements	Des mesures de sécurité physique aux bureaux, aux salles et aux équipements doivent être conçues et appliquées.	Déplacer le rack de serveurs dans une pièce non accessible au public. Ne pas indiquer sur la porte, ni afficher qu'il s'agit de la salle des serveurs. Seul le personnel habilité sera tenu au courant. Désactiver les cartes sans-fil sur les serveurs ainsi que sur les routeurs. Mettre en place un système d'isolement type cage de faraday dans la pièce selon le budget et le besoin.	+++

				Installer des cadenas/antivols sur le matériel informatique lorsque c'est possible en priorisant les biens en terme de valeur (moniteurs, les unités centrales, le rack des serveurs…)	
Sécurité physique et personnelle	A.11.1.2	Contrôle d'accès physique	Les zones sécurisées doivent être protégées par des contrôles adéquats à l'entrée pour s'assurer que seul le personnel autorisé est admis.	Mise en place de portes blindés pour accéder à la salle des serveurs avec double authentification (code + carte d'identification). Enregistrer à l'accueil du bâtiment les heures d'arrivée et de départ avec vérification par l'hôte/l'hôtesse d'accueil de véracité du rendez-vous. Surveillance particulière des personnes exceptionnellement	+++

				présente sur le site et disposant d'une autorisation temporaire. Surveillance de l'entrée principale d'un agent de sécurité et de caméras de surveillance. Mise en place de portique avec usage de la carte d'identification avec puce type RFID ou NFC. Porter la carte d'identification avec photo autour du coup de manière visible.	

C) 3 menaces qui visent les actifs suivants : serveurs locaux, système de commande local, information client

Bien	Catégorie de menace	Scénario de risque	Profil	Positionnement	Nature	Moyens techniques des attaquants
3 Serveurs locaux	Infraction et espionnage	Mise en place d'un keylogger et d'une backdoor	Pirates, concurrents	Externe	Malveillance	Moyens
	Vol	Vol des backups et des disques durs	Pirates, concurrents	Externe	Malveillance	Moyens
	Evènements naturels	Incendie dans la salle des serveurs	Surchauffe d'un composant informatique	Interne	Accident	N/A
Système de commande	Pannes et interruptions matérielles	Coupure de courant	Défaillance du système électrique	Interne	Accident	N/A
	Pannes et interruptions applicatives	ATP	Gouvernement	Externe	Malveillance	Elevés
	Atteinte à la propriété intellectuelle	Usage d'un logiciel piraté afin de	Shadow IT	Interne	Accident	

		réaliser des économies				
Information client	Obsolescence Technologique	Messages d'erreurs fréquents du CRM qui provoque des pertes de données	DSI et le prestataire externe	Interne	Accident	N/A
	Extorsion d'information	Employé qui vient d'être licencié et fait du chantage (fuite de donnée et divulgation d'informations stratégiques)	Employé	Interne	Malveillance	Moyens
	Accidents et erreurs humaines	Ajout et modification d'informations erronées. Suppression involontaires	Employés	Interne	Accident	N/A

Identification du risque

Scénario de risque	Vulnérabilité	Vraisemblance (Peu vraisemblable, Vraisemblable, Très	Gravité de l'impact (mineure, significative, Grave, Critique)	Conséquences	Acceptabilité du risque (Acceptable en l'état, Tolérable sous

		vraisemblable, Quasi Certain)			contrôle, innaceptable
A. Mise en place d'un keylogger et d'une backdoor	Accès au bureau non protégé et mot de passe des comptes faibles	Très vraisemblable	Grave	Cout important. Perte de confiance clients, défiance des actionnaires et des partenaires, risques pénales (violation RGPD…)	Innaceptable
B. Vol des backups et des disques durs	Accès au bureau non protégé et aucun contrôle des personnes habilitées	Très vraisemblable	Critique	Cout important. Perte de confiance clients, défiance des actionnaires et des partenaires, risques pénales (violation RGPD…)	Innaceptable
C. Incendie dans la salle des serveurs	Mauvaise ventilation du rack des 3 serveurs et détecteur de fumée absent	Vraisemblable	Critique	Destruction du matériel et des données clients	Innaceptable
D. Coupure de courant	Pas de générateurs de secours ni de sondes. Pas de	Vraisemblable	Grave	Interruption de l'activité et du travail réalisé si absence de sauvegardes	Innaceptable

	plan de reprise ni de continuité.				
E. ATP (Advanced Persistent Threat)	Anti-malware pas à jour, aucune défense en profondeur (allant des compagnes de sensibilisation des salariés contre le social engineering jusqu'à l'absence de SIEM, endpoints)	Vraisemblable	Critique	Espionnage, vol des données, destruction des données et du matériel possible.	Innaceptable
F. Usage d'un logiciel piraté afin de réaliser des économies (qui contient des backdoors)	Pas de droits Admin pour installer des applications et aucune sensibilisation des employés concernant la sécurité informatique (dont le shadow it)	Très vraisemblable	Critique	Vol de données, destruction, perturbation du fonctionnement SI, coût important	Innaceptable
G. Messages d'erreurs fréquents du CRM qui provoque des	Incompatibilités entre le CRM et le système d'exploitation utilisé en	Vraisemblable	Grave	Perte de données, ralentissement de la production, retard des	Innaceptable

pertes de données	entreprise (Windows XP)			projets à réaliser, données clients non fiables	
I. Employé qui vient d'être licencié et fait du chantage (fuite de donnée et divulgation d'informations stratégiques)	Pas de contrôle RH des salariés (casier judiciaire, références profesionelles…) en entrée et en sortie	Vraisemblable	Grave	Fuite donnée, image et réputation de l'entreprise ternie, avantage stratégique des concurrents	Tolérable sous contrôle
J. Ajout et modification d'informations erronées. Suppression involontaires	Absence de supervision, de logs. Pas de système de demande de confirmation et vérification au moment de l'écriture	Vraisemblable	significative	Données non fiables, délais supplémentaires pour corriger les erreurs.	Innaceptable

Evaluation du risque

Vraisemblance	Quasi certain			**A**	
	Très vraisemblable				**B, F**
	Vraisemblable	**J**		**D, G, I**	**C, E**
	Peu vraisemblable				
		Mineure	Significative	Grave	Critique
		Gravité			

D) 3 risques résiduels après la mise en place des contrôles

Un risque résiduel est un scénario de risque subsistant après application de la stratégie de traitement du risque.

Cette évaluation repose sur la gravité et la vraisemblance du risque.

Risques traités : serveurs locaux, système de commande local, information client (voir section précédente)

Modèle : selon EBIOS RM (version 2018)

Options de traitement du risque : Réduction du risque

Risque C : Incendie dans la salle des serveurs

■ Description sommaire : Mauvaise ventilation du rack des 3 serveurs et détecteur de fumée absent

■ Vulnérabilités résiduelles susceptibles d'être exploitées par la source de risque : Panne des ventilateurs, accumulation de poussières

■ Autres causes ou facteurs aggravants (négligence, erreur, concours de circonstance, etc) : câbles non protégés qui peuvent créer un départ d'incendie, cigarette et autres combustibles

Événements redoutés concernés :

■ Événement redouté : Destruction du matériel et des données clients

Mesures de traitement du risque existantes et complémentaires :

■ Mesure : Achat de ventilateurs pour les serveurs, câblage correcte au niveau du rack + VMC

■ Mesure : Contrôle des applications qui utilisent trop de ressources systèmes et chauffent les composants

■ Mesure : Dispositif de détecteur de fumée dans la salle des serveurs conforme NF EN 14604

■ Mesure : Mise en place de sauvegardes supplémentaires sur site (hebdomadaire) sur des NAS et bandes magnétiques + Hors site via un cloud protégé et prestataire certifié PASSI et ISO 27017.

Evaluation du risque résiduel					
Gravité initiale	Critique	Vraisemblance initiale	Vraisemblable	Niveau de risque initial	
Gravité résiduelle	Grave	Vraisemblance résiduelle	Peu vraisemblable	Niveau de risque résiduel	

Gestion du risque résiduel : Contrôle annuel du détecteur de fumée et monitoring des ressources systèmes (CPU, GPU, Disques Dur avec alerte au-delà de 120°=

Risque A : Mise en place d'un keylogger et d'une backdoor

■ Description sommaire : Accès au bureau non protégé et mot de passe des comptes faibles

■ Vulnérabilités résiduelles susceptibles d'être exploitées par la source de risque : Attaque par mouvements latéraux possible après élévation de privilèges, consulter les logs des outils de sécurité du SI en corrélation avec les SIEM.

■ Autres causes ou facteurs aggravants (négligence, erreur, concours de circonstance, etc.) : Tentative de phishing (dépôt de supports amovibles type clés usb sur le parking, offert par des faux jeux-concours ou quelqu'un de malveillant…)

Événements redoutés concernés :

■ Événement redouté : Cout important. Perte de confiance clients, défiance des actionnaires et des partenaires, risques pénales (violation RGPD…)

Mesures de traitement du risque existantes et complémentaires :

■ Mesure : Mise en place d'une porte blindée avec badge numérique + boitier d'authentification par mot de passe

■ Mesure : Mise en place du verrouillage automatique de compte avec économiseur d'écran + mot de passe

■ Mesure : Politique de mot de passe avec 10 caractères dont alphanumériques + spéciaux à changer chaque mois.

■ Mesure : Paramétrer l'anti-malware pour le scan des ports USB avant de pouvoir l'exécuter.

■ Mesure : Désactiver les réseaux sans fils

Evaluation du risque résiduel					
Gravité initiale	Grave	Vraisemblance initiale	Très vraisemblable	Niveau de risque initial	
Gravité résiduelle	significative	Vraisemblance résiduelle	Peu vraisemblable	Niveau de risque résiduel	

Gestion du risque résiduel : Audit interne, tests de pénétration physique périodique, maintenance des outils de protection et d'identification.

Risque I : Employé qui vient d'être licencié et fait du chantage (fuite de donnée et divulgation d'informations stratégiques)

■ Description sommaire (dont impacts à craindre) : Fuite donnée, image et réputation de l'entreprise ternie, avantage stratégique des concurrents

■ Vulnérabilités résiduelles susceptibles d'être exploitées par la source de risque : Facteur humain difficile à prévoir, habilitations à surveiller.

■ Autres causes ou facteurs aggravants (négligence, erreur, concours de circonstance, etc.) : Facteur humain difficile à prévoir.

Événements redoutés concernés :

■ Événement redouté : Fuite donnée, image et réputation de l'entreprise ternie, avantage stratégique des concurrents

Mesures de traitement du risque existantes et complémentaires :

■ Mesure : Procédures de contrôles lors du recrutement et lors du départ

■ Mesure : Former les managers pour détecter les salariés qui sont tentés de réaliser des fuites de données

■ Mesure : Analyse régulier des alertes, logs lorsqu'il y a des tentatives d'accéder à des informations confidentielles ou lorsqu'il y a un téléchargement massif d'informations.

Evaluation du risque résiduel					
Gravité initiale	Grave	Vraisemblance initiale	Vraisemblable	Niveau de risque initial	
Gravité résiduelle	Grave	Vraisemblance résiduelle	Peu vraisemblable	Niveau de risque résiduel	

Gestion du risque résiduel : Dispositifs RH et du management pour encadrer le personnel et améliorer les conditions de travail, comprendre les blocages, améliorer la communication entre les collaborateurs.