PREMIER MINISTRE
Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Sous-direction assistance, conseil et expertise
Bureau assistance et conseil

EBIOS 2010

ETUDE DE CAS : ACCES DISTANT

Version du 20 juillet 2011

Les commentaires et suggestions sont encouragés et peuvent être adressés à l'adresse suivante (voir formulaire de recueil de commentaires en fin de guide) :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Sous-direction assistance, conseil et expertise
Bureau assistance et conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP

ebios@ssi.gouv.fr

Historique des modifications

Date	Objet de la modification	Statut
20/07/2011	Création du document	Validé

Table des matières

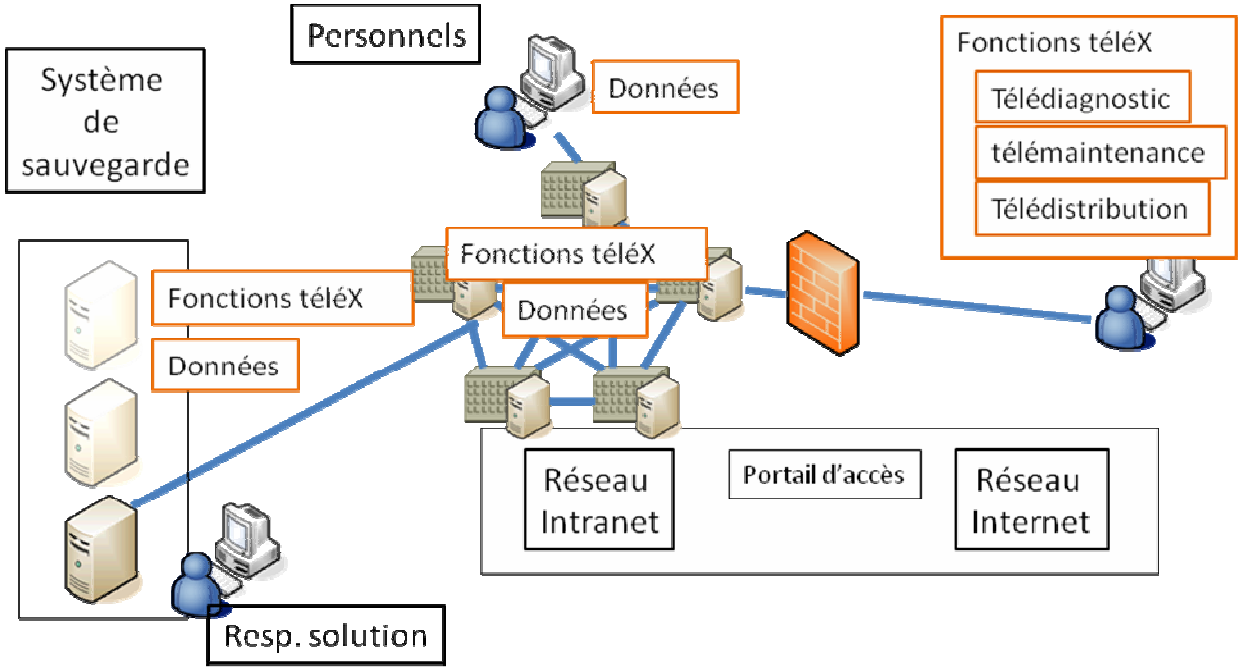
1 Module 1 – Étude du contexte

[Exploitation des éléments décrits dans le document de l'ANSSI « Externalisation des systèmes d'information »]

1.1 Activité 1.1 – Définir le cadre de la gestion des risques

Service externalisé de maintenance d'une solution de sauvegarde de données par un prestataire extérieur.

- le télédiagnostic : supervision d'équipements réseau et sécurité, diagnostic d'anomalies sur une application, etc. ;
- la télémaintenance : réalisation, après le diagnostic, des opérations à distance sur le dispositif ;
- la télédistribution : mise à jour d'une application à distance.



La définition détaillée du cadre de la gestion des risques sera faite avec le logiciel.

1.1.1 Identifier les sources de menaces

Types de sources de menaces	Retenu ou non	Exemple
Source humaine interne, malveillante, avec de faibles capacités	Non	
Source humaine interne, malveillante, avec des capacités importantes	Non	
Source humaine interne, malveillante, avec des capacités illimitées	Oui	Administrateur malveillant Technicien du centre de support malveillant
Source humaine externe, malveillante, avec de faibles capacités	Non	
Source humaine externe, malveillante, avec des capacités importantes	Oui	Pirate Concurrent
Source humaine externe, malveillante, avec des capacités illimitées	Non	
Source humaine interne, sans intention de nuire, avec de faibles capacités	Oui	Employé peu sérieux
Source humaine interne, sans intention de nuire, avec	Non	

des capacités importantes		
Source humaine interne, sans intention de nuire, avec des capacités illimitées	Oui	Administrateur peu sérieux Technicien du centre de support peu sérieux
Source humaine externe, sans intention de nuire, avec de faibles capacités	Non	
Source humaine externe, sans intention de nuire, avec des capacités importantes	Non	
Source humaine externe, sans intention de nuire, avec des capacités illimitées	Non	
Code malveillant d'origine inconnue	Non	
Phénomène naturel	Oui	Panne Faille dans l'application
Catastrophe naturelle ou sanitaire	Non	
Activité animale	Non	
Evènement interne	Non	

1.2 Activité 1.2 – Préparer les métriques

1.2.1 Action 1.2.1 – Définir les critères de sécurité et élaborer les échelles de besoins

Afin d'exprimer les besoins de sécurité, les critères de sécurité retenus sont les suivants :

Critères de sécurité	Définitions
Disponibilité	Propriété d'accessibilité au moment voulu des biens essentiels
Intégrité	Propriété d'exactitude et de complétude des biens essentiels
Confidentialité	Propriété des biens essentiels de n'être accessibles que par utilisateurs autorisés

L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes de disponibilité :

Niveau de l'échelle	Description détaillée de l'échelle
Plus de 48h	Le bien essentiel peut être indisponible plus de 48 heures
Entre 24 et 48h	Le bien essentiel doit être disponible dans les 48 heures
Entre 4 et 24h	Le bien essentiel doit être disponible dans les 24 heures
Moins de 4h	Le bien essentiel doit être disponible dans les 4 heures

L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes d'intégrité :

Niveau de l'échelle	Description détaillée de l'échelle
Détectable	Le bien essentiel peut ne pas être intègre si l'altération est identifiée
Maîtrisé	Le bien essentiel peut ne pas être intègre, si l'altération est identifiée et l'intégrité du bien essentiel retrouvée
Intègre	Le bien essentiel doit être rigoureusement intègre

L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes de confidentialité :

Niveau de l'échelle	Description détaillée de l'échelle
Public	Le bien essentiel est public
Limité	Le bien essentiel ne doit être accessible qu'au personnel et aux partenaires
Réservé	Le bien essentiel ne doit être accessible qu'au personnel interne impliqué
Privé	Le bien essentiel ne doit être accessible qu'à des personnes identifiées et ayant le besoin d'en connaître

1.2.2 Action 1.2.2 – Elaborer une échelle de niveaux de gravité

L'échelle suivante sera utilisée pour estimer la gravité des évènements redoutés et des risques.

Niveau de l'échelle	Description détaillée de l'échelle

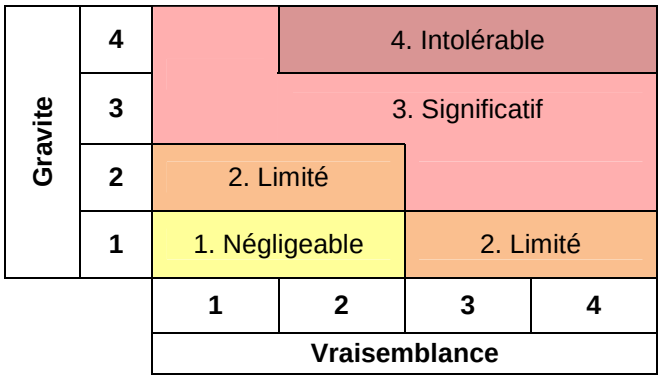
0. Insignifiant	L'évènement redouté n'est pas retenu dans le contexte de cette étude
1. Négligeable	La société surmontera les impacts sans aucune difficulté
2. Limitée	La société surmontera les impacts malgré quelques difficultés
3. Importante	La société surmontera les impacts avec de sérieuses difficultés
4. Critique	La société surmontera les impacts avec de très sérieuses difficultés et sur une très longue période

1.2.3 Action 1.2.3 – Elaborer une échelle de niveaux de vraisemblance

L'échelle suivante sera utilisée pour estimer la vraisemblance des scénarios de menaces et des risques.

Niveau de l'échelle	Description détaillée de l'échelle
1. Minime	Cela ne devrait pas se (re)produire dans les 3 ans / Besoin des privilèges d'administrateur
2. Significative	Cela pourrait se (re)produire dans les 3 ans / Besoin de connaissances et d'un accès aux utilisateurs
3. Forte	Cela devrait se (re)produire dans l'année / Sans besoin de connaissances et avec un besoin d'accès aux utilisateurs
4. Maximale	Cela va certainement se (re)produire plusieurs fois dans l'année / Sans besoin de connaissances ni d'accès aux utilisateurs

1.2.4 Echelle de niveaux de risque



1.3 Activité 1.3 – Identifier les biens

1.3.1 Biens essentiels

• Système d'information	• Données de l'entreprise
• Fonctions externalisées	• Télédiagnostic • Télémaintenance • Télédistribution

1.3.2 Biens supports

• Système de sauvegarde (SYS_SAV)	• Logiciel de sauvegarde • Serveurs de sauvegarde
• Système d'accès (SYS_ACC)	• Réseau intranet

	• Passerelle Internet (logiciel et serveur) • Réseau internet
• Système du prestataire (SYS_EXT)	• Réseau du prestataire • Postes de travail du prestataire (logiciel d'accès distant, logiciel de supervision et PC) • Passerelle Internet du prestataire (logiciel et serveur)
• Organisation interne (ORG_INT)	• Personnel de l'entreprise • Administrateurs techniques (réseau et système)
• Organisation prestataire (ORG_EXT)	• Techniciens du centre de support • Echanges avec l'entreprise

1.3.3 Liens entre les biens

Biens essentiels / Biens supports	SYS_SAV	SYS_ACC	SYS_EXT	ORG_INT	ORG_EXT
SI- Données	X	X		X	
Fonctions externalisées (télex)	X	X	X		X

1.3.4 Mesures de sécurité existantes

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
1	5.1 Politique de sécurité de l'information	5.1.1 Document de politique de sécurité de l'information	Il convient qu'un document de politique de sécurité de l'information soit approuvé par la direction, puis publié et diffusé auprès de l'ensemble des salariés et des tiers concernés.	X	X	X	ORG_INT ORG_EXT
2	6.1 Organisation interne	6.1.5 Engagement de confidentialité	Il convient d'identifier et de réexaminer régulièrement les exigences en matière d'engagements de confidentialité ou de non-divulgation, conformément aux besoins de l'organisme.	X	X		ORG_EXT
3	6.2 Tiers	6.2.3 La sécurité dans les accords conclus avec des tiers	Il convient que les accords conclus avec des tiers qui portent sur l'accès, le traitement, la communication ou la gestion de l'information, ou des moyens de traitement de l'information de l'organisme, ou qui portent sur l'ajout de produits ou de services aux moyens de traitement de l'information, couvrent l'ensemble des exigences applicables en matière de sécurité.	X	X	X	ORG_EXT
4	10.2 Gestion de la prestation de service par un tiers	10.2.2 Surveillance et réexamen des services tiers	Il convient que les services, rapports et enregistrements fournis par les tiers soient régulièrement contrôlés et réexaminés, et que des audits soient régulièrement réalisés.		X		ORG_EXT
5	10.3 Planification et acceptation du système	10.3.1 Dimensionnement	Il convient de surveiller et d'ajuster au plus près l'utilisation des ressources et il convient de faire des projections sur les dimensionnements futurs pour assurer les performances requises pour le système.	X			SYS_ACC SYS_EXT
5	10.4 Protection contre les codes	10.4.1 Mesures contre les codes	Il convient de mettre en œuvre des mesures de détection, de prévention et de récupération pour se protéger des	X	X	X	SYS_EXT

	malveillants	malveillants	codes malveillants ainsi que des procédures appropriées de sensibilisation des utilisateurs.				
7	10.5 Sauvegarde	10.5.1 Sauvegarde des informations	Il convient de réaliser des copies de sauvegarde des informations et logiciels et de les soumettre régulièrement à essai conformément à la politique de sauvegarde convenue.	X	X	X	SYS_SAV SYS_EXT
8	10.6 Gestion de la sécurité des réseaux	10.6.2Sécurité de services réseaux	Pour tous les services réseau, il convient d'identifier les fonctions réseau, les niveaux de service et les exigences de gestion, et de les intégrer dans tout accord sur les services réseau, qu'ils soient fournis en interne ou en externe.	X	X		SYS_ACC ORG_EXT
9	14.1 Aspects de la sécurité de l'information en matière de gestion de la continuité d'activité	14.1.3 Elaboration et mise en œuvre des plans de continuité intégrant la sécurité de l'information	Il convient d'élaborer et de mettre en oeuvre des plans destinés à maintenir ou à restaurer l'exploitation et à assurer la disponibilité des informations au niveau et dans les délais requis suite à une interruption ou une panne affectant les processus métier cruciaux.			X	SYS_SAV SYS_ACC
10	14.1 Aspects de la sécurité de l'information en matière de gestion de l'activité	Plan de continuité de l'activité du prestataire	Le prestataire doit fournir les garanties de continuité de l'activité au travers d'un plan de continuité de l'activité. Ce PCA doit prendre en compte les exigences en matière de sécurité de l'information, les évènements pouvant être à l'origine d'interruption des processus métier, les mesures de restauration et de maintien de la disponibilité du système d'information, ainsi que la mise à l'essai dudit plan de continuité de l'activité.	x		x	SYS_EXT ORG_EXT
11	15.2 Conformité avec les politiques et normes de sécurité et conformité technique	15.2.2 vérification de la conformité technique	Il convient de vérifier régulièrement la conformité des systèmes d'information avec les normes relatives à la mise en œuvre de la sécurité.			X	ORG_EXT

2 Module 2 – Étude des évènements redoutés

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Données de l'entreprise					
ER1	Divulgation des données de l'entreprise	Privé	• Pirate • Concurrent • Technicien du centre de support	• Perte de notoriété • Perte d'avance concurrentielle • Action en justice à l'encontre de la société	4. Critique
ER2	Altération des données de l'entreprise	Intègre	• Pirate • Concurrent • Technicien du centre de support	• Perte de crédibilité • Dépenses imprévues • Perte de mémoire de l'entreprise ou de savoir-faire • Perte de confiance vis-à-vis des collaborateurs internes • Impossibilité de remplir les obligations légales	3. Importante
ER3	Indisponibilités des données de l'entreprise	Entre 4h et 24h	• Pirate • Concurrent • Administrateur	• Impossibilité d'assurer ou de fournir un service • Perte de confiance vis-à-vis des collaborateurs internes	2. Limitée
Fonction Téléx					
ER4	Compromission de la fonction Téléx	Privée	• Technicien du centre de support	• Mise en péril du système d'information • Perte de confiance vis-à-vis des clients • Impossibilité d'assurer ou de fournir un des services de la fonction Téléx	3. Importante
ER5	Altération de la fonction Téléx	Intègre	• Technicien du centre de support	• Perte de données • Impossibilité d'assurer ou de fournir un des services de la fonction Téléx • Mise en péril du système d'information	3. Importante
ER6	Indisponibilités de la fonction Téléx	Moins de 4 heures	• Technicien du centre de support • Panne	• Perte de données • Impossibilité d'assurer ou de fournir un service	2. Limitée

L'importance relative des évènements redoutés précédemment analysés est évaluée à l'aide du tableau suivant :

Gravité	Evénements redoutés
4. Critique	• ER1 : Divulgation des données de l'entreprise
3. Importante	• ER2 : Altération des données de l'entreprise • ER4 : Compromission de la fonction Téléx • ER5 : Altération de la fonction Téléx
2. Limitée	• ER3 : Indisponibilités des données de l'entreprise • ER6 : Indisponibilités de la fonction Téléx
1. Négligeable	• /
0. Insignifiant	• /

3 Module 3 – Étude des scénarios de menaces

3.1 Organisation Interne (ORG_INT)

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Organisation Interne (ORG_INT)	Menace sur l'organisation interne causant une indisponibilité	D	• Administrateur technique interne	• M21. PER-DEP (D, I) Surcharge des capacités d'une personne	• Surcharge des activités • Mauvaise utilisation des compétences • Manque de formation du personnel interne	3. Forte
	Menace sur l'organisation interne causant une altération	I	• Technicien du centre de support	• M21. PER-DEP (D, I) Surcharge des capacités d'une personne	• Perturbation des conditions de travail • Mauvaise utilisation des compétences • Manque de formation du personnel interne	3. Forte
	Menace sur l'organisation interne causant une compromission	C	• Administrateur	• M24. PER-PTE (D, C) Départ d'une personne	• Départ d'une personne	2. Significative

Menace	Vulnérabilités	Pré-requis	Vraisemblance
Surcharge des activités	• Ressources insuffisantes pour réaliser les activités	• Ressources allouées par le prestataire insuffisantes	3. Forte
Mauvaise utilisation des compétences	• Personnels responsables de ces dispositifs non conscients des problèmes de sécurité ou mal formés • Compétences inappropriées		3. Forte
Perturbation des conditions de travail	• Personnels responsables de ces dispositifs non conscients des problèmes de sécurité ou mal formés		2. Significative
Manque de formation du personnel interne	• Compétences inappropriées		2. Significative
Départ d'une personne	• Faible loyauté vis-à-vis de l'organisme		2. Significative

3.2 Organisation Externe (ORG_EXT)

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Organisation Externe (ORG_EXT)	Menace sur l'organisation externe causant une indisponibilité	D	• Technicien du centre de support	• M21. PER-DEP (D,I) Surcharge des capacités d'une personne	• Surcharge des activités	3. Forte
	Menace sur l'organisation externe causant une altération	I	• Technicien du centre de support	• M21. PER-DEP (D,I) Surcharge des capacités d'une personne	• Perturbation des conditions de travail • Mauvaise utilisation des compétences • Manque de maîtrise du prestataire	3. Forte
	Menace sur l'organisation externe causant une compromission	C	• Technicien du centre de support	• M24. PER-PTE (D, C) Départ d'une personne	• Départ d'un prestataire	3. Forte

Menace	Vulnérabilités	Pré-requis	Vraisemblance

Surcharge des activités	• Ressources insuffisantes pour réaliser les activités	• Ressources allouées par le prestataire insuffisantes	3. Forte
Mauvaise utilisation des compétences	• Personnels responsables de ces dispositifs non conscients des problèmes de sécurité ou mal formés • Compétences inappropriées		3. Forte
Perturbation des conditions de travail	• Personnels responsables de ces dispositifs non conscients des problèmes de sécurité ou mal formés		2. Significative
Manque de maîtrise du prestataire	• Compétences inappropriées		2. Significative
Départ d'un prestataire	• Privilèges élevés sur les logiciels d'accès distant	• Turn-over élevé •	3. Forte

3.3 Système de sauvegarde (SYS_SAV)

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Système de sauvegarde (SYS_SAV)	Menace sur le système de sauvegarde causant une indisponibilité	D	• Pirate • Concurrent	• M11. LOG-MOD (D, I, C) Modification d'un logiciel	• Défaut d'exploitation du système de sauvegarde	2. Significatif
	Menace sur le système de sauvegarde causant une altération	I	• Pirate • Concurrent • Technicien du centre de support	• M7. LOG-USG(D, I, C) Détournement de l'usage prévu d'un logiciel • M11. LOG-MOD (D, I, C) Modification d'un logiciel	• Suppression de données, fichiers, de traces • Défaut d'exploitation du système de sauvegarde	2. Significatif
	Menace sur le système de sauvegarde causant une compromission	C	• Pirate • Concurrent • Technicien du centre de support	• M7. LOG-USG(D, I, C) Détournement de l'usage prévu d'un logiciel • M11. LOG-MOD (D, I, C) Modification d'un logiciel	• Collecte de données • Défaut d'exploitation du système de sauvegarde	2. Significatif

Menace	Vulnérabilités	Pré-requis	Vraisemblance
Défaut d'exploitation du système de sauvegarde	• Liaison établie de façon permanente avec l'extérieur • Systèmes d'exploitation des dispositifs non tenus à jour	• Accès logique au logiciel	2. Significatif
Suppression de données, fichiers, de traces	• Mots de passe par défaut (connus dans le monde entier) ou faibles • Absence de traçabilité des actions	• Connaissance du logiciel • Accès logique au logiciel	2. Significatif
Collecte de données	• Liaison établie de façon permanente avec l'extérieur • Mots de passe par défaut (connus dans le monde entier) ou faibles • Absence de traçabilité des actions • Présence de failles dans les interfaces d'accès (porte ou accès dérobés)	• Accès logique au logiciel	1. Minime

3.4 Système d'accès (SYS_ACC)

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Système d'accès (SYS_ACC)	Menace sur le système d'accès causant une indisponibilité	D	• Pirate • Concurrent	• M13. RSX-USG (D, I) Attaque du milieu sur un canal informatique ou de	• Attaque de type Man in the Middle sur le réseau	4. Maximale

			• Panne de réseau	téléphonie • M15. RSX-DEP (D) Saturation d'un canal informatique ou de téléphonie	internet • Déni de service sur la passerelle internet • Réseau Intranet congestionné • Rupture du canal d'accès internet	
	Menace sur le système d'accès causant une altération	I	• Pirate • Concurrent • Technicien du centre de support	• M13. RSX-USG (D, I) Attaque du milieu sur un canal informatique ou de téléphonie	• Attaque de type Man in the Middle	2. Significatif
	Menace sur le système d'accès causant une compromission	C	• Pirate • Concurrent • Technicien du centre de support	• M14. RSX-ESP (C) Ecoute passive d'un canal informatique ou de téléphonie	• Acquisition de données par écoute sur le réseau Intranet	2. Significatif

Menace	Vulnérabilités	Pré-requis	Vraisemblance
Attaque de type Man in the Middle	• Interconnexion de systèmes sécurisés de confiance à des systèmes de niveau faible (internet par exemple) • Routage altérable	• Accès à la table de routage	2. Significatif
Déni de service (sur la passerelle internet)	• Interconnexion de systèmes sécurisés de confiance à des systèmes de niveau faible (internet par exemple) • Dimensionnement insuffisant de la passerelle internet	• Connaissance de l'existence et de la localisation de la passerelle internet	2. Significatif
Acquisition de données par écoute sur le réseau intranet	• Réseau perméable • Données transmises interprétables	• Accès physique et/ou logique au réseau intranet	2. Significatif
Réseau intranet congestionné	• Dimensionnement insuffisant du réseau Intranet	• Intégration d'un élément légitime ou non sur le réseau Intranet	4. Maximale
Rupture du canal d'accès internet	• Point d'accès internet unique		4. Maximale

3.5 Système du prestataire (SYS_EXT)

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Système du prestataire (SYS_EXT)	Menace sur le système du prestataire causant une indisponibilité	D	• Pirate • Concurrent • Technicien du centre de support	• M7 LOG-USG (D, I, C) Détournement de l'usage prévu d'un logiciel • M11. LOG-MOD (D, I, C) Modification d'un logiciel • M13. RSX-USG (D, I) Attaque du milieu sur un canal informatique ou de téléphonie • M15. RSX-DEP (D) Saturation d'un canal informatique ou de téléphonie	• Déni de service sur la passerelle internet du prestataire • Réseau du prestataire congestionné • Rupture du canal d'accès internet • Perte ou effacement des données	4. Maximale
	Menace sur le système du prestataire causant une altération	I	• Pirate • Concurrent • Technicien du centre de support	• M7 LOG-USG (D, I, C) Détournement de l'usage prévu d'un logiciel • M11. LOG-MOD (D, I, C) Modification d'un logiciel	• Modification des traces, des données • Erreur d'exploitation sur la passerelle internet du prestataire	3. Forte
	Menace sur le système du prestataire causant une compromission	C	• Pirate • Concurrent • Technicien du centre de support	• M7 LOG-USG (D, I, C) Détournement de l'usage prévu d'un logiciel • M11. LOG-MOD (D, I, C) Modification d'un logiciel	• Collecte des données sur les PC des prestataires • Défaut d'exploitation du système du prestataire (poste	3. Forte

					de travail, passerelle internet, logiciel d'accès distant)	

Menace	Vulnérabilités	Pré-requis	Vraisemblance
Déni de service sur la passerelle internet du prestataire	• Présence de failles dans les interfaces d'accès • Systèmes d'exploitation des dispositifs non tenus à jour	• Connaissance de l'existence de la passerelle	3. Forte
Perte ou effacement des données	• Personnels responsables de ces dispositifs non conscients des problèmes de sécurité ou mal formés	• Accès logique aux logiciels	3. Forte
Modification des traces, des données	• Absence de traçabilité des actions	• Accès logique aux logiciels • Connaissance de l'existence des logiciels d'accès distant et de supervision	2. Significative
Erreur d'exploitation sur la passerelle internet du prestataire	• Personnels responsables de ces dispositifs non conscients des problèmes de sécurité ou mal formés	• Accès logique à la passerelle internet	3. Forte
Collecte des données	• Présence de failles dans les interfaces d'accès • Mots de passe par défaut (connus dans le monde entier) ou faibles	• Accès logique aux logiciels, à la passerelle internet du prestataire	2. Significative
Défaut d'exploitation des postes de travail du prestataire et de la passerelle internet du prestataire	• Personnels responsables de ces dispositifs non conscients des problèmes de sécurité ou mal formés • Systèmes d'exploitation des dispositifs non tenus à jour	• Accès logique aux postes de travail et à la passerelle internet	3. Forte
Réseau du prestataire congestionné	• Dimensionnement insuffisant du réseau Intranet	• Intégration d'un élément légitime ou non sur le réseau Intranet	4. Maximale
Rupture du canal d'accès internet	• Point d'accès internet unique		4. Maximale

L'importance relative des scénarios de menaces précédemment analysés est évaluée de la façon suivante :

Vraisemblance	Scénarios de menaces
4. Maximale	• Menace sur le système d'accès causant une indisponibilité • Menace sur le système du prestataire causant une indisponibilité
3. Forte	• Menace sur l'organisation interne causant une indisponibilité • Menace sur l'organisation interne causant une altération • Menace sur l'organisation externe causant une indisponibilité • Menace sur l'organisation externe causant une altération • Menace sur l'organisation externe causant une compromission • Menace sur le système du prestataire causant une compromission • Menace sur le système du prestataire causant une altération
2. Significative	• Menace sur le système de sauvegarde causant une indisponibilité • Menace sur le système de sauvegarde causant une altération • Menace sur le système de sauvegarde causant une compromission • Menace sur le système d'accès causant une altération • Menace sur le système d'accès causant une compromission • Menace sur l'organisation interne causant une compromission
1. Minime	

4 Module 4 – Étude des risques

4.1 Analyse et évaluation des risques

4.1.1 R1 : Compromission de données de l'entreprise liée à un défaut d'exploitation du système de sauvegarde

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Données de l'entreprise					
ER1	Divulgation des données de l'entreprise	Privé	• Pirate • Concurrent • Technicien du centre de support	• Perte de notoriété • Perte d'avance concurrentielle • Action en justice à l'encontre de la société	4. Critique

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Système de sauvegarde (SYS_SAV)	Menace sur le système de sauvegarde causant une compromission	C	• Pirate • Concurrent • Technicien du centre de support	• M7. LOG-USG(D, I, C) Détournement de l'usage prévu d'un logiciel • M11. LOG-MOD (D, I, C) Modification d'un logiciel	• Collecte de données • Défaut d'exploitation du système de sauvegarde	2. Significative

Niveau de risque	1. Négligeable	2. Limité	3. Significatif	**4. Intolérable**
Gravité	1. Négligeable	2. Limitée	3. Importante	**4. Critique**
Vraisemblance	1. Minime	**2. Significative**	3. Forte	4. Maximale

Mesures de sécurité existantes :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
6	10.5 Sauvegarde	10.5.1 Sauvegarde des informations	Il convient de réaliser des copies de sauvegarde des informations et logiciels et de les soumettre régulièrement à essai conformément à la politique de sauvegarde convenue.	X	X	X	SYS_SAV
8	14.1 Aspects de la sécurité de l'information en matière de gestion de la continuité d'activité	14.1.3 Elaboration et mise en œuvre des plans de continuité intégrant la sécurité de l'information	Il convient d'élaborer et de mettre en œuvre des plans destinés à maintenir ou à restaurer l'exploitation et à assurer la disponibilité des informations au niveau et dans les délais requis suite à une interruption ou une panne affectant les processus métier cruciaux.			X	SYS_SAV SYS_ACC

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	~~4. Intolérable~~
Gravité	1. Négligeable	2. Limitée	**3. Importante**	~~4. Critique~~
Vraisemblance	**1. Minime**	~~2. Significative~~	3. Forte	4. Maximale

Mesures de sécurité complémentaires :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
1	10.1 Procédures et responsabilités liées à l'exploitation	10.1.1 Procédures d'exploitation documentées	Il convient que les procédures d'exploitation soient documentées, tenues à jour et disponibles pour tous les utilisateurs concernés.	X	X	X	SYS_SAV
2	10.10 Surveillance	10.10.2 Surveillance de l'exploitation du système	Il convient d'établir des procédures permettant de surveiller l'utilisation des moyens de traitement de l'information et de réexaminer périodiquement les résultats des activités de surveillance.	X	X	X	SYS_SAV
3	10.10 Surveillance	10.10.3 Protection des informations journalisées	Il convient de protéger les équipements de journalisation et les informations journalisées contre le sabotage et les accès non autorisés.	X	X		SYS_SAV
4	10.10 Surveillance	10.10.4 Journal administrateur et journal des opérations	Il convient de journaliser les activités de l'administrateur système et de l'opérateur système.	X	X		SYS_SAV
5	13.2 Gestion des améliorations et incidents liés à la sécurité de l'information	13.2.1 Responsabilités et procédures	Il convient d'établir des responsabilités et des procédures permettant de garantir une réponse rapide, efficace et pertinente en cas d'incident lié à la sécurité de l'information.			X	SYS_SAV

Niveau de risque	1. Négligeable	**2. Limité**	~~3. Significatif~~	4. Intolérable

Gravité	1. Négligeable	**2. Limitée**	~~3. Importante~~	4. Critique
Vraisemblance	**1. Minime**	2. Significative	3. Forte	4. Maximale

4.1.2 R2 : Compromission des données de l'entreprise liée à une écoute passive sur le réseau Intranet

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Données de l'entreprise					
ER1	Divulgation des données de l'entreprise	Privé	• Pirate • Concurrent • Technicien du centre de support	• Perte de notoriété • Perte d'avance concurrentielle • Action en justice à l'encontre de la société	4. Critique

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Système d'accès (SYS_ACC)	Menace sur le système d'accès causant une compromission	C	• Pirate • Concurrent • Technicien du centre de support	• M14. RSX-ESP (C) Ecoute passive d'un canal informatique ou de téléphonie	• Acquisition de données par écoute sur le réseau Intranet	2. Significatif

Niveau de risque	1. Négligeable	2. Limité	3. Significatif	**4. Intolérable**
Gravité	1. Négligeable	2. Limitée	3. Importante	**4. Critique**
Vraisemblance	1. Minime	**2. Significative**	3. Forte	4. Maximale

Mesures de sécurité existantes :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
5	10.3 Planification et acceptation du système	10.3.1 Dimensionnement	Il convient de surveiller et d'ajuster au plus près l'utilisation des ressources et il convient de faire des projections sur les dimensionnements futurs pour assurer les performances requises pour le système.	X			SYS_ACC SYS_EXT
7	10.6 Gestion de la sécurité des réseaux	10.6.2Sécurité de services réseaux	Pour tous les services réseau, il convient d'identifier les fonctions réseau, les niveaux de service et les exigences de gestion, et de les intégrer dans tout accord sur les services réseau, qu'ils soient fournis en interne ou en externe.	X	X		SYS_ACC ORG_EXT
8	14.1 Aspects de la sécurité de l'information en matière de gestion de la continuité d'activité	14.1.3 Elaboration et mise en œuvre des plans de continuité intégrant la sécurité de l'information	Il convient d'élaborer et de mettre en œuvre des plans destinés à maintenir ou à restaurer l'exploitation et à assurer la disponibilité des informations au niveau et dans les délais requis suite à une interruption ou une panne affectant les processus métier cruciaux.			X	SYS_SAV SYS_ACC

Niveau de risque	1. Négligeable	2. Limité	3. Significatif	**4. Intolérable**
Gravité	1. Négligeable	2. Limitée	3. Importante	**4. Critique**
Vraisemblance	**1. Minime**	~~2. Significative~~	3. Forte	4. Maximale

Mesures de sécurité complémentaires :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
	10.10 Surveillance	10.10.2 Surveillance de l'exploitation du système	Il convient d'établir des procédures permettant de surveiller l'utilisation des moyens de traitement de l'information et de réexaminer périodiquement les résultats des activités de surveillance.	X	X	X	SYS_ACC
	10.10 Surveillance	10.10.3 Protection des informations journalisées	Il convient de protéger les équipements de journalisation et les informations journalisées contre le sabotage et les accès non autorisés.	X	X		SYS_ACC
	10.10 Surveillance	10.10.4 Journal administrateur et journal des opérations	Il convient de journaliser les activités de l'administrateur système et de l'opérateur système.	X	X		SYS_ACC
	11.4 Contrôle d'accès au réseau	11.4.2 Authentification de l'utilisateur pour les connexions externes	Il convient d'utiliser des méthodes d'authentification appropriées pour contrôler l'accès d'utilisateurs distants.	X	X		SYS_ACC
	11.4 Contrôle d'accès au réseau	11.4.3 Identification des matériels en réseau	Il convient de considérer l'identification automatique de matériels comme un moyen d'authentification des connexions à partir de lieux et matériels spécifiques	X	X		SYS_ACC

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	~~4. Intolérable~~
Gravité	1. Négligeable	2. Limitée	**3. Importante**	~~4. Critique~~
Vraisemblance	**1. Minime**	2. Significative	3. Forte	4. Maximale

4.1.3 R3 : Compromission des données de l'entreprise suite à un départ d'un collaborateur

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Données de l'entreprise					
ER1	Divulgation des données de l'entreprise	Privé	• Pirate • Concurrent • Technicien du centre de support	• Perte de notoriété • Perte d'avance concurrentielle • Action en justice à l'encontre de la société	4. Critique

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Organisation Interne (ORG_INT)	Menace sur l'organisation interne causant une compromission	C	• Administrateur	• M24. PER-PTE (D, C) Départ d'une personne	• Départ d'une personne	2. Significative

Niveau de risque	1. Négligeable	2. Limité	3. Significatif	**4. Intolérable**

Gravité	1. Négligeable	2. Limitée	3. Importante	**4. Critique**
Vraisemblance	1. Minime	**2. Significative**	3. Forte	4. Maximale

Mesures de sécurité existantes :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
1	5.1 Politique de sécurité de l'information	5.1.1 Document de politique de sécurité de l'information	Il convient qu'un document de politique de sécurité de l'information soit approuvé par la direction, puis publié et diffusé auprès de l'ensemble des salariés et des tiers concernés.	X	X	X	ORG_INT ORG_EXT

Niveau de risque	1. Négligeable	2. Limité	3. Significatif	**4. Intolérable**
Gravité	1. Négligeable	2. Limitée	3. Importante	**4. Critique**
Vraisemblance	1. Minime	**2. Significative**	3. Forte	4. Maximale

Mesures de sécurité complémentaires :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
1	8.2 Pendant la durée du contrat	8.2.2 Sensibilisation, qualification et formations en matière de sécurité de l'information	Il convient que l'ensemble des salariés d'un organisme et, le cas échéant, les contractants et utilisateurs tiers suivent une formation adaptée sur la sensibilisation et reçoivent régulièrement les mises à jour des politiques et procédures de l'organisme, pertinentes pour leurs fonctions	X	X		ORG_INT
1	10.1 Procédures et responsabilités liées à l'exploitation	10.1.1 Procédures d'exploitation documentées	Il convient que les procédures d'exploitation soient documentées, tenues à jour et disponibles pour tous les utilisateurs concernés.	X	X	X	SYS_SAV ORG_INT

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	~~4. Intolérable~~
Gravité	1. Négligeable	2. Limitée	**3. Importante**	~~4. Critique~~
Vraisemblance	1. Minime	**2. Significative**	~~3. Forte~~	4. Maximale

4.1.4 R4 : Altération des données de l'entreprise liée à un manque de formation du personnel interne

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Données de l'entreprise					

ER2	Altération des données	Intègre	• Pirate • Concurrent • Employé du prestataire peu sérieux • Employé peu sérieux • Hébergeur/Faille dans l'application	• Perte de crédibilité • Dépenses imprévues • Perte de mémoire de l'entreprise ou de savoir-faire • Perte de confiance vis-à-vis des collaborateurs internes • Impossibilité de remplir les obligations légales	3. Importante

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Organisation Interne (ORG_INT)	Menace sur l'organisation interne causant une altération	I	• Technicien du centre de support	• M21. PER-DEP (D, I) Surcharge des capacités d'une personne	• Perturbation des conditions de travail • Mauvaise utilisation des compétences • Manque de formation du personnel interne	3. Forte

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable
Gravité	1. Négligeable	2. Limitée	**3. Importante**	4. Critique
Vraisemblance	1. Minime	2. Significative	**3. Forte**	4. Maximale

Mesures de sécurité existantes :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
1	5.1 Politique de sécurité de l'information	5.1.1 Document de politique de sécurité de l'information	Il convient qu'un document de politique de sécurité de l'information soit approuvé par la direction, puis publié et diffusé auprès de l'ensemble des salariés et des tiers concernés.	X	X	X	ORG_INT ORG_EXT

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable
Gravité	1. Négligeable	2. Limitée	**3. Importante**	4. Critique
Vraisemblance	1. Minime	2. Significative	**3. Forte**	4. Maximale

Mesures de sécurité complémentaires :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
1	8.2 Pendant la durée du contrat	8.2.2 Sensibilisation, qualification et formations en matière de sécurité de l'information	Il convient que l'ensemble des salariés d'un organisme et, le cas échéant, les contractants et utilisateurs tiers suivent une formation adaptée sur la sensibilisation et reçoivent régulièrement les mises à jour des politiques et procédures de l'organisme, pertinentes pour leurs fonctions	X	X		ORG_INT
2	10.1 Procédures et responsabilités liées à l'exploitation	10.1.1 Procédures d'exploitation documentées	Il convient que les procédures d'exploitation soient documentées, tenues à jour et disponibles pour tous les utilisateurs concernés.	X	X	X	ORG_INT
3	10.1 Procédures et responsabilités liées à l'exploitation	10.1.2 Gestion des modifications	Il convient de contrôler les changements apportés aux systèmes et moyens de traitement de l'information	X	X		ORG_INT

Niveau de risque	1. Négligeable	**2. Limité**	~~3. Significatif~~	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	~~3. Importante~~	4. Critique
Vraisemblance	1. Minime	**2. Significative**	~~3. Forte~~	4. Maximale

4.1.5 R5 : Altération des données de l'entreprise liée à un défaut d'exploitation du système de sauvegarde

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Données de l'entreprise					
ER2	Altération des données	Intègre	• Pirate • Concurrent • Employé du prestataire peu sérieux • Employé peu sérieux • Hébergeur/Faille dans l'application	• Perte de crédibilité • Dépenses imprévues • Perte de mémoire de l'entreprise ou de savoir-faire • Perte de confiance vis-à-vis des collaborateurs internes • Impossibilité de remplir les obligations légales	3. Importante

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Système de sauvegarde (SYS_SAV)	Menace sur le système de sauvegarde causant une altération	I	• Pirate • Concurrent • Technicien du centre de support	• M7. LOG-USG(D, I, C) Détournement de l'usage prévu d'un logiciel • M11. LOG-MOD (D, I, C) Modification d'un logiciel	• Suppression de données, fichiers, de traces • Défaut d'exploitation du système de sauvegarde	2. Significative

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable
Gravité	1. Négligeable	2. Limitée	**3. Importante**	4. Critique
Vraisemblance	1. Minime	**2. Significative**	3. Forte	4. Maximale

Mesures de sécurité existantes :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
6	10.5 Sauvegarde	10.5.1 Sauvegarde des informations	Il convient de réaliser des copies de sauvegarde des informations et logiciels et de les soumettre régulièrement à essai conformément à la politique de sauvegarde convenue.	X	X	X	SYS_SAV
8	14.1 Aspects de la sécurité de l'information en matière de gestion de la continuité d'activité	14.1.3 Elaboration et mise en œuvre des plans de continuité intégrant la sécurité de l'information	Il convient d'élaborer et de mettre en œuvre des plans destinés à maintenir ou à restaurer l'exploitation et à assurer la disponibilité des informations au niveau et dans les délais requis suite à une interruption ou une panne affectant les processus métier cruciaux.			X	SYS_SAV SYS_ACC

Niveau de risque	1. Négligeable	**2. Limité**	~~3. Significatif~~	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	~~3. Importante~~	4. Critique
Vraisemblance	1. Minime	**2. Significative**	3. Forte	4. Maximale

Mesures de sécurité complémentaires :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
	10.1 Procédures et responsabilités liées à l'exploitation	10.1.1 Procédures d'exploitation documentées	Il convient que les procédures d'exploitation soient documentées, tenues à jour et disponibles pour tous les utilisateurs concernés.	X	X	X	SYS_SAV ORG_INT
3	10.1 Procédures et responsabilités liées à l'exploitation	10.1.2 Gestion des modifications	Il convient de contrôler les changements apportés aux systèmes et moyens de traitement de l'information	X	X		ORG_INT
3	10.10 Surveillance	10.10.3 Protection des informations journalisées	Il convient de protéger les équipements de journalisation et les informations journalisées contre le sabotage et les accès non autorisés.	X	X		SYS_SAV SYS_ACC
3	10.1 Procédures et responsabilités liées à l'exploitation	10.1.2 Gestion des modifications	Il convient de contrôler les changements apportés aux systèmes et moyens de traitement de l'information	X	X		ORG_INT

Niveau de risque	1. Négligeable	**2. Limité**	3. Significatif	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	3. Importante	4. Critique
Vraisemblance	**1. Minime**	~~2. Significative~~	3. Forte	4. Maximale

4.1.6 R6 : Altération des données de l'entreprise liée à une attaque de type Man in The Middle

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Données de l'entreprise					
ER2	Altération des données	Intègre	• Pirate • Concurrent • Employé du prestataire peu sérieux • Employé peu sérieux • Hébergeur/Faille dans l'application	• Perte de crédibilité • Dépenses imprévues • Perte de mémoire de l'entreprise ou de savoir-faire • Perte de confiance vis-à-vis des collaborateurs internes • Impossibilité de remplir les obligations légales	3. Importante

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Système d'accès (SYS_ACC)	Menace sur le système d'accès causant une altération	I	• Pirate • Concurrent • Technicien du centre de support	• M13. RSX-USG (D, I) Attaque du milieu sur un canal informatique ou de téléphonie	• Attaque de type Man in the Middle	2. Significatif

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable
Gravité	1. Négligeable	2. Limitée	**3. Importante**	4. Critique
Vraisemblance	1. Minime	**2. Significative**	3. Forte	4. Maximale

Mesures de sécurité existantes :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
5	10.3 Planification et acceptation du système	10.3.1 Dimensionnement	Il convient de surveiller et d'ajuster au plus près l'utilisation des ressources et il convient de faire des projections sur les dimensionnements futurs pour assurer les performances requises pour le système.	X			SYS_ACC SYS_EXT
7	10.6 Gestion de la sécurité des réseaux	10.6.2Sécurité de services réseaux	Pour tous les services réseau, il convient d'identifier les fonctions réseau, les niveaux de service et les exigences de gestion, et de les intégrer dans tout accord sur les services réseau, qu'ils soient fournis en interne ou en externe.	X	X		SYS_ACC ORG_EXT
8	14.1 Aspects de la sécurité de l'information en matière de gestion de la continuité d'activité	14.1.3 Elaboration et mise en œuvre des plans de continuité intégrant la sécurité de l'information	Il convient d'élaborer et de mettre en oeuvre des plans destinés à maintenir ou à restaurer l'exploitation et à assurer la disponibilité des informations au niveau et dans les délais requis suite à une interruption ou une panne affectant les processus métier cruciaux.			X	SYS_SAV SYS_ACC

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable
Gravité	1. Négligeable	2. Limitée	**3. Importante**	4. Critique
Vraisemblance	**1. Minime**	~~2. Significative~~	3. Forte	4. Maximale

Mesures de sécurité complémentaires :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
2	10.10 Surveillance	10.10.2 Surveillance de l'exploitation du système	Il convient d'établir des procédures permettant de surveiller l'utilisation des moyens de traitement de l'information et de réexaminer périodiquement les résultats des activités de surveillance.	X	X	X	SYS_SAV SYS_ACC
	11.4 Contrôle d'accès au réseau	11.4.2 Authentification de l'utilisateur pour les connexions externes	Il convient d'utiliser des méthodes d'authentification appropriées pour contrôler l'accès d'utilisateurs distants.	X	X		SYS_ACC
	11.4 Contrôle d'accès au réseau	11.4.3 Identification des matériels en réseau	Il convient de considérer l'identification automatique de matériels comme un moyen d'authentification des connexions à partir de lieux et matériels spécifiques	X	X		SYS_ACC
	11.4 Contrôle d'accès au réseau	11.4.7 Contrôle du routage réseau	S'assurer que l'organisation mette en œuvre des mesures de routage des réseaux afin d'éviter que les connexions réseau et les flux d'informations ne portent atteinte à la politique de contrôle d'accès des applications de gestion.	x	x		SYS_ACC
	11.4 Contrôle d'accès au réseau	11.4.6 Mesure relative à la connexion réseau	Pour les réseaux partagés, en particulier les réseaux qui s'étendent au-delà des limites de l'organisme, il convient de restreindre la capacité de connexion réseau des utilisateurs, conformément à la politique de contrôle d'accès et les exigences relatives aux applications de gestion.				SYS_ACC

Niveau de risque	1. Négligeable	**2. Limité**	~~3. Significatif~~	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	~~3. Importante~~	4. Critique
Vraisemblance	**1. Minime**	2. Significative	3. Forte	4. Maximale

4.1.7 R7 : Indisponibilité des données de l'entreprise liée à un manque de formation du personnel interne

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Données de l'entreprise					
ER3	Indisponibilités des données de l'entreprise	Entre 4h et 24h	• Pirate • Concurrent • Administrateur	• Impossibilité d'assurer ou de fournir un service • Perte de confiance vis-à-vis des collaborateurs internes	2. Limitée

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Organisation Interne (ORG_INT)	Menace sur l'organisation interne causant une indisponibilité	D	• Administrateur technique interne	• M21. PER-DEP (D, I) Surcharge des capacités d'une personne	• Surcharge des activités • Mauvaise utilisation des compétences • Manque de formation du personnel interne	3. Forte

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	3. Importante	4. Critique
Vraisemblance	1. Minime	2. Significative	**3. Forte**	4. Maximale

Mesures de sécurité existantes :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
1	5.1 Politique de sécurité de l'information	5.1.1 Document de politique de sécurité de l'information	Il convient qu'un document de politique de sécurité de l'information soit approuvé par la direction, puis publié et diffusé auprès de l'ensemble des salariés et des tiers concernés.	X	X	X	ORG_INT ORG_EXT

Niveau de risque	1. Négligeable	**2. Limité**	~~3. Significatif~~	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	3. Importante	4. Critique
Vraisemblance	1. Minime	**2. Significative**	~~3. Forte~~	4. Maximale

Mesures de sécurité complémentaires :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
5	13.2 Gestion des améliorations et incidents liés à la sécurité de l'information	13.2.1 Responsabilités et procédures	Il convient d'établir des responsabilités et des procédures permettant de garantir une réponse rapide, efficace et pertinente en cas d'incident lié à la sécurité de l'information.			X	SYS_SAV
	8.2 Pendant la durée du contrat	8.2.2 Sensibilisation, qualification et formations en matière de sécurité de l'information	Il convient que l'ensemble des salariés d'un organisme et, le cas échéant, les contractants et utilisateurs tiers suivent une formation adaptée sur la sensibilisation et reçoivent régulièrement les mises à jour des politiques et procédures de l'organisme, pertinentes pour leurs fonctions	X	X		ORG_INT

Niveau de risque	1. Négligeable	**2. Limité**	3. Significatif	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	3. Importante	4. Critique
Vraisemblance	**1. Minime**	~~2. Significative~~	3. Forte	4. Maximale

4.1.8 R8 : Indisponibilité des données de l'entreprise liée à un défaut d'exploitation du système de sauvegarde

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Données de l'entreprise					

ER3	Indisponibilités des données de l'entreprise	Entre 4h et 24h	• Pirate • Concurrent • Administrateur	• Impossibilité d'assurer ou de fournir un service • Perte de confiance vis-à-vis des collaborateurs internes	2. Limitée

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Système de sauvegarde (SYS_SAV)	Menace sur le système de sauvegarde causant une indisponibilité	D	• Pirate • Concurrent	• M11. LOG-MOD (D, I, C) Modification d'un logiciel	• Défaut d'exploitation du système de sauvegarde	2. Significative

Niveau de risque	1. Négligeable	**2. Limité**	3. Significatif	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	3. Importante	4. Critique
Vraisemblance	1. Minime	**2. Significative**	3. Forte	4. Maximale

Mesures de sécurité existantes :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
6	10.5 Sauvegarde	10.5.1 Sauvegarde des informations	Il convient de réaliser des copies de sauvegarde des informations et logiciels et de les soumettre régulièrement à essai conformément à la politique de sauvegarde convenue.	X	X	X	SYS_SAV
8	14.1 Aspects de la sécurité de l'information en matière de gestion de la continuité d'activité	14.1.3 Elaboration et mise en œuvre des plans de continuité intégrant la sécurité de l'information	Il convient d'élaborer et de mettre en oeuvre des plans destinés à maintenir ou à restaurer l'exploitation et à assurer la disponibilité des informations au niveau et dans les délais requis suite à une interruption ou une panne affectant les processus métier cruciaux.			X	SYS_SAV SYS_ACC

Niveau de risque	**1. Négligeable**	~~2. Limité~~	3. Significatif	4. Intolérable
Gravité	**1. Négligeable**	~~2. Limitée~~	3. Importante	4. Critique
Vraisemblance	1. Minime	**2. Significative**	3. Forte	4. Maximale

Mesures de sécurité complémentaires :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
1	10.1 Procédures et responsabilités liées à l'exploitation	10.1.2 Gestion des modifications	Il convient de contrôler les changements apportés aux systèmes et moyens de traitement de l'information	X	X		ORG_INT
2	13.2 Gestion des améliorations et incidents liés à la sécurité de l'information	13.2.1 Responsabilités et procédures	Il convient d'établir des responsabilités et des procédures permettant de garantir une réponse rapide, efficace et pertinente en cas d'incident lié à la sécurité de l'information.			X	SYS_SAV

3	11.4 Contrôle d'accès au réseau	11.4.2 Authentification de l'utilisateur pour les connexions externes	Il convient d'utiliser des méthodes d'authentification appropriées pour contrôler l'accès d'utilisateurs distants.	X	X		SYS_ACC
4	11.4 Contrôle d'accès au réseau	11.4.3 Identification des matériels en réseau	Il convient de considérer l'identification automatique de matériels comme un moyen d'authentification des connexions à partir de lieux et matériels spécifiques	X	X		SYS_ACC
5	10.1 Procédures et responsabilités liées à l'exploitation	10.1.2 Gestion des modifications	Il convient de contrôler les changements apportés aux systèmes et moyens de traitement de l'information	X	X		ORG_INT

Niveau de risque	**1. Négligeable**	2. Limité	3. Significatif	4. Intolérable
Gravité	**1. Négligeable**	2. Limitée	3. Importante	4. Critique
Vraisemblance	**1. Minime**	~~2. Significative~~	3. Forte	4. Maximale

4.1.9 R9 : Indisponibilité des données de l'entreprise liée à un défaut d'exploitation du système de sauvegarde

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Données de l'entreprise					
ER3	Indisponibilités des données de l'entreprise	Entre 4h et 24h	• Pirate • Concurrent • Administrateur	• Impossibilité d'assurer ou de fournir un service • Perte de confiance vis-à-vis des collaborateurs internes	2. Limitée

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Système d'accès (SYS_ACC)	Menace sur le système d'accès causant une indisponibilité	D	• Pirate • Concurrent • Panne de réseau	• M13. RSX-USG (D, I) Attaque du milieu sur un canal informatique ou de téléphonie • M15. RSX-DEP (D) Saturation d'un canal informatique ou de téléphonie	• Attaque de type Man in the Middle sur le réseau internet • Déni de service sur la passerelle internet • Réseau Intranet congestionné • Rupture du canal d'accès internet	4. Maximale

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	3. Importante	4. Critique
Vraisemblance	1. Minime	2. Significative	3. Forte	**4. Maximale**

Mesures de sécurité existantes :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
5	10.3 Planification et acceptation du système	10.3.1 Dimensionnement	Il convient de surveiller et d'ajuster au plus près l'utilisation des ressources et il convient de faire des projections sur les dimensionnements futurs pour assurer	X			SYS_ACC SYS_EXT

			les performances requises pour le système.				
7	10.6 Gestion de la sécurité des réseaux	10.6.2Sécurité de services réseaux	Pour tous les services réseau, il convient d'identifier les fonctions réseau, les niveaux de service et les exigences de gestion, et de les intégrer dans tout accord sur les services réseau, qu'ils soient fournis en interne ou en externe.	X	X		SYS_ACC ORG_EXT
8	14.1 Aspects de la sécurité de l'information en matière de gestion de la continuité d'activité	14.1.3 Elaboration et mise en œuvre des plans de continuité intégrant la sécurité de l'information	Il convient d'élaborer et de mettre en oeuvre des plans destinés à maintenir ou à restaurer l'exploitation et à assurer la disponibilité des informations au niveau et dans les délais requis suite à une interruption ou une panne affectant les processus métier cruciaux.			X	SYS_SAV SYS_ACC

Niveau de risque	1. Négligeable	**2. Limité**	3. Significatif	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	3. Importante	4. Critique
Vraisemblance	**1. Minime**	2. Significative	3. Forte	~~4. Maximale~~

Mesures de sécurité complémentaires :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
	11.4 Contrôle d'accès au réseau	11.4.7 Contrôle du routage réseau	S'assurer que l'organisation mette en œuvre des mesures de routage des réseaux afin d'éviter que les connexions réseau et les flux d'informations ne portent atteinte à la politique de contrôle d'accès des applications de gestion.	x	x		SYS_ACC
	11.4 Contrôle d'accès au réseau	11.4.6 Mesure relative à la connexion réseau	Pour les réseaux partagés, en particulier les réseaux qui s'étendent au-delà des limites de l'organisme, il convient de restreindre la capacité de connexion réseau des utilisateurs, conformément à la politique de contrôle d'accès et les exigences relatives aux applications de gestion.	x	x		SYS_ACC
	10.3 Planification et acceptation du système	10.3.1 Dimensionnement	Les ressources doivent correspondre aux besoins. Il est nécessaire de faire des projections et des tests de performance pour connaître les limites du système et pouvoir anticiper toute surcharge.	x			SYS_ACC
5	13.2 Gestion des améliorations et incidents liés à la sécurité de l'information	13.2.1 Responsabilités et procédures	Il convient d'établir des responsabilités et des procédures permettant de garantir une réponse rapide, efficace et pertinente en cas d'incident lié à la sécurité de l'information.			X	SYS_SAV

Niveau de risque	**1. Négligeable**	~~2. Limité~~	3. Significatif	4. Intolérable
Gravité	**1. Négligeable**	~~2. Limitée~~	3. Importante	4. Critique
Vraisemblance	**1. Minime**	2. Significative	3. Forte	4. Maximale

4.1.10 R10 : Compromission de la fonction Téléx liée au départ d'un prestataire

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Données de l'entreprise					
ER4	Compromission de la fonction Téléx	Privée	• Technicien du centre de support	• Mise en péril du système d'information • Perte de confiance vis-à-vis des clients • Impossibilité d'assurer ou de fournir un des services de la fonction Téléx	3. Importante

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Organisation Externe (ORG_EXT)	Menace sur l'organisation externe causant une compromission	C	• Technicien du centre de support	• M24. PER-PTE (D, C) Départ d'une personne	• Départ d'un prestataire	3. Forte

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable
Gravité	1. Négligeable	2. Limitée	**3. Importante**	4. Critique
Vraisemblance	1. Minime	2. Significative	**3. Forte**	4. Maximale

Mesures de sécurité existantes :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
1	5.1 Politique de sécurité de l'information	5.1.1 Document de politique de sécurité de l'information	Il convient qu'un document de politique de sécurité de l'information soit approuvé par la direction, puis publié et diffusé auprès de l'ensemble des salariés et des tiers concernés.	X	X	X	ORG_INT ORG_EXT
2	6.1 Organisation interne	6.1.5 Engagement de confidentialité	Il convient d'identifier et de réexaminer régulièrement les exigences en matière d'engagements de confidentialité ou de non-divulgation, conformément aux besoins de 'organisme.	X	X		ORG_EXT
3	6.2 Tiers	6.2.3 La sécurité dans les accords conclus avec des tiers	Il convient que les accords conclus avec des tiers qui portent sur l'accès, le traitement, la communication ou la gestion de l'information, ou des moyens de traitement de l'information de l'organisme, ou qui portent sur l'ajout de produits ou de services aux moyens de traitement de l'information, couvrent l'ensemble des exigences applicables en matière de sécurité.	X	X	X	ORG_EXT
4	10.2 Gestion de la prestation de service par un tiers	10.2.2 Surveillance et réexamen des services tiers	Il convient que les services, rapports et enregistrements fournis par les tiers soient régulièrement contrôlés et réexaminés, et que des audits soient régulièrement réalisés.		X		ORG_EXT
8	10.6 Gestion de la sécurité des réseaux	10.6.2Sécurité de services réseaux	Pour tous les services réseau, il convient d'identifier les fonctions réseau, les niveaux de service et les exigences de gestion, et de les intégrer dans tout accord sur les services réseau, qu'ils soient fournis en interne ou en externe.	X	X		SYS_ACC ORG_EXT
10	14.1 Aspects de la sécurité de l'information en matière de gestion de l'activité	Plan de continuité de l'activité du prestataire	Le prestataire doit fournir les garanties de continuité de l'activité au travers d'un plan de continuité de l'activité. Ce PCA doit prendre en compte les exigences en matière de sécurité de l'information, les évènements pouvant être à l'origine d'interruption des processus métier, les mesures	x		x	SYS_EXT ORG_EXT

			de restauration et de maintien de la disponibilité du système d'information, ainsi que la mise à l'essai dudit plan de continuité de l'activité.				
11	15.2 Conformité avec les politiques et normes de sécurité et conformité technique	15.2.2 vérification de la conformité technique	Il convient de vérifier régulièrement la conformité des systèmes d'information avec les normes relatives à la mise en œuvre de la sécurité.			X	ORG_EXT

Niveau de risque	1. Négligeable	**2. Limité**	~~3. Significatif~~	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	~~3. Importante~~	4. Critique
Vraisemblance	1. Minime	**2. Significative**	~~3. Forte~~	4. Maximale

Mesures de sécurité complémentaires :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
5	13.2 Gestion des améliorations et incidents liés à la sécurité de l'information	13.2.1 Responsabilités et procédures	Il convient d'établir des responsabilités et des procédures permettant de garantir une réponse rapide, efficace et pertinente en cas d'incident lié à la sécurité de l'information.			X	SYS_SAV
	8.3 Fin ou modification de contrat	8.3.1 Responsabilités en fin de contrat	Il convient que les responsabilités relatives aux fins ou aux modifications de contrats soient clairement définies et attribuées.	x	x		ORG_EXT
	8.3 Fin ou modification de contrat	8.3.3 Retrait des droits d'accès	Les droits d'accès de tout utilisateur ou administrateur aux données et aux logiciels doivent être supprimés en fin de contrat ou doivent être modifiés en cas de changement de contrat ou de responsabilités.	x			ORG_EXT

Niveau de risque	1. Négligeable	**2. Limité**	3. Significatif	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	3. Importante	4. Critique
Vraisemblance	**1. Minime**	~~2. Significative~~	3. Forte	4. Maximale

4.1.11 R11: Compromission de la fonction Téléx liée à un défaut d'exploitation du système de sauvegarde

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Données de l'entreprise					
ER4	Compromission de la fonction Téléx	Privée	• Technicien du centre de support	• Mise en péril du système d'information • Perte de confiance vis-à-vis des clients • Impossibilité d'assurer ou de fournir un des services de la fonction Téléx	3. Importante

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Système de	Menace sur le système de	C	• Pirate	• M7. LOG-USG(D, I, C) Détournement de l'usage	• Collecte de	2. Significative

sauvegarde (SYS_SAV)	sauvegarde causant une compromission		• Concurrent • Technicien du centre de support	prévu d'un logiciel • M11. LOG-MOD (D, I, C) Modification d'un logiciel	données • Défaut d'exploitation du système de sauvegarde	

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable
Gravité	1. Négligeable	2. Limitée	**3. Importante**	4. Critique
Vraisemblance	1. Minime	**2. Significative**	3. Forte	4. Maximale

Mesures de sécurité existantes :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
7	10.5 Sauvegarde	10.5.1 Sauvegarde des informations	Il convient de réaliser des copies de sauvegarde des informations et logiciels et de les soumettre régulièrement à essai conformément à la politique de sauvegarde convenue.	X	X	X	SYS_SAV SYS_EXT
9	14.1 Aspects de la sécurité de l'information en matière de gestion de la continuité d'activité	14.1.3 Elaboration et mise en œuvre des plans de continuité intégrant la sécurité de l'information	Il convient d'élaborer et de mettre en oeuvre des plans destinés à maintenir ou à restaurer l'exploitation et à assurer la disponibilité des informations au niveau et dans les délais requis suite à une interruption ou une panne affectant les processus métier cruciaux.			X	SYS_SAV SYS_ACC

Niveau de risque	1. Négligeable	**2. Limité**	~~3. Significatif~~	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	~~3. Importante~~	4. Critique
Vraisemblance	**1. Minime**	2. Significative	3. Forte	4. Maximale

Mesures de sécurité complémentaires :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
1	10.1 Procédures et responsabilités liées à l'exploitation	10.1.1 Procédures d'exploitation documentées	Il convient que les procédures d'exploitation soient documentées, tenues à jour et disponibles pour tous les utilisateurs concernés.	X	X	X	SYS_SAV
2	10.1 Procédures et responsabilités liées à l'exploitation	10.1.2 Gestion des modifications	Il convient de contrôler les changements apportés aux systèmes et moyens de traitement de l'information	X	X		SYS_SAV
3	10.10 Surveillance	10.10.4 Journal administrateur et journal des opérations	Il convient de journaliser les activités de l'administrateur système et de l'opérateur système.	X	X		SYS_SAV
4	13.2 Gestion des améliorations et	13.2.1 Responsabilités	Il convient d'établir des responsabilités et des procédures permettant de garantir une réponse rapide, efficace et			X	SYS_SAV

	incidents liés à la sécurité de l'information	et procédures	pertinente en cas d'incident lié à la sécurité de l'information.				

Niveau de risque	**1. Négligeable**	~~2. Limité~~	3. Significatif	4. Intolérable
Gravité	**1. Négligeable**	~~2. Limitée~~	3. Importante	4. Critique
Vraisemblance	**1. Minime**	2. Significative	3. Forte	4. Maximale

4.1.12 R12 : Compromission de la fonction Téléx liée à une écoute passive sur le réseau Intranet

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Données de l'entreprise					
ER4	Compromission de la fonction Téléx	Privée	• Technicien du centre de support	• Mise en péril du système d'information • Perte de confiance vis-à-vis des clients • Impossibilité d'assurer ou de fournir un des services de la fonction Téléx	3. Importante

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Système d'accès (SYS_ACC)	Menace sur le système d'accès causant une compromission	C	• Pirate • Concurrent • Technicien du centre de support	• M14. RSX-ESP (C) Ecoute passive d'un canal informatique ou de téléphonie	• Acquisition de données par écoute sur le réseau Intranet	2. Significatif

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable
Gravité	1. Négligeable	2. Limitée	**3. Importante**	4. Critique
Vraisemblance	1. Minime	**2. Significative**	3. Forte	4. Maximale

Mesures de sécurité existantes :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
5	10.3 Planification et acceptation du système	10.3.1 Dimensionnement	Il convient de surveiller et d'ajuster au plus près l'utilisation des ressources et il convient de faire des projections sur les dimensionnements futurs pour assurer les performances requises pour le système.	X			SYS_ACC SYS_EXT
8	10.6 Gestion de la sécurité des réseaux	10.6.2Sécurité de services réseaux	Pour tous les services réseau, il convient d'identifier les fonctions réseau, les niveaux de service et les exigences de gestion, et de les intégrer dans tout accord sur les services réseau, qu'ils soient fournis en interne ou en externe.	X	X		SYS_ACC ORG_EXT
9	14.1 Aspects de la sécurité de l'information en matière de gestion de la continuité d'activité	14.1.3 Elaboration et mise en œuvre des plans de continuité intégrant la sécurité de	Il convient d'élaborer et de mettre en œuvre des plans destinés à maintenir ou à restaurer l'exploitation et à assurer la disponibilité des informations au niveau et dans les délais requis suite à une interruption ou une panne affectant les processus métier cruciaux.			X	SYS_SAV SYS_ACC

		l'information					

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable
Gravité	1. Négligeable	2. Limitée	**3. Importante**	4. Critique
Vraisemblance	1. Minime	**2. Significative**	3. Forte	4. Maximale

Mesures de sécurité complémentaires :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
1	10.10 Surveillance	10.10.2 Surveillance de l'exploitation du système	Il convient d'établir des procédures permettant de surveiller l'utilisation des moyens de traitement de l'information et de réexaminer périodiquement les résultats des activités de surveillance.	X	X	X	SYS_ACC
2	10.10 Surveillance	10.10.3 Protection des informations journalisées	Il convient de protéger les équipements de journalisation et les informations journalisées contre le sabotage et les accès non autorisés.	X	X		SYS_ACC
3	10.10 Surveillance	10.10.4 Journal administrateur et journal des opérations	Il convient de journaliser les activités de l'administrateur système et de l'opérateur système.	X	X		SYS_ACC
4	11.4 Contrôle d'accès au réseau	11.4.2 Authentification de l'utilisateur pour les connexions externes	Il convient d'utiliser des méthodes d'authentification appropriées pour contrôler l'accès d'utilisateurs distants.	X	X		SYS_ACC
5	11.4 Contrôle d'accès au réseau	11.4.3 Identification des matériels en réseau	Il convient de considérer l'identification automatique de matériels comme un moyen d'authentification des connexions à partir de lieux et matériels spécifiques	X	X		SYS_ACC

Niveau de risque	1. Négligeable	**2. Limité**	~~3. Significatif~~	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	~~3. Importante~~	4. Critique
Vraisemblance	**1. Minime**	~~2. Significative~~	3. Forte	4. Maximale

4.1.13 R13 : Compromission de la fonction Téléx liée à un défaut d'exploitation du système des prestataires

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Données de l'entreprise					
ER4	Compromission de la fonction Téléx	Privée	• Technicien du centre de support	• Mise en péril du système d'information • Perte de confiance vis-à-vis des clients • Impossibilité d'assurer ou de fournir	3. Importante

				un des services de la fonction Téléx	

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Système du prestataire (SYS_EXT)	Menace sur le système du prestataire causant une compromission	C	• Pirate • Concurrent • Technicien du centre de support	• M7 LOG-USG (D, I, C) Détournement de l'usage prévu d'un logiciel • M11. LOG-MOD (D, I, C) Modification d'un logiciel	• Collecte des données sur les PC des prestataires • Défaut d'exploitation du système du prestataire (poste de travail, passerelle internet, logiciel d'accès distant)	3. Forte

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable
Gravité	1. Négligeable	2. Limitée	**3. Importante**	4. Critique
Vraisemblance	1. Minime	2. Significative	**3. Forte**	4. Maximale

Mesures de sécurité existantes :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
5	10.3 Planification et acceptation du système	10.3.1 Dimensionnement	Il convient de surveiller et d'ajuster au plus près l'utilisation des ressources et il convient de faire des projections sur les dimensionnements futurs pour assurer les performances requises pour le système.	X			SYS_ACC SYS_EXT
5	10.4 Protection contre les codes malveillants	10.4.1 Mesures contre les codes malveillants	Il convient de mettre en œuvre des mesures de détection, de prévention et de récupération pour se protéger des codes malveillants ainsi que des procédures appropriées de sensibilisation des utilisateurs.	X	X	X	SYS_EXT
7	10.5 Sauvegarde	10.5.1 Sauvegarde des informations	Il convient de réaliser des copies de sauvegarde des informations et logiciels et de les soumettre régulièrement à essai conformément à la politique de sauvegarde convenue.	X	X	X	SYS_SAV SYS_EXT
10	14.1 Aspects de la sécurité de l'information en matière de gestion de l'activité	Plan de continuité de l'activité du prestataire	Le prestataire doit fournir les garanties de continuité de l'activité au travers d'un plan de continuité de l'activité. Ce PCA doit prendre en compte les exigences en matière de sécurité de l'information, les évènements pouvant être à l'origine d'interruption des processus métier, les mesures de restauration et de maintien de la disponibilité du système d'information, ainsi que la mise à l'essai dudit plan de continuité de l'activité.	x		x	SYS_EXT ORG_EXT

Niveau de risque	1. Négligeable	**2. Limité**	~~3. Significatif~~	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	~~3. Importante~~	4. Critique
Vraisemblance	1. Minime	**2. Significative**	~~3. Forte~~	4. Maximale

Mesures de sécurité complémentaires :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support

1	10.1 Procédures et responsabilités liées à l'exploitation	10.1.1 Procédures d'exploitation documentées	Il convient que les procédures d'exploitation soient documentées, tenues à jour et disponibles pour tous les utilisateurs concernés.	X	X	X	SYS_EXT
2	10.10 Surveillance	10.10.2 Surveillance de l'exploitation du système	Il convient d'établir des procédures permettant de surveiller l'utilisation des moyens de traitement de l'information et de réexaminer périodiquement les résultats des activités de surveillance.	X	X	X	SYS_EXT
3	10.10 Surveillance	10.10.3 Protection des informations journalisées	Il convient de protéger les équipements de journalisation et les informations journalisées contre le sabotage et les accès non autorisés.	X	X		SYS_EXT
4	10.10 Surveillance	10.10.4 Journal administrateur et journal des opérations	Il convient de journaliser les activités de l'administrateur système et de l'opérateur système.	X	X		SYS_EXT
5	13.2 Gestion des améliorations et incidents liés à la sécurité de l'information	13.2.1 Responsabilités et procédures	Il convient d'établir des responsabilités et des procédures permettant de garantir une réponse rapide, efficace et pertinente en cas d'incident lié à la sécurité de l'information.			X	SYS_EXT

Niveau de risque	**1. Négligeable**	~~2. Limité~~	3. Significatif	4. Intolérable
Gravité	**1. Négligeable**	~~2. Limitée~~	3. Importante	4. Critique
Vraisemblance	**1. Minime**	~~2. Significative~~	3. Forte	4. Maximale

4.1.14 R14 : Altération de la fonction Téléx liée à un manque de maîtrise du prestataire

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Données de l'entreprise					
ER5	Altération de la fonction Téléx	Intègre	• Technicien du centre de support	• Perte de données • Impossibilité d'assurer ou de fournir un des services de la fonction Téléx • Mise en péril du système d'information	3. Importante

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Organisation Externe (ORG_EXT)	Menace sur l'organisation externe causant une altération	I	• Pirate • Concurrent • Technicien du centre de support	• M21. PER-DEP (D,I) Surcharge des capacités d'une personne	• Perturbation des conditions de travail • Mauvaise utilisation des competences • Manque de maîtrise du prestataire	3. Forte

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable
Gravité	1. Négligeable	2. Limitée	**3. Importante**	4. Critique
Vraisemblance	1. Minime	2. Significative	**3. Forte**	4. Maximale

Mesures de sécurité existantes :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
1	5.1 Politique de sécurité de l'information	5.1.1 Document de politique de sécurité de l'information	Il convient qu'un document de politique de sécurité de l'information soit approuvé par la direction, puis publié et diffusé auprès de l'ensemble des salariés et des tiers concernés.	X	X	X	ORG_INT ORG_EXT
2	6.1 Organisation interne	6.1.5 Engagement de confidentialité	Il convient d'identifier et de réexaminer régulièrement les exigences en matière d'engagements de confidentialité ou de non-divulgation, conformément aux besoins de 'organisme.	X	X		ORG_EXT
3	6.2 Tiers	6.2.3 La sécurité dans les accords conclus avec des tiers	Il convient que les accords conclus avec des tiers qui portent sur l'accès, le traitement, la communication ou la gestion de l'information, ou des moyens de traitement de l'information de l'organisme, ou qui portent sur l'ajout de produits ou de services aux moyens de traitement de l'information, couvrent l'ensemble des exigences applicables en matière de sécurité.	X	X	X	ORG_EXT
4	10.2 Gestion de la prestation de service par un tiers	10.2.2 Surveillance et réexamen des services tiers	Il convient que les services, rapports et enregistrements fournis par les tiers soient régulièrement contrôlés et réexaminés, et que des audits soient régulièrement réalisés.		X		ORG_EXT
8	10.6 Gestion de la sécurité des réseaux	10.6.2Sécurité de services réseaux	Pour tous les services réseau, il convient d'identifier les fonctions réseau, les niveaux de service et les exigences de gestion, et de les intégrer dans tout accord sur les services réseau, qu'ils soient fournis en interne ou en externe.	X	X		SYS_ACC ORG_EXT
10	14.1 Aspects de la sécurité de l'information en matière de gestion de l'activité	Plan de continuité de l'activité du prestataire	Le prestataire doit fournir les garanties de continuité de l'activité au travers d'un plan de continuité de l'activité. Ce PCA doit prendre en compte les exigences en matière de sécurité de l'information, les évènements pouvant être à l'origine d'interruption des processus métier, les mesures de restauration et de maintien de la disponibilité du système d'information, ainsi que la mise à l'essai dudit plan de continuité de l'activité.	x		x	SYS_EXT ORG_EXT
11	15.2 Conformité avec les politiques et normes de sécurité et conformité technique	15.2.2 vérification de la conformité technique	Il convient de vérifier régulièrement la conformité des systèmes d'information avec les normes relatives à la mise en œuvre de la sécurité.			X	ORG_EXT

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable
Gravité	1. Négligeable	2. Limitée	**3. Importante**	4. Critique
Vraisemblance	**1. Minime**	2. Significative	~~3. Forte~~	4. Maximale

Mesures de sécurité complémentaires :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
	10.1 Procédures et responsabilités liées à l'exploitation	10.1.1 Procédures d'exploitation	Il convient que les procédures d'exploitation soient documentées, tenues à jour et disponibles pour tous les utilisateurs concernés.	X	X	X	ORG_EXT

		documentées					
	10.10 Surveillance	10.10.4 Journal administrateur et journal des opérations	Il convient de journaliser les activités de l'administrateur système et de l'opérateur système.	X	X		ORG_EXT
	8.2 Pendant la durée du contrat	8.2.2 Sensibilisation, qualification et formations en matière de sécurité de l'information	Il convient que l'ensemble des salariés d'un organisme et, le cas échéant, les contractants et utilisateurs tiers suivent une formation adaptée sur la sensibilisation et reçoivent régulièrement les mises à jour des politiques et procédures de l'organisme, pertinentes pour leurs fonctions	X	X		ORG_EXT
	10.1 Procédures et responsabilités liées à l'exploitation	10.1.2 Gestion des modifications	Il convient de contrôler les changements apportés aux systèmes et moyens de traitement de l'information	X	X		ORG_EXT

Niveau de risque	1. Négligeable	**2. Limité**	~~3. Significatif~~	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	~~3. Importante~~	4. Critique
Vraisemblance	**1. Minime**	2. Significative	3. Forte	4. Maximale

4.1.15 R15 : Altération de la fonction Téléx liée à un défaut d'exploitation du système de sauvegarde

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Données de l'entreprise					
ER5	Altération de la fonction Téléx	Intègre	• Technicien du centre de support	• Perte de données • Impossibilité d'assurer ou de fournir un des services de la fonction Téléx • Mise en péril du système d'information	3. Importante

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Système de sauvegarde (SYS_SAV)	Menace sur le système de sauvegarde causant une altération	I	• Pirate • Concurrent • Technicien du centre de support	• M7. LOG-USG(D, I, C) Détournement de l'usage prévu d'un logiciel • M11. LOG-MOD (D, I, C) Modification d'un logiciel	• Suppression de données, fichiers, de traces • Défaut d'exploitation du système de sauvegarde	2. Significatif

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable
Gravité	1. Négligeable	2. Limitée	**3. Importante**	4. Critique
Vraisemblance	1. Minime	**2. Significative**	3. Forte	4. Maximale

Mesures de sécurité existantes :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
7	10.5 Sauvegarde	10.5.1 Sauvegarde des	Il convient de réaliser des copies de sauvegarde des informations et logiciels et de les soumettre régulièrement	X	X	X	SYS_SAV

		informations	à essai conformément à la politique de sauvegarde convenue.				SYS_EXT
9	14.1 Aspects de la sécurité de l'information en matière de gestion de la continuité d'activité	14.1.3 Elaboration et mise en œuvre des plans de continuité intégrant la sécurité de l'information	Il convient d'élaborer et de mettre en œuvre des plans destinés à maintenir ou à restaurer l'exploitation et à assurer la disponibilité des informations au niveau et dans les délais requis suite à une interruption ou une panne affectant les processus métier cruciaux.			X	SYS_SAV SYS_ACC

Niveau de risque	1. Négligeable	**2. Limité**	~~3. Significatif~~	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	~~3. Importante~~	4. Critique
Vraisemblance	1. Minime	**2. Significative**	3. Forte	4. Maximale

Mesures de sécurité complémentaires :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
	10.1 Procédures et responsabilités liées à l'exploitation	10.1.4 Séparation des équipements de développement, de test et d'exploitation	Il convient de séparer les équipements de développement, de test et d'exploitation pour réduire les risques d'accès ou de changements non autorisés dans le système en exploitation.	X	X		SYS_SAV
	10. 3 Planification et acceptation du système	10.3.2 Acceptation du système	Il convient de fixer les critères d'acceptation pour les nouveaux systèmes d'information, les nouvelles versions et les mises à niveau, et de réaliser les tests adaptés du (des) système(s) au moment du développement et préalablement à leur acceptation.		X		SYS_SAV
	10.10 Surveillance	10.10.4 Journal administrateur et journal des opérations	Il convient de journaliser les activités de l'administrateur système et de l'opérateur système.	X	X		SYS_SAV SYS_ACC SYS_EXT
	13.2 Gestion des améliorations et incidents liés à la sécurité de l'information	13.2.1 Responsabilités et procédures	Il convient d'établir des responsabilités et des procédures permettant de garantir une réponse rapide, efficace et pertinente en cas d'incident lié à la sécurité de l'information.			X	SYS_SAV

Niveau de risque	1. Négligeable	**2. Limité**	3. Significatif	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	3. Importante	4. Critique
Vraisemblance	**1. Minime**	~~2. Significative~~	3. Forte	4. Maximale

4.1.16 R16 : Altération de la fonction Téléx liée à une attaque de type Man in The Middle

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Données de l'entreprise					

ER5	Altération de la fonction Téléx	Intègre	• Technicien du centre de support	• Perte de données • Impossibilité d'assurer ou de fournir un des services de la fonction Téléx • Mise en péril du système d'information	3. Importante

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Système d'accès (SYS_ACC)	Menace sur le système d'accès causant une altération	I	• Pirate • Concurrent • Technicien du centre de support	• M13. RSX-USG (D, I) Attaque du milieu sur un canal informatique ou de téléphonie	• Attaque de type Man in the Middle	2. Significatif

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable
Gravité	1. Négligeable	2. Limitée	**3. Importante**	4. Critique
Vraisemblance	1. Minime	**2. Significative**	3. Forte	4. Maximale

Mesures de sécurité existantes :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
5	10.3 Planification et acceptation du système	10.3.1 Dimensionnement	Il convient de surveiller et d'ajuster au plus près l'utilisation des ressources et il convient de faire des projections sur les dimensionnements futurs pour assurer les performances requises pour le système.	X			SYS_ACC SYS_EXT
8	10.6 Gestion de la sécurité des réseaux	10.6.2Sécurité de services réseaux	Pour tous les services réseau, il convient d'identifier les fonctions réseau, les niveaux de service et les exigences de gestion, et de les intégrer dans tout accord sur les services réseau, qu'ils soient fournis en interne ou en externe.	X	X		SYS_ACC ORG_EXT
9	14.1 Aspects de la sécurité de l'information en matière de gestion de la continuité d'activité	14.1.3 Elaboration et mise en œuvre des plans de continuité intégrant la sécurité de l'information	Il convient d'élaborer et de mettre en œuvre (des plans destinés à maintenir ou à restaurer l'exploitation et à assurer la disponibilité des informations au niveau et dans les délais requis suite à une interruption ou une panne affectant les processus métier cruciaux.			X	SYS_SAV SYS_ACC

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable
Gravité	1. Négligeable	2. Limitée	**3. Importante**	4. Critique
Vraisemblance	1. Minime	**2. Significative**	3. Forte	4. Maximale

Mesures de sécurité complémentaires :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
2	10.10 Surveillance	10.10.2 Surveillance de l'exploitation du système	Il convient d'établir des procédures permettant de surveiller l'utilisation des moyens de traitement de l'information et de réexaminer périodiquement les résultats des activités de surveillance.	X	X	X	SYS_SAV SYS_ACC

	11.4 Contrôle d'accès au réseau	11.4.2 Authentification de l'utilisateur pour les connexions externes	Il convient d'utiliser des méthodes d'authentification appropriées pour contrôler l'accès d'utilisateurs distants.	X	X		SYS_ACC
	11.4 Contrôle d'accès au réseau	11.4.3 Identification des matériels en réseau	Il convient de considérer l'identification automatique de matériels comme un moyen d'authentification des connexions à partir de lieux et matériels spécifiques	X	X		SYS_ACC
	11.4 Contrôle d'accès au réseau	11.4.7 Contrôle du routage réseau	S'assurer que l'organisation mette en œuvre des mesures de routage des réseaux afin d'éviter que les connexions réseau et les flux d'informations ne portent atteinte à la politique de contrôle d'accès des applications de gestion.	x	x		SYS_ACC
	11.4 Contrôle d'accès au réseau	11.4.6 Mesure relative à la connexion réseau	Pour les réseaux partagés, en particulier les réseaux qui s'étendent au-delà des limites de l'organisme, il convient de restreindre la capacité de connexion réseau des utilisateurs, conformément à la politique de contrôle d'accès et les exigences relatives aux applications de gestion.				SYS_ACC

Niveau de risque	1. Négligeable	**2. Limité**	~~3. Significatif~~	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	~~3. Importante~~	4. Critique
Vraisemblance	**1. Minime**	~~2. Significative~~	3. Forte	4. Maximale

4.1.17 R17 : Altération de la fonction Téléx liée à une erreur d'exploitation sur la passerelle Internet du prestataire

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Données de l'entreprise					
ER5	Altération de la fonction Téléx	Intègre	• Technicien du centre de support	• Perte de données • Impossibilité d'assurer ou de fournir un des services de la fonction Téléx • Mise en péril du système d'information	3. Importante

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Système du prestataire (SYS_EXT)	Menace sur le système du prestataire causant une altération	I	• Pirate • Concurrent • Technicien du centre de support	• M7 LOG-USG (D, I, C) Détournement de l'usage prévu d'un logiciel • M11. LOG-MOD (D, I, C) Modification d'un logiciel	• Modification des traces, des données • Erreur d'exploitation sur la passerelle internet du prestataire	3. Forte

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable
Gravité	1. Négligeable	2. Limitée	**3. Importante**	4. Critique
Vraisemblance	1. Minime	2. Significative	**3. Forte**	4. Maximale

Mesures de sécurité existantes :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support

5	10.3 Planification et acceptation du système	10.3.1 Dimensionnement	Il convient de surveiller et d'ajuster au plus près l'utilisation des ressources et il convient de faire des projections sur les dimensionnements futurs pour assurer les performances requises pour le système.	X			SYS_ACC SYS_EXT
5	10.4 Protection contre les codes malveillants	10.4.1 Mesures contre les codes malveillants	Il convient de mettre en œuvre des mesures de détection, de prévention et de récupération pour se protéger des codes malveillants ainsi que des procédures appropriées de sensibilisation des utilisateurs.	X	X	X	SYS_EXT
10	14.1 Aspects de la sécurité de l'information en matière de gestion de l'activité	Plan de continuité de l'activité du prestataire	Le prestataire doit fournir les garanties de continuité de l'activité au travers d'un plan de continuité de l'activité. Ce PCA doit prendre en compte les exigences en matière de sécurité de l'information, les évènements pouvant être à l'origine d'interruption des processus métier, les mesures de restauration et de maintien de la disponibilité du système d'information, ainsi que la mise à l'essai dudit plan de continuité de l'activité.	x		x	SYS_EXT ORG_EXT

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable
Gravité	1. Négligeable	2. Limitée	**3. Importante**	4. Critique
Vraisemblance	1. Minime	**2. Significative**	~~3. Forte~~	4. Maximale

Mesures de sécurité complémentaires :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
	10.1 Procédures et responsabilités liées à l'exploitation	10.1.4 Séparation des équipements de développement, de test et d'exploitation	Il convient de séparer les équipements de développement, de test et d'exploitation pour réduire les risques d'accès ou de changements non autorisés dans le système en exploitation.	X	X		SYS_EXT
	10. 3 Planification et acceptation du système	10.3.2 Acceptation du système	Il convient de fixer les critères d'acceptation pour les nouveaux systèmes d'information, les nouvelles versions et les mises à niveau, et de réaliser les tests adaptés du (des) système(s) au moment du développement et préalablement à leur acceptation.		X		SYS_EXT
	10.10 Surveillance	10.10.4 Journal administrateur et journal des opérations	Il convient de journaliser les activités de l'administrateur système et de l'opérateur système.	X	X		SYS_EXT
	13.2 Gestion des améliorations et incidents liés à la sécurité de l'information	13.2.1 Responsabilités et procédures	Il convient d'établir des responsabilités et des procédures permettant de garantir une réponse rapide, efficace et pertinente en cas d'incident lié à la sécurité de l'information.			X	SYS_EXT

Niveau de risque	1. Négligeable	**2. Limité**	~~3. Significatif~~	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	~~3. Importante~~	4. Critique
Vraisemblance	**1. Minime**	~~2. Significative~~	3. Forte	4. Maximale

4.1.18 R18 : Indisponibilité de la fonction Télex liée à une surcharge des activités du prestataire

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Données de l'entreprise					
ER6	Indisponibilités de la fonction Téléx	Moins de 4 heures	• Technicien du centre de support • Panne	• Perte de données • Impossibilité d'assurer ou de fournir un service	2. Limitée

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Organisation Externe (ORG_EXT)	Menace sur l'organisation externe causant une indisponibilité	D	• Technicien du centre de support	• M21. PER-DEP (D,I) Surcharge des capacités d'une personne	• Surcharge des activités	3. Forte

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	3. Importante	4. Critique
Vraisemblance	1. Minime	2. Significative	**3. Forte**	4. Maximale

Mesures de sécurité existantes :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
1	5.1 Politique de sécurité de l'information	5.1.1 Document de politique de sécurité de l'information	Il convient qu'un document de politique de sécurité de l'information soit approuvé par la direction, puis publié et diffusé auprès de l'ensemble des salariés et des tiers concernés.	X	X	X	ORG_INT ORG_EXT
2	6.1 Organisation interne	6.1.5 Engagement de confidentialité	Il convient d'identifier et de réexaminer régulièrement les exigences en matière d'engagements de confidentialité ou de non-divulgation, conformément aux besoins de 'organisme.	X	X		ORG_EXT
3	6.2 Tiers	6.2.3 La sécurité dans les accords conclus avec des tiers	Il convient que les accords conclus avec des tiers qui portent sur l'accès, le traitement, la communication ou la gestion de l'information, ou des moyens de traitement de l'information de l'organisme, ou qui portent sur l'ajout de produits ou de services aux moyens de traitement de l'information, couvrent l'ensemble des exigences applicables en matière de sécurité.	X	X	X	ORG_EXT
4	10.2 Gestion de la prestation de service par un tiers	10.2.2 Surveillance et réexamen des services tiers	Il convient que les services, rapports et enregistrements fournis par les tiers soient régulièrement contrôlés et réexaminés, et que des audits soient régulièrement réalisés.		X		ORG_EXT
8	10.6 Gestion de la sécurité des réseaux	10.6.2Sécurité de services réseaux	Pour tous les services réseau, il convient d'identifier les fonctions réseau, les niveaux de service et les exigences de gestion, et de les intégrer dans tout accord sur les services réseau, qu'ils soient fournis en interne ou en externe.	X	X		SYS_ACC ORG_EXT
10	14.1 Aspects de la sécurité de l'information en matière de gestion de l'activité	Plan de continuité de l'activité du prestataire	Le prestataire doit fournir les garanties de continuité de l'activité au travers d'un plan de continuité de l'activité. Ce PCA doit prendre en compte les exigences en matière de sécurité de l'information, les évènements pouvant être à l'origine d'interruption des processus métier, les mesures de restauration et de maintien de la disponibilité du système d'information, ainsi que la mise à l'essai dudit plan de continuité de l'activité.	x		x	SYS_EXT ORG_EXT

11	15.2 Conformité avec les politiques et normes de sécurité et conformité technique	15.2.2 vérification de la conformité technique	Il convient de vérifier régulièrement la conformité des systèmes d'information avec les normes relatives à la mise en œuvre de la sécurité.			X	ORG_EXT

Niveau de risque	**1. Négligeable**	2. Limité	~~3. Significatif~~	4. Intolérable
Gravité	**1. Négligeable**	~~2. Limitée~~	3. Importante	4. Critique
Vraisemblance	**1. Minime**	2. Significative	~~3. Forte~~	4. Maximale

Mesures de sécurité complémentaires :

Aucune mesure de sécurité complémentaire identifiée.

4.1.19 R19 : Indisponibilité de la fonction Télex liée à un défaut d'exploitation du système de sauvegarde

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Données de l'entreprise					
ER6	Indisponibilités de la fonction Téléx	Moins de 4 heures	• Technicien du centre de support • Panne	• Perte de données • Impossibilité d'assurer ou de fournir un service	2. Limitée

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Système de sauvegarde (SYS_SAV)	Menace sur le système de sauvegarde causant une indisponibilité	D	• Pirate • Concurrent	• M11. LOG-MOD (D, I, C) Modification d'un logiciel	• Défaut d'exploitation du système de sauvegarde	2. Significatif

Niveau de risque	1. Négligeable	**2. Limité**	3. Significatif	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	3. Importante	4. Critique
Vraisemblance	1. Minime	**2. Significative**	3. Forte	4. Maximale

Mesures de sécurité existantes :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
7	10.5 Sauvegarde	10.5.1 Sauvegarde des informations	Il convient de réaliser des copies de sauvegarde des informations et logiciels et de les soumettre régulièrement à essai conformément à la politique de sauvegarde convenue.	X	X	X	SYS_SAV SYS_EXT
9	14.1 Aspects de la sécurité de l'information en matière de gestion de la continuité d'activité	14.1.3 Elaboration et mise en œuvre des plans de continuité intégrant la sécurité de l'information	Il convient d'élaborer et de mettre en œuvre des plans destinés à maintenir ou à restaurer l'exploitation et à assurer la disponibilité des informations au niveau et dans les délais requis suite à une interruption ou une panne affectant les processus métier cruciaux.			X	SYS_SAV SYS_ACC

Niveau de risque	**1. Négligeable**	~~2. Limité~~	3. Significatif	4. Intolérable
Gravité	**1. Négligeable**	~~2. Limitée~~	3. Importante	4. Critique
Vraisemblance	1. Minime	**2. Significative**	3. Forte	4. Maximale

Mesures de sécurité complémentaires :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
1	10.1 Procédures et responsabilités liées à l'exploitation	10.1.2 Gestion des modifications	Il convient de contrôler les changements apportés aux systèmes et moyens de traitement de l'information	X	X		SYS_SAV
2	13.2 Gestion des améliorations et incidents liés à la sécurité de l'information	13.2.1 Responsabilités et procédures	Il convient d'établir des responsabilités et des procédures permettant de garantir une réponse rapide, efficace et pertinente en cas d'incident lié à la sécurité de l'information.			X	SYS_SAV
3	11.4 Contrôle d'accès au réseau	11.4.2 Authentification de l'utilisateur pour les connexions externes	Il convient d'utiliser des méthodes d'authentification appropriées pour contrôler l'accès d'utilisateurs distants.	X	X		SYS_SAV
4	11.4 Contrôle d'accès au réseau	11.4.3 Identification des matériels en réseau	Il convient de considérer l'identification automatique de matériels comme un moyen d'authentification des connexions à partir de lieux et matériels spécifiques	X	X		SYS_SAV
5	10.1 Procédures et responsabilités liées à l'exploitation	10.1.2 Gestion des modifications	Il convient de contrôler les changements apportés aux systèmes et moyens de traitement de l'information	X	X		SYS_SAV

Niveau de risque	**1. Négligeable**	2. Limité	3. Significatif	4. Intolérable
Gravité	**1. Négligeable**	2. Limitée	3. Importante	4. Critique
Vraisemblance	**1. Minime**	~~2. Significative~~	3. Forte	4. Maximale

4.1.20 R20 : Indisponibilité de la fonction Télex liée à une rupture du canal d'accès internet

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Données de l'entreprise					
ER6	Indisponibilités de la fonction Téléx	Moins de 4 heures	• Technicien du centre de support • Panne	• Perte de données • Impossibilité d'assurer ou de fournir un service	2. Limitée

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Système d'accès (SYS_ACC)	Menace sur le système d'accès causant une indisponibilité	D	• Pirate • Concurrent • Panne de réseau	• M13. RSX-USG (D, I) Attaque du milieu sur un canal informatique ou de téléphonie • M15. RSX-DEP (D) Saturation d'un canal informatique ou de téléphonie	• Attaque de type Man in the Middle sur le réseau internet • Déni de service sur la passerelle internet • Réseau Intranet congestionné • Rupture du canal d'accès internet	4. Maximale

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	3. Importante	4. Critique
Vraisemblance	1. Minime	2. Significative	3. Forte	**4. Maximale**

Mesures de sécurité existantes :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
5	10.3 Planification et acceptation du système	10.3.1 Dimensionnement	Il convient de surveiller et d'ajuster au plus près l'utilisation des ressources et il convient de faire des projections sur les dimensionnements futurs pour assurer les performances requises pour le système.	X			SYS_ACC SYS_EXT
8	10.6 Gestion de la sécurité des réseaux	10.6.2Sécurité de services réseaux	Pour tous les services réseau, il convient d'identifier les fonctions réseau, les niveaux de service et les exigences de gestion, et de les intégrer dans tout accord sur les services réseau, qu'ils soient fournis en interne ou en externe.	X	X		SYS_ACC ORG_EXT
9	14.1 Aspects de la sécurité de l'information en matière de gestion de la continuité d'activité	14.1.3 Elaboration et mise en œuvre des plans de continuité intégrant la sécurité de l'information	Il convient d'élaborer et de mettre en œuvre des plans destinés à maintenir ou à restaurer l'exploitation et à assurer la disponibilité des informations au niveau et dans les délais requis suite à une interruption ou une panne affectant les processus métier cruciaux.			X	SYS_SAV SYS_ACC

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	3. Importante	4. Critique
Vraisemblance	1. Minime	2. Significative	**3. Forte**	~~4. Maximale~~

Mesures de sécurité complémentaires :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
1	14.1 Aspects de la sécurité de l'information en matière de gestion de la continuité de l'activité	14.1.2 Continuité de l'activité et appréciation du risque	Il convient d'identifier les évènements pouvant être à l'origine d'interruptions des processus métier tout comme la probabilité et l'impact de telles interruptions et leurs conséquences pour la sécurité de l'information	X		X	SYS_ACC
2	14.1 Aspects de la sécurité de l'information en matière de gestion de la continuité de l'activité	14.1.3 Elaboration et mise en œuvre des plans de continuité intégrant la sécurité de l'information	Il convient d'élaborer et de mettre en œuvre des plans destinés à maintenir ou à restaurer l'exploitation et à assurer la disponibilité des informations au niveau et dans les délais requis suite à une interruption ou une panne affectant les processus métier cruciaux			X	SYS_ACC

3	14.1 Aspects de la sécurité de l'information en matière de gestion de la continuité de l'activité	14.1.5 Mise à l'essai, gestion et appréciation constante des plans de continuité de l'activité	Il convient de soumettre à essai et de mettre à jour régulièrement les plans de continuité de l'activité afin de s'assurer qu'ils sont actualisés et efficaces			X	SYS_ACC

Niveau de risque	1. Négligeable	**2. Limité**	~~3. Significatif~~	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	3. Importante	4. Critique
Vraisemblance	1. Minime	**2. Significative**	~~3. Forte~~	4. Maximale

4.1.21 R21 : Indisponibilité de la fonction Télex liée à un déni de service sur la passerelle du prestataire

N°	Evènement Redouté	Besoin	Sources de menaces	Impacts	Gravité
Données de l'entreprise					
ER6	Indisponibilités de la fonction Téléx	Moins de 4 heures	• Technicien du centre de support • Panne	• Perte de données • Impossibilité d'assurer ou de fournir un service	2. Limitée

Bien Support	Scénario de menace	Critère	Sources de menaces	Types de menace	Menaces	Vraisemblance
Système du prestataire (SYS_EXT)	Menace sur le système du prestataire causant une indisponibilité	D	• Pirate • Concurrent • Technicien du centre de support	• M7 LOG-USG (D, I, C) Détournement de l'usage prévu d'un logiciel • M11. LOG-MOD (D, I, C) Modification d'un logiciel • M13. RSX-USG (D, I) Attaque du milieu sur un canal informatique ou de téléphonie • M15. RSX-DEP (D) Saturation d'un canal informatique ou de téléphonie	• Déni de service sur la passerelle internet du prestataire • Réseau du prestataire congestionné • Rupture du canal d'accès internet • Perte ou effacement des données	4. Maximale

Niveau de risque	1. Négligeable	2. Limité	**3. Significatif**	4. Intolérable
Gravité	1. Négligeable	**2. Limitée**	3. Importante	4. Critique
Vraisemblance	1. Minime	2. Significative	3. Forte	**4. Maximale**

Mesures de sécurité existantes :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
5	10.3 Planification et acceptation du système	10.3.1 Dimensionnement	Il convient de surveiller et d'ajuster au plus près l'utilisation des ressources et il convient de faire des projections sur les dimensionnements futurs pour assurer les performances requises pour le système.	X			SYS_ACC SYS_EXT
5	10.4 Protection contre les codes malveillants	10.4.1 Mesures contre les codes malveillants	Il convient de mettre en œuvre des mesures de détection, de prévention et de récupération pour se protéger des codes malveillants ainsi que des procédures appropriées de sensibilisation des utilisateurs.	X	X	X	SYS_EXT

7	10.5 Sauvegarde	10.5.1 Sauvegarde des informations	Il convient de réaliser des copies de sauvegarde des informations et logiciels et de les soumettre régulièrement à essai conformément à la politique de sauvegarde convenue.	X	X	X	SYS_SAV SYS_EXT
10	14.1 Aspects de la sécurité de l'information en matière de gestion de l'activité	Plan de continuité de l'activité du prestataire	Le prestataire doit fournir les garanties de continuité de l'activité au travers d'un plan de continuité de l'activité. Ce PCA doit prendre en compte les exigences en matière de sécurité de l'information, les évènements pouvant être à l'origine d'interruption des processus métier, les mesures de restauration et de maintien de la disponibilité du système d'information, ainsi que la mise à l'essai dudit plan de continuité de l'activité.	x		x	SYS_EXT ORG_EXT

Niveau de risque	**1. Négligeable**	2. Limité	~~3. Significatif~~	4. Intolérable
Gravité	**1. Négligeable**	~~2. Limitée~~	3. Importante	4. Critique
Vraisemblance	1. Minime	**2. Significative**	3. Forte	~~4. Maximale~~

Mesures de sécurité complémentaires :

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
1	10.3 Planification et acceptation du système	10.3.1 Dimensionnement	Les ressources doivent correspondre aux besoins. Il est nécessaire de faire des projections et des tests de performance pour connaître les limites du système et pouvoir anticiper toute surcharge.	x			SYS_EXT

Niveau de risque	**1. Négligeable**	2. Limité	3. Significatif	4. Intolérable
Gravité	**1. Négligeable**	2. Limitée	3. Importante	4. Critique
Vraisemblance	**1. Minime**	~~2. Significative~~	3. Forte	4. Maximale

4.2 Identification des objectifs de sécurité

Le tableau suivant présente les objectifs de sécurité identifiés :

Identifiant	Description du risque	Traitement			
		Evitement	Réduction	Prise	Transfert
R1	Compromission de données de l'entreprise liée à un défaut d'exploitation du système de sauvegarde		X		
R2	Compromission des données de l'entreprise liée à une écoute passive sur le réseau Intranet		X		
R3	Compromission des données de l'entreprise suite à un départ d'un collaborateur		X		
R4	Altération des données de l'entreprise liée à un manque de formation du personnel interne		X		
R5	Altération des données de l'entreprise liée à un défaut d'exploitation du système de sauvegarde		X		
R6	Altération des données de l'entreprise liée à une attaque de type Man in The Middle		X		
R7	Indisponibilité des données de l'entreprise liée à un manque de formation du personnel interne		X		
R8	Indisponibilité des données de l'entreprise liée à un défaut d'exploitation du système de sauvegarde		X		
R9	Indisponibilité des données de l'entreprise liée à un défaut d'exploitation du système de sauvegarde		X		
R10	Compromission de la fonction Téléx liée au départ d'un prestataire		X		
R11	Compromission de la fonction Téléx liée à un défaut d'exploitation du système de sauvegarde		x		
R12	Compromission de la fonction Téléx liée à une écoute passive sur le réseau Intranet		X		
R13	Compromission de la fonction Téléx liée à un défaut d'exploitation du système des prestataires		X		
R14	Altération de la fonction Téléx liée à un manque de maîtrise du prestataire		X		
R15	Altération de la fonction Téléx liée à un défaut d'exploitation du système de sauvegarde		X		
R16	Altération de la fonction Téléx liée à une attaque de type Man in The Middle		X		
R17	Altération de la fonction Téléx liée à une erreur d'exploitation sur la passerelle Internet du prestataire		X		
R18	Indisponibilité de la fonction Télex liée à une surcharge des activités du prestataire		X		
R19	Indisponibilité de la fonction Télex liée à un défaut d'exploitation du système de sauvegarde		X		
R20	Indisponibilité de la fonction Télex liée à une rupture du canal d'accès internet		X		
R21	Indisponibilité de la fonction Télex liée à un déni de service sur la passerelle du prestataire		X		

4.3 Identification des risques résiduels

A l'issue de l'identification des objectifs de sécurité, l'organisation a mis en évidence les risques résiduels suivants :

Identifiant	Description du risque	Gravité	Vraisemblance
R1	Compromission de données de l'entreprise liée à un défaut d'exploitation du système de sauvegarde	2. Limitée	1. Minime
R2	Compromission des données de l'entreprise liée à une écoute passive sur le réseau Intranet	3. Importante	1. Minime
R3	Compromission des données de l'entreprise suite à un départ d'un collaborateur	3. Importante	1. Minime
R4	Altération des données de l'entreprise liée à un manque de formation du personnel interne	2. Limitée	2. Significative
R5	Altération des données de l'entreprise liée à un défaut d'exploitation du système de sauvegarde	2. Limitée	1. Minime
R6	Altération des données de l'entreprise liée à une attaque de type Man in The Middle	2. Limitée	1. Minime
R7	Indisponibilité des données de l'entreprise liée à un manque de formation du personnel interne	2. Limitée	1. Minime
R8	Indisponibilité des données de l'entreprise liée à un défaut d'exploitation du système de sauvegarde	1. Négligeable	1. Minime
R9	Indisponibilité des données de l'entreprise liée à un défaut d'exploitation du système de sauvegarde	2. Limitée	2. Significative
R10	Compromission de la fonction Téléx liée au départ d'un prestataire	2. Limitée	2. Significative
R11	Compromission de la fonction Téléx liée à un défaut d'exploitation du système de sauvegarde	2. Limitée	1. Minime
R12	Compromission de la fonction Téléx liée à une écoute passive sur le réseau Intranet	2. Limitée	1. Minime
R13	Compromission de la fonction Téléx liée à un défaut d'exploitation du système des prestataires	2. Limitée	1. Minime
R14	Altération de la fonction Téléx liée à un manque de maîtrise du prestataire	3. Importante	2. Significative
R15	Altération de la fonction Téléx liée à un défaut d'exploitation du système de sauvegarde	2. Limitée	1 Minime
R16	Altération de la fonction Téléx liée à une attaque de type Man in The Middle	2. Limitée	2. Significative
R17	Altération de la fonction Téléx liée à une erreur d'exploitation sur la passerelle Internet du prestataire	2. Limitée	1. Minime
R18	Indisponibilité de la fonction Télex liée à une surcharge des activités du prestataire	1. Négligeable	1. Minime
R19	Indisponibilité de la fonction Télex liée à un défaut d'exploitation du système de sauvegarde	1. Négligeable	2. Minime
R20	Indisponibilité de la fonction Télex liée à une rupture du canal d'accès internet	2. Limitée	2. Significative
R21	Indisponibilité de la fonction Télex liée à un déni de service sur la passerelle du prestataire	1. Négligeable	3. Minime

5 Module 5 – Étude des mesures de sécurité

5.1 Définition des mesures de sécurité

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
1	8.2 Pendant la durée du contrat	8.2.2 Sensibilisation, qualification et formations en matière de sécurité de l'information	Il convient que l'ensemble des salariés d'un organisme et, le cas échéant, les contractants et utilisateurs tiers suivent une formation adaptée sur la sensibilisation et reçoivent régulièrement les mises à jour des politiques et procédures de l'organisme, pertinentes pour leurs fonctions	X	X		ORG_INT
2	8.3 Fin ou modification de contrat	8.3.1 Responsabilités en fin de contrat	Il convient que les responsabilités relatives aux fins ou aux modifications de contrats soient clairement définies et attribuées.	x	x		ORG_EXT
3	8.3 Fin ou modification de contrat	8.3.3 Retrait des droits d'accès	Les droits d'accès de tout utilisateur ou administrateur aux données et aux logiciels doivent être supprimés en fin de contrat ou doivent être modifiés en cas de changement de contrat ou de responsabilités.	x			ORG_EXT
4	10.1 Procédures et responsabilités liées à l'exploitation	10.1.1 Procédures d'exploitation documentées	Il convient que les procédures d'exploitation soient documentées, tenues à jour et disponibles pour tous les utilisateurs concernés.	X	X	X	SYS_SAV ORG_INT
5	10.1 Procédures et responsabilités liées à l'exploitation	10.1.2 Gestion des modifications	Il convient de contrôler les changements apportés aux systèmes et moyens de traitement de l'information	X	X		ORG_INT
6	10.3 Planification et acceptation du système	10.3.1 Dimensionnement	Les ressources doivent correspondre aux besoins. Il est nécessaire de faire des projections et des tests de performance pour connaître les limites du système et pouvoir anticiper toute surcharge.	x			SYS_ACC
7	10.10 Surveillance	10.10.2 Surveillance de l'exploitation du système	Il convient d'établir des procédures permettant de surveiller l'utilisation des moyens de traitement de l'information et de réexaminer périodiquement les résultats des activités de surveillance.	X	X	X	SYS_SAV SYS_ACC
8	10.10 Surveillance	10.10.3 Protection des informations journalisées	Il convient de protéger les équipements de journalisation et les informations journalisées contre le sabotage et les accès non autorisés.	X	X		SYS_SAV SYS_ACC
9	10.10 Surveillance	10.10.4 Journal administrateur et journal des opérations	Il convient de journaliser les activités de l'administrateur système et de l'opérateur système.	X	X		SYS_SAV SYS_ACC
10	13.2 Gestion des améliorations et incidents liés à la sécurité de l'information	13.2.1 Responsabilités et procédures	Il convient d'établir des responsabilités et des procédures permettant de garantir une réponse rapide, efficace et pertinente en cas d'incident lié à la sécurité de l'information.			X	SYS_SAV
11	11.4 Contrôle d'accès au réseau	11.4.2 Authentification de l'utilisateur pour les	Il convient d'utiliser des méthodes d'authentification appropriées pour contrôler l'accès d'utilisateurs distants.	X	X		SYS_ACC

N°	Thème ISO 27002	Mesure de sécurité	Description	Prévention	Protection	Récupération	Bien support
		connexions externes					
12	11.4 Contrôle d'accès au réseau	11.4.3 Identification des matériels en réseau	Il convient de considérer l'identification automatique de matériels comme un moyen d'authentification des connexions à partir de lieux et matériels spécifiques	X	X		SYS_ACC
13	11.4 Contrôle d'accès au réseau	11.4.6 Mesure relative à la connexion réseau	Pour les réseaux partagés, en particulier les réseaux qui s'étendent au-delà des limites de l'organisme, il convient de restreindre la capacité de connexion réseau des utilisateurs, conformément à la politique de contrôle d'accès et les exigences relatives aux applications de gestion.	x	x		SYS_ACC
14	11.4 Contrôle d'accès au réseau	11.4.7 Contrôle du routage réseau	S'assurer que l'organisation mette en œuvre des mesures de routage des réseaux afin d'éviter que les connexions réseau et les flux d'informations ne portent atteinte à la politique de contrôle d'accès des applications de gestion.	x	x		SYS_ACC

5.2 Analyse des risque résiduels

Ce point sera à complété avec le logiciel.

5.3 Déclaration d'applicabilité

Ce point sera à complété avec le logiciel.

5.4 Mise en œuvre des mesures de sécurité

Ce point sera à complété avec le logiciel.

Formulaire de recueil de commentaires

Ce formulaire peut être envoyé à l'adresse suivante :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Sous-direction assistance, conseil et expertise
Bureau assistance et conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP
ebios@ssi.gouv.fr

Identification de la contribution
Nom et organisme (facultatif) : .....
Adresse électronique : .....
Date : .....

Remarques générales sur le document
Le document répond-il à vos besoins ? Oui ☐ Non ☐

Si oui :

Pensez-vous qu'il puisse être amélioré dans son fond ? Oui ☐ Non ☐

Si oui :

Qu'auriez-vous souhaité y trouver d'autre ?
.....
.....

Quelles parties du document vous paraissent-elles inutiles ou mal adaptées ?
.....
.....

Pensez-vous qu'il puisse être amélioré dans sa forme ? Oui ☐ Non ☐

Si oui :

Dans quel domaine peut-on l'améliorer ?
- lisibilité, compréhension ☐
- présentation ☐
- autre ☐

Précisez vos souhaits quant à la forme :
.....
.....

Si non :

Précisez le domaine pour lequel il ne vous convient pas et définissez ce qui vous aurait convenu :
.....
.....

Quels autres sujets souhaiteriez-vous voir traiter ?
.....
.....

Remarques particulières sur le document

Des commentaires détaillés peuvent être formulés à l'aide du tableau suivant.

"N°" indique un numéro d'ordre.

"Type" est composé de deux lettres :

La première lettre précise la catégorie de remarque :

- O Faute d'orthographe ou de grammaire
- E Manque d'explications ou de clarification d'un point existant
- I Texte incomplet ou manquant
- R Erreur

La seconde lettre précise son caractère :

- m mineur
- M Majeur

"Référence" indique la localisation précise dans le texte (numéro de paragraphe, ligne…).

"Énoncé de la remarque" permet de formaliser le commentaire.

"Solution proposée" permet de soumettre le moyen de résoudre le problème énoncé.

N°	Type	Référence	Énoncé de la remarque	Solution proposée
1				
2				
3				
4				
5				

Merci de votre contribution