Ecole Nationale de Sciences Appliquées Khouribga

Filière : Ingénierie des Réseaux Intelligents et de la Cybersécurité (IRIC2)

Année Académique : 2022-2023

Rapport Projet SMSI

Certification ISO 27001 pour service de réservation de billet en ligne de la RAM

Réaliser par :

NAOUR Nada
NASSIRI Selma
OUBORK Aymane
OUQA Racid
PEZONGO Mickael

Encadrer par :

Mr. Yassine MALEH

Table de matières

Introduction

Avec le développement d'internet, de plus en plus d'entreprise ouvre leur service sur internet en mettant en place des sites de gestion de différentes manières dont les achats de vente et d'achat en ligne. La société marocaine Royal Air Maroc (RAM) ne se dérobe pas de cette avancée informatique et a mis en place un service de réservation de billet en ligne. Mais pour être crédible aux yeux de ses clients et être en règles avec les lois en vigueur, la RAM décide de se certifier en ISO 27001. ISO/IEC 27001 est la norme la plus connue de la famille de normes ISO/IEC 27000 qui n'en compte pas moins d'une douzaine. Elle spécifie les exigences relatives aux systèmes de management de la sécurité des informations (SMSI). La mise en œuvre des normes de cette famille par tout type d'organisation facilite le management de la sécurité d'actifs sensibles tels que les données financières, les documents de propriété intellectuelle, les données relatives au personnel ou les informations confiées par des tiers.

Nous sommes amenés à contrôler l'infrastructure de la RAM afin de nous assurer qu'elle est conforme pour obtenir la certification ISO 27001. Notre travail se scindera en 7 grandes parties :

La première partie consistera à définir le champ d'application de notre projet de certification.

La deuxième partie se basera sur la détermination des actifs et la classification de ces actifs selon leur degré de criticité.

Dans la troisième partie, nous mènerons un audit organisationnel avec l'outil de suivi de l'implémentation de la DNSSI

Dans la quatrième partie nous identifierons des menaces puis nous les analyserons et les prioriserons selon une grille qualitative et quantitative.

La cinquième partie consistera à définir l'énoncé d'applicabilité

Dans la sixième partie nous allons modéliser un processus de gestion des incidents de la sécurité de l'information relatif par rapport l'organisation.

Pour finir la septième partie consistera à enregistrez nos actifs et soumettre les risques dans l'outil Simple Risk

I. <u>Le champ d'application (scope) de notre projet :</u>

Notre étude s'étalera sur le tunnel entier de connexion qui relie l'utilisateur souhaitant avoir un billet de vol de chez la RAM avec le serveur qui lui affectera ce dernier.

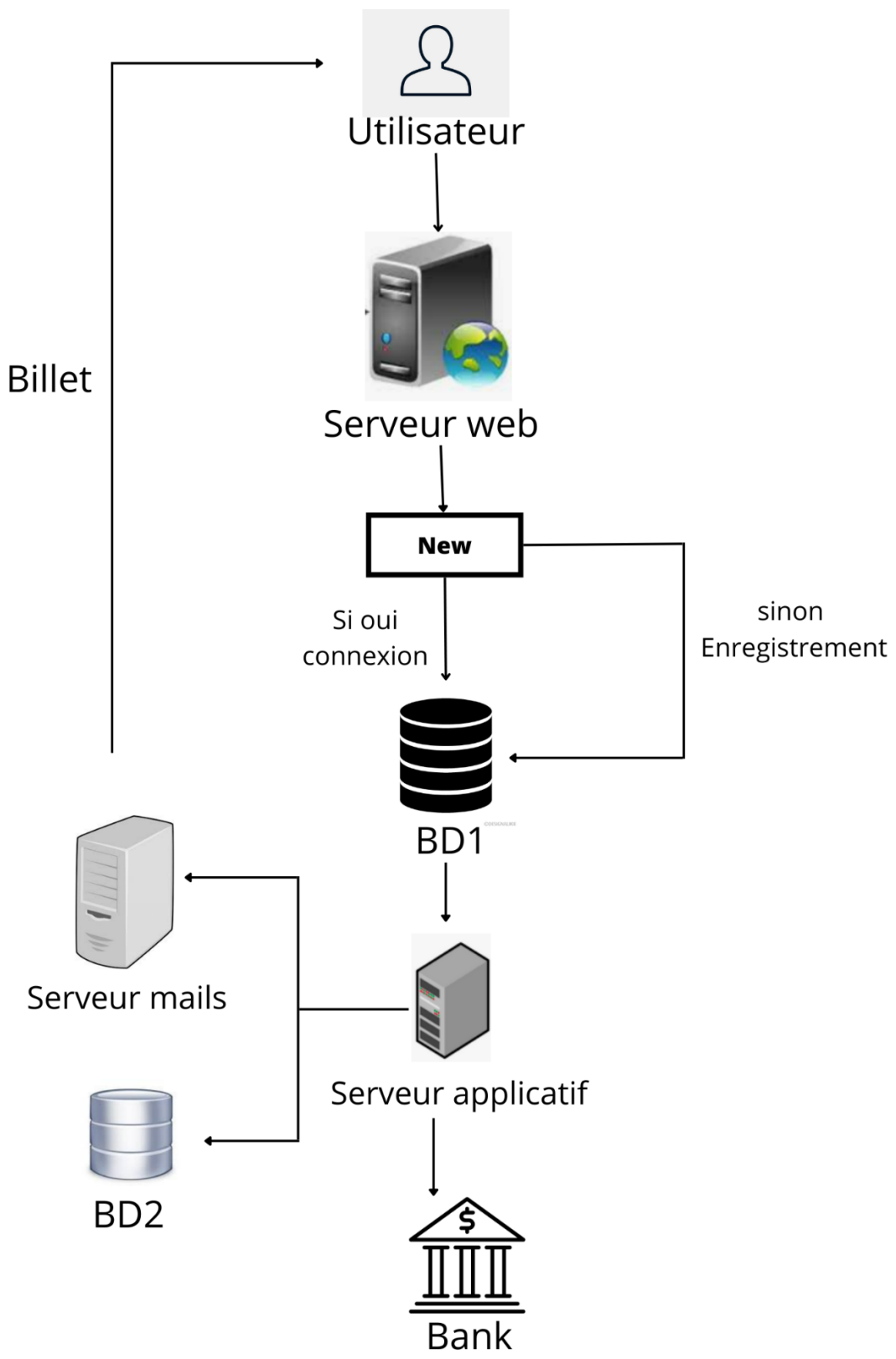
Pour cela l'utilisateur va accéder au site de la RAM réservée pour le service de réservation en ligne. Cet accès est supposé ouvert pour n'importe quel utilisateur autrement dit n'importe quelle personne souhaitant naviguer sur le site pourra le faire sans aucune contrainte.

A l'instant où l'utilisateur cliquera pour réserver un billet une fenêtre va s'afficher pour lui demander s'il s'agit de sa première réservation si c'est le cas il sera amené à remplir ses renseignements afin de créer son compte et s'enregistrer dans la base de données réservée aux clients avec leurs différents identifiants qu'on choisit de noter «BD1 », sinon il sera directement authentifié à l'aide de la même base des données.

Apres être bien authentifié le serveur applicatif prend la main pour faire la correspondance de chaque utilisateur avec son billet dans une autre base de données réservé pour cela qu'on notera « BD2 » pour une ultérieure vérification à l'aéroport au cas de besoin, plus il va être le serveur qui se chargera de faire la transaction avec la Bank du client.

Par la suite un serveur sera chargé d'envoyer à cet utilisateur son propre billet avec une facture sur son e-mail.

Ce chemin entier va faire le sujet de notre étude :



II. Les actifs informationnels selon leur degré de criticité :

Ordre de criticité	Actifs informationnels	Description
1	Serveur web	Comme il est déjà mentionné la page web sera accessible à n'importe quelle personne souhaitant y naviguer ce qui augmente le risque que ce site soit attaqué ce ainsi il ne sera plus possible d'accéder au site la chose qui n'est pas souhaitable car ceci causera de vraies pertes pour l'entreprise.
2	Serveur applicatif	C'est le serveur responsable de faire la transaction avec la banque il lui faut une protection particulière, en plus il est bien le serveur qui va se charger d'affecter à chaque utilisateur son billet dans la BD, si jamais un pirate réussit à y accéder il peut modifier comme il veut dans la BD.
3	DB1	C'est la base de données qui contient les différentes informations des clients et leur identifiants bancaires ce sont des informations personnelles que personne n'a le droit de les voir**.**
4	DB2	Cette base concerne l'attribution de chaque utilisateur avec son propre billet et bien évidemment elle doit être protégé pour éviter qu'un inconnu arrive a
5	Serveur factures	C'est le serveur responsable d'envoyer aux clients leur factures accompagné du billet
6	Terminaux des employés	Ce sont les différents terminaux (pc portables, pc postes, imprimantes…) qui doivent être protégé contre tout risque par exemple un accès non autorisé a un certain terminal

III. Outil de suivi de l'implémentation de la DNSSI :

1-Identification de l'entité :

L'identification de l'entité est un processus important dans la mise en œuvre de la Direction Nationale de Sécurité des Systèmes d'Information (DNSSI). Elle permet d'avoir une idée globale par rapport à l'entreprise qu'on souhaite auditer. Cette phase comprend plusieurs informations, commençons par :

- Informations générales
  - Dénomination de l'entité
  - Département d'appartenance
  - Adresse
  - Ville
  - Adresse du site web
- Responsable de la sécurité des SI
  - Nom et Prénom
  - Rattachement
  - E-mail
  - Téléphone
- Gestion du document
  - Auteur de l'évaluation
  - Date de l'évaluation
  - Validé par
  - Date de validation

2. Introduction :

1. Classe de sensibilité du SI :

Cette feuille permet à l'entité de définir la classe de sensibilité de son SI, en effet, la classe d'un SI est fonction :

- De la dépendance de l'entité par rapport au SI ;
- Des fonctions majeures assurées par le SI ;
- De l'ampleur de l'impact d'un incident de sécurité sur la capacité de l'entité à remplir ses missions vitales de l'Etat, sur ses biens essentiels, ou sur les individus.

2. Maturité de la SSI :

L'objectif de cette feuille est de calculer le niveau de maturité de la sécurité des systèmes d'information atteint au sein de l'entité par rapport à la DNSSI. Pour chacune des règles, l'auteur de l'évaluation est invité à donner une cotation allant de 0 à 4 définit comme suit :

- 0 : si l'entité n'est pas concernée par la règle.
- 1 : si la règle n'est pas mise en œuvre.
- 2 : si la mise en œuvre de la règle est en cours de réflexion (une règle est jugée en cours de réflexion si une étude d'opportunité ou de faisabilité est initiée).
- 3 : si la règle est mise en œuvre partiellement.
- 4 : si la règle est totalement mise en œuvre.

Les moyennes se calculent automatiquement en prenant en compte le poids de la règle et la cotation saisie.

3. Représentation graphique de la maturité :

Cette feuille a pour but de donner une synthèse de la maturité de la SSI selon les valeurs renseignées par l'entité, à l'aide de diagrammes de kiviat.

4. Indicateurs de la SSI :

Ces indicateurs ont été déduits des principes directeurs définis dans la DNSSI, ils vont permettre d'une part aux responsables des entités à tous les niveaux de définir les axes de progrès et de s'inscrire dans un processus d'amélioration continue, et d'autre part, d'aider la DGSSI à consolider une synthèse servant à la prise de décision.

Maturité de la SSI :

Chapitre	Objectifs	Règle	Question	Poids	Niveau de maturié choisi	Moyenne par objectifs
1.POLITIQUE DE SECURITE	Objectif O.1: Apporter à la sécurité de l'information une orientation et un soutien de la part du management de l'entité, conformément aux exigences de la DNSSI.	DS-BESOIN	Besoins de sécurité définis ?	4	4	4.00
		DS-EXAM	Examen annuel de l'application des mesures ?	2	4	
		DS-TDB	Tableaux de bord renseignés ?	3	4	
2.ORGANISATION DE LA SECURITE	Objectif O.2: Mettre en place au sein de l'entité une organisation adéquate garantissant une gestion préventive et réactive de la sécurité de l'information.	ORG-INTER-DIR	Implication de la direction ?	4	3	3.20
		ORG-INTER-RSSI	RSSI désigné ?	4	4	
		ORG-INTER-AUT	Relations avec les autorités compétentes en SSI entretenues ?	2	2	
	Objectif O.3: Assurer la sécurité de l'information et des moyens de traitement de l'information de l'entité, consultés, opérés, communiqués ou gérés par des tiers.	ORG-TIER-EXIG	Exigences vis-à-vis des tiers rédigés ?	4	3	2.80
		ORG-TIER-RISQ	Risques émanant des tiers pris en compte ?	3	2	
		ORG-TIER-EXTER	Externalisation maîtrisée ?	4	2	
		ORG-TIER-HEBERG	Hébergement sur territoire national ?	4	4	
3.GESTION DES BIENS	Responsabilités relatives aux biens Objectif O.4: Inventorier tous les biens et leur attribuer un propriétaire.	RESP-BIEN-INV	Inventaire des biens réalisé ?	2	2	3.00
		RESP-BIEN-CARTO	Cartographie SI réalisée et maintenue ?	4	3	
		RESP-BIEN-PROP	Propriétaires des biens identifiés ?	2	4	
	Classification des informations Objectif O.5: Classer les informations en termes d'exigences légales, de sensibilité et de criticité, afin de garantir un niveau de protection approprié.	CLASSIF-INFO-ECH	Echelle de classification établie ?	4	3	1.80
		CLASSIF-INFO-MES	Mesures de protection des informations mises en œuvre ?	4	1	
		CLASSIF-INFO-EXAM	Examen annuel de la classification ?	2	1	
4.SECURITE LIEE AUX RESSOURCES HUMAINES	Objectif O.6: Garantir que le personnel, les contractants et les utilisateurs tiers connaissent leurs	RH-AVT-ENQ	Personnel de confiance ?	3	1	2.13
		RH-AVT-CONFID	Engagements de confidentialité ?	4	1	
		RH-PDT- FORM	Formation du personnel	3	2	

	obligations en matière de SSI.	RH-FIN-REST	Restitution des biens ?	3	3	
		RH-FIN-ACC	Retrait des accès ?	3	4	
5.SECURITE PHYSIQUE	Zones sécurisées Objectif O.7: Empêcher tout accès physique non autorisé, tout dommage ou intrusion dans les locaux et les informations de l'entité	PHYS-DECOUP	Zones physiques de sécurité délimitées ?	4	3	3.17
		PHYS-SIGNAL	Signalétique déployée ?	1	3	
		PHYS-PROC	Procédure de contrôle d'accès physique formalisée ?	3	3	
		PHYS-PUBLIC-RES	Accès réseau installé dans une zone d'accueil du public filtré ou isolé ?	4	2	
		PHYS-PUBLIC-INFO.SENS	Mesures spécifiques pour informations sensibles en zone publique ?	3	3	
		PHYS-INTER/RESTR-DISPO	Dispositif de contrôle d'accès physique individualisé dans les zones restreintes ?	4	3	
		PHYS-INTER/RESTR-TRACE	Traçabilité des accès du personnel et des visiteurs externes aux zones restreintes ?	4	4	
		PHYS-INTER/RESTR-VIDEOPROT	Vidéo-protection dans les zones restreintes ?	3	3	
		PHYS-ENVIR-INCEN.FUM	Détecteurs d'incendie dans les zones restreintes ?	4	4	
		PHYS-ENVIR-INCEN.EXTINCT	Extinction automatique d'incendie dans les zones restreintes ?	4	3	
		PHYS-ENVIR-EAU	Protections contre les dégâts des eaux des équipements sensibles ?	2	4	
	Sécurité du matériel Objectif O8 : Empêcher la perte, l'endommagement ou la compromission des biens et	PHYS-MAT-CABL	Sécurité du câblage ?	4	3	2.50
		PHYS-MAT-OND	Protections par onduleurs ?	4	1	
		PHYS-MAT-ELECTROG	Groupe électrogène en secours ?	2	2	
		PHYS-MAT-CLIM	Climatisation en zones restreintes ?	4	4	

	l'interruption des activités de l'entité	PHYS-MAT-MAINT	Contrôle périodique des équipements de sécurité ?	3	3	
		PHYS-MAT-MAINT. DELAI	Délais d'intervention spécifiés dans contrats de maintenance ?	2	2	
		PHYS-MAT-REB	Procédures de mise au rebut avec effacements ?	3	2	
6.GESTION DE L'EXPLOITATION ET DES TELECOMMUNICATIONS	Procédures et responsabilités liées à l'exploitation Objectif O.9: Assurer l'exploitation correcte et sécurisée des moyens de traitement de l'information et gérer les actions d'administration du SI.	EXP-PROC-FORMEL	Procédures d'exploitation rédigées et maintenues ?	4	3	3.05
		PROC-ADMIN-ACC	Procédure formelle d'autorisation d'accès aux outils et interfaces d'administration ?	4	3	
		PROC-ADMIN-TRACE	Traçabilité des actions d'administration ?	4	4	
		PROC-ADMIN-DIST	Sécurisation de l'administration à distance ?	4	3	
		PROC-ADMIN-CENTR	Outils centralisés d'automatisation et de supervision ?	3	2	
	Planification et acceptation du système Objectif O.10: Réduire le plus possible le risque de pannes du système	EXP-SYS-CONFIG	Procédures formalisées de configurations systèmes ?	4	2	2.43
		EXP-SYS-ANAL	Analyses de dimensionnement ?	3	3	
	Protection contre les codes malveillants Objectif O.11: Protéger l'intégrité des logiciels et de l'information	EXP-PROTEC-CODE.MALVEIL	Logiciels de protection déployés ?	4	3	3.43
		EXP-PROTEC-NAVIG	Configuration sécurisée des navigateurs	3	4	
	Sauvegarde des informations Objectif O.12: Maintenir l'intégrité et la disponibilité des informations et des moyens de traitement de l'information	EXP-SAUV-PROC	Procédures de sauvegardes ?	3	2	3.07
		EXP-SAUV-RESTAUR	Restauration en temps voulu ?	4	3	
		EXP-SAUV-PHYS	Protection physique des sauvegardes ?	3	3	
		EXP-SAUV-SENSI	Sauvegarde chiffrée des données sensibles ?	4	4	
	Gestion de la sécurité des	EXP-RES-CONFIG	Configurations durcies ?	4	3	3.00

	réseaux Objectif O.13: Assurer la protection des informations sur les réseaux et la protection de l'infrastructure sur laquelle ils s'appuient	EXP-RES-WIFI	Étude de sécurité spécifique pour le sans-fil ?	3	3	
	Manipulation des supports Objectif O.14: Contrôler et protéger les supports amovibles et nomades	EXP-NOM/AMOV-GEST	Traitement de sécurité adapté aux supports amovibles ?	4	4	3.00
		EXP-NOM/AMOV-STOCK	Stockage sécurisé des postes nomades et supports amovibles contenant des données sensibles ?	3	3	
		EXP-NOM/AMOV-MES	Mesures de sécurité appliquées aux postes nomades et supports amovibles ?	0	0	
		EXP-AMOV-SENSI	Chiffrement des données sensibles sur poste nomade ou support amovible par dispositif de confiance ?	4	2	
	Echange des informations Objectif O.15: Maintenir la sécurité des échanges des informations et des supports physiques au sein de l'entité et avec un organisme externe.	EXP-ECHG-TELECOM	Exigences de confidentialité pour les échanges d'informations sensibles ?	4	3	2.86
		EXP-ECHG-PHYS.COUR	Sécurisation des échanges physiques de supports ?	2	4	
		EXP-ECHG-MAIL.PERSO	Bon usage de la messagerie professionnelle ?	4	2	
		EXP-ECHG-MAIL.FILTR	Filtrage de sécurité des mails ?	4	3	
	Supervision Objectif O.16: Détecter les traitements non autorisés de l'information	EXP-SUPERV-MAINT	Actions de maintenance tracées ?	4	3	3.00
		EXP-SUPERV-JOURNAL	Journalisation des événements ?	4	2	
		EXP-SUPERV-SYNCHRON	Base de temps unique ?	4	4	
7.CONTROLE D'ACCES	Gestion de l'accès utilisateur Objectif O.17: Maîtriser l'accès à l'information par	ACC-UTILIS-IDF/AUTH	Droits individuels d'accès aux ressources nécessaires et suffisants ?	4	3	3.50

	l'application d'une politique du moindre privilège	ACC-UTILIS - MULTIUTILIS	Traçabilité des comptes métiers ?	4	3	
		ACC-UTILIS-MDP	Règles de gestion des mots de passe définies et appliquées ?	4	4	
		ACC-UTILIS-EXAM	Examen périodique des droits d'accès ?	4	4	
	Contrôle d'accès au réseau Objectif O.18: Empêcher les accès non autorisés aux services disponibles sur le réseau	ACC-DISTANT-AUT	Authentification forte des accès distants ?	4	3	3.48
		ACC-DISTANT-CHIFFR	Chiffrement des connexions à distance ?	4	4	
		ACC-PORT-DIS	Désactivation des ports d'accès inutiles ?	4	4	
		ACC-PORT-CONFIG	Accès strictement limité et contrôlé aux ports de diagnostic et de configuration ?	4	3	
		ACC-RES-SEG	Segmentation du réseau ?	3	4	
		ACC-RES-SEG.PROTEC	Filtrages entre zones documentés et maintenus ?	4	3	
	Contrôle d'accès aux applications et à l'information Objectif O.19 : Empêcher les accès non autorisés aux informations stockées dans les applications	ACC-APP-SENSI	Filtrage applicatif pour les applications à risque ?	4	3	3.00
8.ACQUISITION, DEVELOPPEMENT ET MAINTENANCE	Exigences de sécurité applicable aux systèmes d'information Objectif O.20: Veiller à ce que la sécurité fasse partie intégrante dans les projets de développement des systèmes d'information	DEV-EXIG-PROJ	Sécurité intégrée dans toutes les étapes du cycle de vie du projet ?	4	4	4.00
	Bon fonctionnement des applications Objectif O. 21 : Empêcher toute erreur, perte, modification non autorisée ou tout mauvais usage des	DEV-FONCT-ENTREE	Contrôles des données en entrée ?	3	3	3.17
		DEV-FCT-INTERN	Programmation défensive ?	1	4	
		DEV-FCT- SORT	Contrôles de validation automatique des sorties des	2	3	

	informations dans les applications		traitement sensibles ?			
	Mesures cryptographiques Objectif O.22: protéger la confidentialité, l'authenticité ou l'intégrité de l'information par des moyens cryptographiques	DEV-CRYPTO-FICH	Usage de la cryptographie spécifiée au niveau de l'architecture applicative ?	3	4	3.43
		DEV-CRYPTO-PKI	PKI ou IGC de confiance ?	4	3	
	Sécurité des fichiers système Objectif O.23: Mener les développements logiciels selon une méthodologie de sécurisation du code source pour son intégrité	DEV-CODE	Protection des codes sources ?	3	4	4.00
	Sécurité en matière de développement et d'assistance technique Objectif O.24: Empêcher toute possibilité de fuite d'informations	DEV-FUITE	Limitation des fuites d'information ?	3	3	3.00
	Gestion des vulnérabilités techniques Objectif O.25: Réduire les risques liés à l'exploitation des vulnérabilités techniques ayant fait l'objet d'une publication	DEV-VULN	Études de vulnérabilités système et applicative ?	4	4	4.00
9.GESTION DES INCIDENTS	Signalement des événements et des failles liés à la sécurité de l'information Objectif O. 26 : Garantir que le mode de notification des événements et failles liés à la sécurité de l'information permette la mise en œuvre d'une action corrective, dans les meilleurs délais	INCID-SIGNAL	Formalisation d'une procédure de signalement d'incidents ?	4	3	3.44
		INCID-PROC	Formalisation des procédures de gestion d'incidents ?	4	4	
		INCID-ACTION	Prise des bonnes décisions pour la collecte de traces ?	4	3	
		INCID-REACT	Mobilisation suite à réception d'une alerte ?	4	4	
		INCID-REP	Constitution d'une base	2	3	

			répertoire des incidents ?			
10.GESTION DU PLAN DE CONTINUITE DE L'ACTIVITE	Aspects de la sécurité de l'information en matière de gestion de la continuité de l'activité Objectif O.27: Neutraliser les interruptions des activités de l'entité, protéger les processus métier cruciaux des effets causés par les principales défaillances des systèmes d'information ou par des sinistres et garantir une reprise de ces processus dans les meilleurs délais.	CONTINU-BIA	Analyse d'impacts sur l'activité ?	4	3	3.43
		CONTINU-ACT	Constitution d'un PCA/PRA ?	4	4	
		INCID-TEST.PLAN	Planification de tests techniques annuels ?	4	4	
		INCID-TEST.EX/SCEN	Exercices de crise ?	2	2	
11.CONFORMITE	Conformité avec les exigences légales Objectif O.28: Eviter toute violation des obligations légales, statutaires, réglementaires ou contractuelles et des exigences de sécurité	CONF-EXIG	Explicitation des exigences réglementaires, contractuelles et légales dans une charte ?	3	3	3.52
		CONF-LIC	Licences en règles ?	4	4	
		CONF-ARCH	Protection des archives conformément à la législation ?	2	3	
		CONF-DONNEE.PERSO	Protection des données à caractère personnel conformément à la législation ?	4	3	
		CONF-CRYPTO	Respect du cadre normatif relatif à la mise en œuvre des mesures cryptographiques ?	4	4	
		CONF-DNSSI	Vérifications régulières de la conformité à la DNSSI ?	2	4	
		CONF-CHART.SI	Charte de sécurité du SI signée par les utilisateurs ?	2	4	
		CONF-RGS	Conformité au référentiel général de la sécurité ?	2	3	

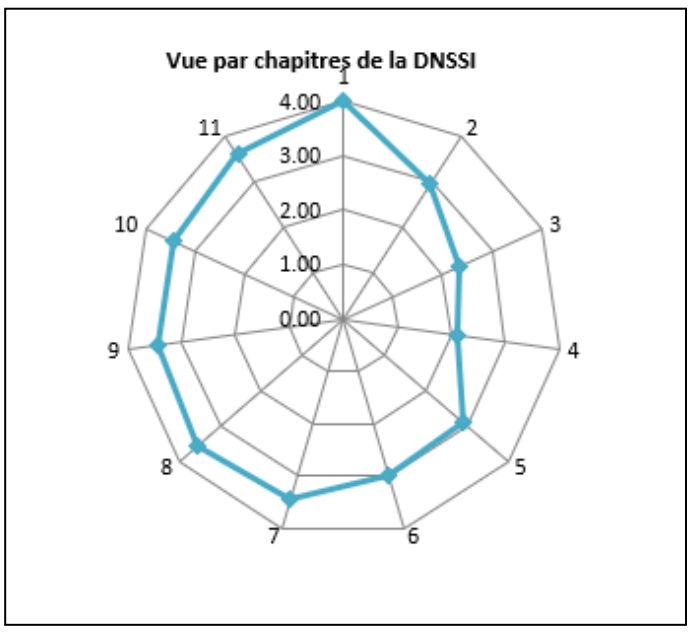
	Prise en compte de l'audit du système d'information Objectif O.29: Mener des opérations d'audit et capitaliser sur les résultats obtenus	CONF-AUDIT	Audits réguliers ?	4	4	4.00

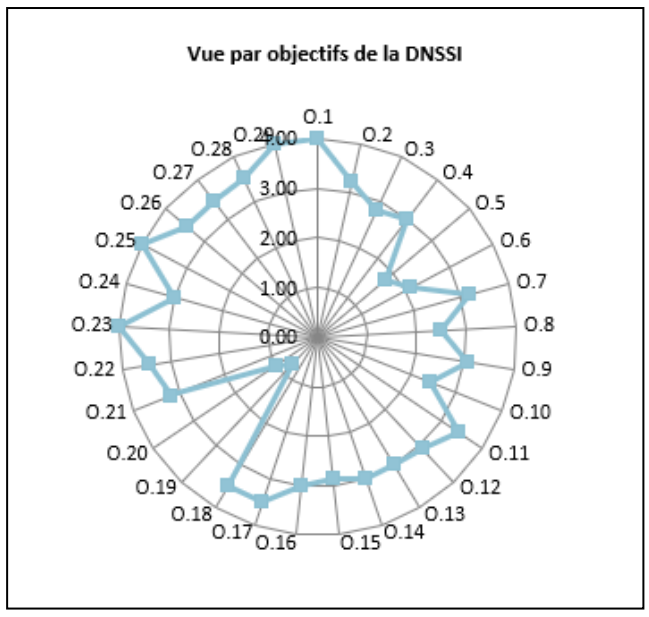
Taux de conformité à la DNSSI	35.29%

Indicateurs de la SSI :

Principes directeurs	Libellé indicateur	Description (méthode de calcul)	Valeur
P1 : Structure organisationnelle	Moyenne obtenue en fonction de l'implémentation des règles de l'objectif 2 de la DNSSI relatif à l'organisation de la SSI.	Valeur indiquée à extraire de la feuille maturité de la SSI. Elle est sur une échelle de 0 à 4. Une valeur inférieure à 2,5 par exemple indique qu'une attention particulière est demandée concernant cet aspect.	3.20
P2 : cartographie des SI	Moyenne obtenue en fonction de l'implémentation des règles de l'objectif 4 de la DNSSI relatif à la gestion des biens.	Valeur indiquée à extraire de la feuille maturité de la SSI. Elle est sur une échelle de 0 à 4. Une valeur inférieure à 2,5 par exemple indique qu'une attention particulière est demandée concernant cet aspect.	3.00
P3 : Budget de la SSI	Taux de budget consacré aux projets SSI par rapport au budget SI	Pourcentage du budget consacré aux projets SSI par rapport au budget total annuel consacré aux projets SI	30%
P4 : Contrôle des administrateurs	Taux de plateformes et de systèmes dont les journaux d'événement sont traités et revus périodiquement	Pourcentage des plateformes et systèmes dont les journaux d'événement sont traités et revus périodiquement par rapport au nombre total des plateformes et systèmes	35%
P5 : Protection de l'information	Nombre d'incidents de sécurité induisant l'indisponibilité d'un /ou des services	Nombre par an	50
	Nombre d'incidents induisant la perte des données sensibles (vol, divulgation, altération)	Nombre par an	35
	Taux d'application de patch et mises à jour logiciels et matériel	Pourcentage de plateformes et de systèmes dont l'application des patchs et mises à jour se font régulièrement par rapport au nombre total des plateformes et systèmes	15%
	Fréquence de vérification des sauvegardes	Nombre d'opération de restauration test par an	12
	Taux de plateformes et de système critiques disposant d'un plan de reprise d'activité	Pourcentage de plateformes et systèmes critiques disposant d'un plan de reprise d'activité par rapport au nombre totale de plateformes et de système critiques	25%
	Nombre des audits effectués	Nombre par an	24
P6 : Formation et sensibilisation	Taux d'utilisateurs sensibilisés en SSI	Pourcentage d'utilisateurs sensibilisés en SSI par rapport au nombre d'utilisateurs cibles devant suivre une formation de sensibilisation en SSI	45%
	Taux d'administrateurs formés en SSI	Pourcentage d'administrateurs formés en SSI par rapport au nombre d'administrateurs	70%

Représentions graphiques :





Moyenne par objectif :

Taux de conformité à la DNSSI	35.29%

Chapitres DNSSI	Objectifs de la DNSSI	Moyenne par objectif
1. Politique de sécurité	O.1	4.00
2. Organisation de la sécurité d'information	O.2	3.20
	O.3	2.80
3. Gestion des biens	O.4	3.00
	O.5	1.80
4. Sécurité liée aux ressources humaines	O.6	2.13
5. Sécurité physique et environnementale	O.7	3.17
	O.8	2.50
6. Gestion de l'exploitation et des télécommunications	O.9	3.05
	O.10	2.43
	O.11	3.43
	O.12	3.07
	O.13	3.00
	O.14	3.00
	O.15	2.86
	O.16	3.00
7. Contrôle d'accès	O.17	3.50
	O.18	3.48
	O.19	0.75
8. Acquisition, développement et maintenance des systèmes d'information	O.20	1.00
	O.21	3.17
	O.22	3.43
	O.23	4.00
	O.24	3.00

	O.25	**4.00**
9. Gestion des incidents liés à la sécurité de l'information	O.26	**3.44**
10. Gestion de plan de continuité de l'activité	O.27	**3.43**
11. Conformité	O.28	**3.52**
	O.29	**4.00**

Moyenne par chapitre :

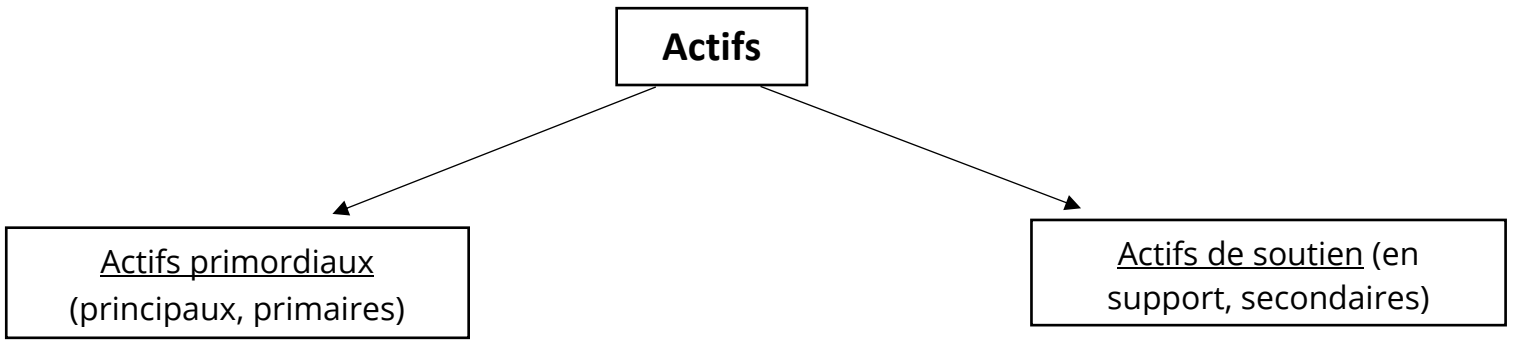
Chapitres DNSSI	Moyenne par chapitre
1. Politique de sécurité	4.00
2. Organisation de la sécurité d'information	2.96
3. Gestion des biens	2.33
4. Sécurité liée aux ressources humaines	2.13
5. Sécurité physique et environnementale	2.91
6. Gestion de l'exploitation et des télécommunications	2.99
7. Contrôle d'accès	3.44
8. Acquisition, développement et maintenance des systèmes d'information	3.56
9. Gestion des incidents liés à la sécurité de l'information	3.44
10. Gestion de plan de continuité de l'activité	3.43
11. Conformité	3.59

IV. Évaluation des menaces :

1- Actif, menace, vulnérabilité, Impact, Risque :

1-1-Définition d'un actif (asset) :

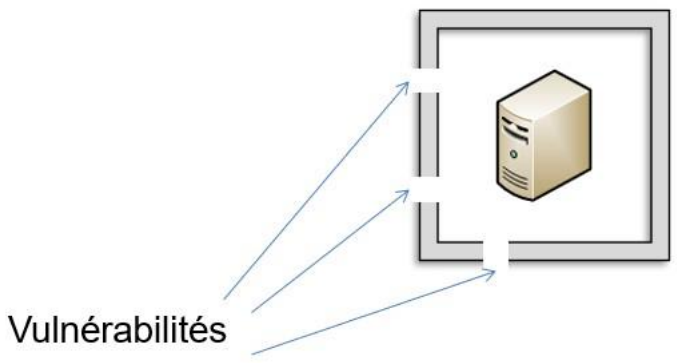
Les actifs comprennent les serveurs, les coordonnées des clients, les documents sensibles des partenaires, les secrets commerciaux, etc.



1-2-Définition de la vulnérabilité :

Faiblesse au niveau d'un bien.

Les menaces peuvent exploiter les vulnérabilités.



Une vulnérabilité est une faiblesse qu'une menace peut exploiter pour enfreindre la sécurité et nuire à votre entreprise. Les vulnérabilités peuvent être identifiées au moyen d'analyses des vulnérabilités et de rapports d'audit.

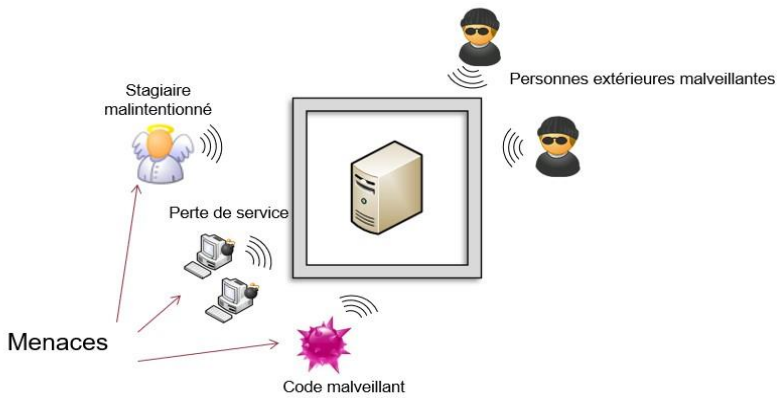
Effectuer des tests sur le système informatique contribue également à identifier les vulnérabilités. Les tests peuvent inclure :

- Procédures de tests et d'évaluation de la sécurité informatique (ST&E)
- Techniques de tests de pénétration
- Outils d'analyse automatisée des vulnérabilités

Vous pouvez réduire les vulnérabilités qui concernent vos logiciels et gérant correctement les correctifs. Mais ne négligez pas les vulnérabilités physiques. Par exemple, en déménageant votre salle de serveurs au premier étage du bâtiment, vous réduisez considérablement votre vulnérabilité aux inondations.

1-3-Définition de la menace :

Une menace est tout ce qui peut exploiter une vulnérabilité pour enfreindre la sécurité et porter préjudice à votre organisation. Les pirates informatiques et les logiciels malveillants viennent spontanément à l'esprit.



Les menaces sont classées par :

- Origine
- Type
- Source, motivation, action

Origines des menaces :

- Accidentelle : **A**
  Action humaine qui endommage accidentellement un actif.
- Délibérée : **D**
  Action délibérée sur un actif.
- Environnementale : **E**
  Tout incident sur un actif qui ne vient pas d'une action humaine.

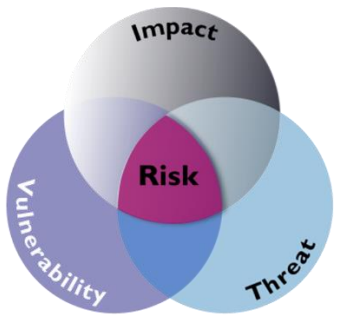
1-4-Définition de risque :

Le risque est un concept économique – la probabilité de pertes financières pour l'organisation est-elle élevée, moyenne, faible ou nulle ? Trois facteurs entrent en ligne de compte dans la détermination du risque : la nature de la menace, la vulnérabilité du système et l'importance de l'actif qui pourrait être endommagé ou rendu indisponible.

1-5-Définition d'impact :

L'impact (ou encore conséquence) d'un événement reflète le niveau, la durée et la nature de la perte résultant de l'incident. Les conséquences potentielles peuvent inclure des impacts sur plusieurs niveaux (santé, la sécurité publiques, psychologiques etc..). Souvent, les gens négligent les conséquences lors de l'évaluation des risques, surtout lorsqu'une menace est probable, mais les conséquences sont insignifiantes. Et parfois, les gens se concentrent sur les conséquences/impacts élevés et les menaces à faible probabilité.

1-6-La relation entre la menace, la vulnérabilité et l'impact :

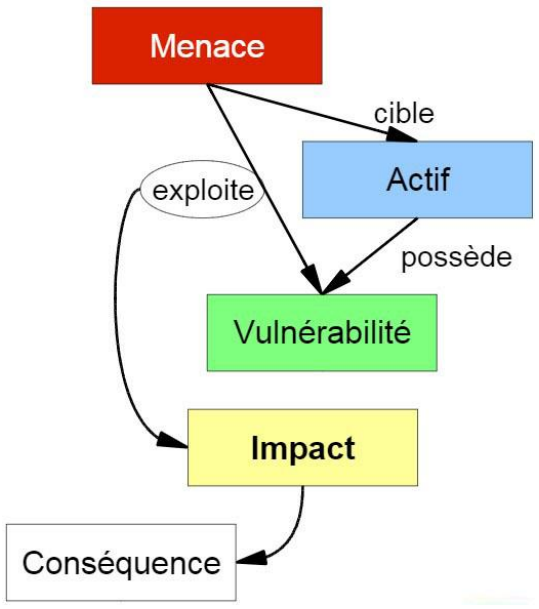


Le risque est généralement caractérisé par :

1. Source ou origine :
   Employé malveillant, employé non sensibiliser, ...
2. Menace :
   Divulgation d'information confidentielle, coupure d'électricité, ...
3. Probabilité d'occurrence ou vraisemblance ou potentialité
   Durée et lieu d'occurrence, probabilité d'occurrence
4. Vulnérabilité : **ayant permis ce risque**
   Erreur de conception, erreur humaine, ...
5. Impact, conséquence ou préjudice

Indisponibilité du service, perte de marché ou d'image, ...

6. Mesure de sécurité ou protection ou contre-mesure pour s'en protéger :
   Contrôle d'accès, politique de sécurité, sensibilisation du personnel...



Le schéma suivant montre qu'il y a une possibilité qu'une **menace** aille exploiter une **vulnérabilité** d'un **actif** et ainsi causer un **impact**(conséquence) à l'organisation.

2- Identification des menaces, vulnérabilités, impact, probabilités et contrôles :

2-1-Identification des menaces :

Les menaces qui peuvent exploiter les vulnérabilités qu'on a déjà cités pour enfreindre la sécurité et porter préjudice à l'organisation sont :

Défaillance technique :

- Dysfonctionnement de système de réservation.
- Panne de matériel.

Catastrophes naturelles :

- Inondation.
- Tremblement de terre.

Actions non autorisées :

- Divulgation d'informations sensibles.
- Interférence humaine accidentelle (suppression des données...)

Menaces informatiques :

- Les attaques DDOS (Distributed Denial of Service).
- Les attaques XSS (Cross-Site Scripting).

Menace	Qualitative	Quantitative
Dysfonctionnement de système de réservation	✗	
Panne de matériel		✗
Inondation		✗
Tremblement de terre		✗
Divulgation d'informations sensibles	✗	
Interférence humaine accidentelle (suppression des données...)	✗	

Les attaques DDOS	✗	
Les attaques XSS	✗	

2-2-Identification des vulnérabilités :

Dans notre étude du service de réservation de biller en ligne de la RAM, on a trouvé plusieurs vulnérabilités que les menaces peuvent les exploiter. Parmi ces vulnérabilités :

- Dysfonctionnement des systèmes développés en interne.
- Software Erreur.
- Les dossiers archivés sont stockés au rez-de-chaussée ou au sous-sol.
- La salle des serveurs est au rez-de-chaussée.
- Classification inappropriée des informations.
- Manque de vérification en amont du type de trafique (normal ou Robot).
- Manque des logiciels de sécurité.
- Manque des sauvegardes régulières du site WEB.
- Manque des logiciels anti-virus sur les ordinateurs des employés.
- Non-usage des navigateurs sécurisés.
- Absence Firewall.

2-3-Déterminons la probabilité d'un incident :

Évaluons la probabilité qu'une vulnérabilité soit effectivement exploitée, en tenant compte du type de vulnérabilité, des capacités et de la motivation de la source de menace, ainsi que de l'existence et de l'efficacité de vos contrôles.

De nombreuses organisations utilisent les catégories élevées, moyenne et faible.

Menace	**Vulnérabilité**	**Degré de possibilité d'exploitation**	**Pourquoi cette degré**
Dysfonctionnement de système de réservation	Software Erreur.	ELEVEE	Lancement du site sans vérifier sa sécurité
Panne de matériel	Dysfonctionnement des systèmes développés en interne.		Il existe un plan de maintenance. La société a processus de développement de qualité
	Loss of Power	MOYEN	
Inondation	Les dossiers archivés sont stockés au rez-de-chaussée ou au sous-sol.	FAIBLE	La dernière inondation/ Tremblement de terre a eu lieu dix ans auparavant dans la région.
Tremblement de terre	The server room is on high floors.		
Divulgation d'informations sensibles	Classification inappropriée des informations	FAIBLE	Les employées sont déjà formées de l'importance de faire attention au cours de

			traiter les informations importantes.
Interférence humaine accidentelle (suppression des données...)	Accidental or Irresponsible Actions of Employees (suppression des dossiers…)		
Les attaques DDOS	Manque de vérification en amont du type de trafique (normal ou Robot).	MOYEN	Une attaque DDoS est découverte tous les deux ans.
	Manque des logiciels de sécurité.		
	Manque des sauvegardes régulières du site WEB.		
Les attaques XSS	Manque des logiciels anti-virus sur les ordinateurs des employés.	ELEVEE	Manque des outils de protection contre les attaques XSS
	Non-usage des navigateurs sécurisés.		
	Absence Firewall.		

2-4- Évaluation de l'impact potentiel d'une menace :

Une analyse d'impact doit inclure les facteurs suivants :

- La mission du système, y compris les processus mis en œuvre par le système
- La criticité du système, déterminée par sa valeur et celle des données pour l'organisation
- La sensibilité du système et de ses données

Menace	Impact	Degré de criticité
Dysfonctionnement de système de réservation	Interruption des activités.	MOYEN
Panne de matériel	Tous les services (site Web…) Seront indisponibles pendant au moins une semaine.	CRITIQUE
	Dommages aux équipements électroniques de l'entreprise.	MOYEN
Inondation	Augmentation des coûts de fonctionnement.	MOYEN
	Dommages physiques aux locaux et aux	MOYEN

	équipements de l'entreprise.	
Tremblement de terre	Tous les services seront indisponibles.	CRITIQUE
Divulgation d'informations sensibles	Des données critiques seront peut-être perdues, mais pourront presque certainement être restaurées depuis une sauvegarde	FAIBLE
Interférence humaine accidentelle (suppression des données...)		
Les attaques DDOS	Les ressources du site Web seront indisponibles.	CRITIQUE
	Perte de confiance des clients	CRITIQUE
Les attaques XSS	Voler des informations sensibles des utilisateurs (des identifiants de connexion, des données financières).	CRITIQUE
	Exécuter des actions malveillantes au nom de l'utilisateur.	CRITIQUE

2.5.

Evaluation des risques

Lors de notre audit, ce sont les risques qu'on a trouvés :

- Des retards de production, critique négative.
- Mauvaise réputation.
- Perte de temps.
- Perte d'argent.
    - Perte potentielle de 45 000 € par occurrence.
    - Pertes de revenus ou des coûts supplémentaires liés à la réparation ou au remplacement du matériel en panne.
    - Perte d'un potentielle de 8 900 € par heure d'indisponibilité.

- Perte de confiance donc perte de clients.
- Poursuite judiciaire.

Apres l'évaluation des impacts et des possibilités, on va se baser sur ce tableau pour déterminer le degré du danger pour les risques :

Likelihood	Likely (3)	3	4	5
	Occasional (2)	2	3	4
	Unlikely (1)	1	2	3
		Insignificant (1)	Medium (2)	High Impact (3)
		Impact		

Menace	Risk	Level
Dysfonctionnement de système de réservation	Perte potentielle de 45 000 € par occurrence.	4
	Des retards de production, critique négative Donc une Mauvaise réputation. Perte de temps et d'argent	4

Panne de matériel	Perte de temps et d'argent	**3**
Inondation	Pertes de revenus ou des coûts supplémentaires liés à la réparation ou au remplacement du matériel en panne.	**2**
Tremblement de terre		**3**
Divulgation d'informations sensibles	Les employées sont déjà formées de l'importance de faire attention au cours de traiter les informations importantes.	**1**
Interférence humaine accidentelle (suppression des données...)		
Les attaques DDOS	Perte d'argent : Perte d'un potentielle de 8 900 € par heure d'indisponibilité	**4**
Les attaques XSS	Perte de confiance de nos clients et perte d'argent	**5**

2-6-Documentation des résultats

Type de menace	Menace	Vulnérabilité	Impact	Impact scale	Probabilités	Probabilité scale	Risk	Risk level
Défaillance technique	Panne de matériel	Dysfonctionnement des systèmes développés en interne.	Tous les services (site Web…) Seront indisponibles pendant au moins une semaine	**3**	Il existe un plan de maintenance. La société a processus de développement de qualité.	**2**	Des retards de production, critique négative Donc une Mauvaise réputation	**4**
		Loss of Power	Dommages aux équipements électroniques de l'entreprise.	**2**			Perte de temps et d'argent	**3**
	Dysfonctionnement de système de réservation	Software Erreur.	Interruption des activities.	**2**	Lancement du site sans vérifier sa sécurité	**3**	Perte potentielle de 45 000 € par occurrence.	**4**
Désastre naturel	Inondation	Les dossiers archivés sont stockés au rez-de-chaussée ou au sous-sol.	Augmentation des coûts de fonctionnement. Dommages physiques aux locaux et aux équipements de l'entreprise.	**2**	La dernière inondation/ Tremblement de terre a eu lieu dix ans auparavant dans la région.	**1**	Pertes de revenus ou des coûts supplémentaires liés à la réparation ou au remplacement du matériel en panne.	**2**
	Tremblement de terre	The server room is on high floors.	Tous les services seront indisponibles.	**3**		**1**		**3**
Actions non Autorisées	Disclosure of sensitive information	Classification inappropriée des informations.	Des données critiques seront peut-être perdues, mais pourront presque certainement être restaurées depuis une sauvegarde	**1**	Les employées sont déjà formées de l'importance de faire attention au cours de traiter les informations importantes.	**1**	Perte de confiance donc perte de clients, Mauvaise réputation Poursuite judiciaire	**1**
	Interference humaine accidentelle	Accidental or Irresponsible Actions of Employees (suppression des dossiers…)						
Menaces Informatiques	Les attaques DDOS	Manque de vérification en amont du type de trafique (normal ou Robot). Manque des logiciels de sécurité. Manque des sauvegardes régulières du site WEB.	Les ressources du site Web seront indisponibles. Perte de confiance des clients	**3**	Une attaque DDoS est découverte tous les deux ans.	**2**	Perte d'argent : Perte d'un potentielle de 8 900 € par heure d'indisponibilité	**4**
	Les attaques XSS	Manque des logiciels anti-virus sur les ordinateurs des employés. Non-usage des navigateurs sécurisés. Absence Firewall.	Voler des informations sensibles des utilisateurs (des identifiants de connexion, des données financières). Exécuter des actions malveillantes au nom de l'utilisateur.	**3**	Manque des outils de protection contre les attaques XSS	**3**	Perte de confiance de nos clients et perte d'argent	**5**

V. Statement Of Applicability

Objet :

Évaluation de l'applicabilité de la réglementation relative à la protection des données personnelles pour le site de vente de billets de voyage en ligne de la RAM.

Introduction :

La RAM est une entreprise qui propose à ses clients la possibilité de réserver et acheter des billets de voyage en ligne. En tant qu'entreprise qui traite des données personnelles de ses clients, la RAM est soumise à la réglementation relative à la protection des données personnelles alors elle doit respecter un ensemble de mesures de sécurité, dans ce qui suit nous essayons d'étudier le niveau de sécurité de cette entreprise.

Objectif :

Le présent rapport a pour objet de déterminer si l'entreprise est soumise aux mesures de l'annexe A de ISO27001, et de décrire les mesures de conformité mises en place par la RAM.

Méthodologie :

Pour réaliser cette évaluation, nous avons procédé de la manière suivante : Nous avons étudié les activités de la RAM au niveau de leur site et les types de données personnelles qu'elle traite. Nous avons examiné les règles de protection des données de l'entreprise et les mesures de sécurité mises en place pour protéger ces données. Nous avons évalué la conformité de l'entreprise à l'annexe A de ISO27001 en comparant les mesures mises en place par l'entreprise aux les exigences de l'annexe A qui fournit une liste de mesures de sécurité qui peuvent être mises en place pour protéger les informations et les systèmes de l'organisation. Ces mesures couvrent différents domaines, tels que la gestion de la sécurité de l'information, les contrôles de sécurité physique et logique, la gestion des incidents de sécurité, la gestion des communications et des opérations de sécurité, et la gestion des accès à l'information.

Voici les contrôles de l'annexe A de la norme ISO/CEI 27001 :

Annexe A.5 - Politiques de sécurité de l'information

L'annexe A.5.1 concerne la direction de la gestion pour la sécurité de l'information. L'objectif de cette annexe est de gérer la direction et le soutien pour la sécurité de l'information conformément aux exigences de l'organisation.

Annexe A.6 - Organisation de la sécurité de l'information

L'annexe A.6.1 concerne l'organisation interne. L'objectif de cette annexe est de mettre en place un cadre de gestion pour initier et contrôler la mise en œuvre et le fonctionnement de la sécurité de l'information dans l'organisation.

L'annexe A.6.2 concerne les appareils mobiles et le télétravail. L'objectif de cette annexe est de mettre en place un cadre de gestion pour assurer la sécurité du télétravail et de l'utilisation des appareils mobiles.

Annexe A.7 - Sécurité des ressources humaines

L'annexe A.7.1 concerne avant l'emploi. L'objectif de cette annexe est de s'assurer que les employés et les prestataires comprennent leurs responsabilités et sont adaptés aux rôles pour lesquels ils sont considérés.

L'annexe A.7.2 - l'objectif de cette annexe est de s'assurer que les employés et les prestataires sont conscients de leurs responsabilités en matière de sécurité de l'information et les respectent pendant l'emploi.

L'annexe A.7.3 concerne la fin et le changement d'emploi. L'objectif de cette annexe est de protéger les intérêts de l'organisation dans le processus de changement et de fin d'emploi.

Annexe A.8 - Gestion des actifs

L'annexe A.8.1 concerne la responsabilité des actifs. L'objectif de l'annexe est de déterminer les actifs de l'information inclus dans le système de gestion et de définir les responsabilités de protection appropriées.

L'annexe A.8.2 concerne la classification de l'information. L'objectif de cette annexe est de s'assurer que l'information reçoit un niveau de protection approprié en fonction de son importance pour l'organisation (et les parties intéressées telles que les clients).

L'annexe A.8.3 concerne la gestion des supports. L'objectif de cette annexe est d'empêcher toute divulgation, modification, suppression ou destruction non autorisée de l'information stockée sur les supports.

Annexe A.9 - Contrôle d'accès

L'annexe A.9.1 concerne les exigences commerciales du contrôle d'accès. L'objectif de cette annexe est de limiter l'accès à l'information et aux installations de traitement de l'information.

L'annexe A.9.2 concerne la gestion de l'accès des utilisateurs. L'objectif de ce contrôle de l'annexe A est de s'assurer que les utilisateurs sont autorisés à accéder aux systèmes et aux services, ainsi qu'à empêcher tout accès non autorisé.

L'annexe A.9.3 concerne les responsabilités des utilisateurs. L'objectif de ce contrôle de l'annexe A est de rendre les utilisateurs responsables de la protection de leurs informations d'authentification.

L'annexe A.9.4 concerne le contrôle d'accès aux systèmes et aux applications. L'objectif de cette annexe est d'empêcher tout accès non autorisé aux systèmes et aux applications.

Annexe A.10 - Cryptographie

L'annexe A.10.1 concerne les contrôles cryptographiques. L'objectif de cette annexe est de garantir une utilisation adéquate et efficace de la cryptographie pour protéger la confidentialité, l'authenticité et/ou l'intégrité de l'information.

Annexe A.11 - Sécurité physique et environnementale

L'annexe A.11.1 concerne la mise en sécurité de zones physiques et environnementales. L'objectif de cette annexe est d'empêcher tout accès physique non autorisé, tout dommage et toute interférence aux installations de traitement de l'information et de l'information de l'organisation.

L'annexe A.11.2 concerne l'équipement. L'objectif de ce contrôle de l'annexe est d'empêcher la perte, le dommage et le vol ou la compromission des actifs et l'interruption des opérations de l'organisation.

Annexe A.12 - Sécurité des opérations

L'annexe A.12.1 concerne les procédures opérationnelles et les responsabilités. L'objectif de cette zone de l'annexe A est de garantir des opérations correctes et sécurisées des installations de traitement de l'information.

L'annexe A.12.2 concerne la protection contre les logiciels malveillants. L'objectif ici est de s'assurer que l'information et les installations de traitement de l'information sont protégées contre les logiciels malveillants.

L'annexe A.12.3 concerne la sauvegarde. L'objectif ici est de protéger contre la perte de données.

L'annexe A.12.4 concerne l'enregistrement et le suivi. L'objectif de cette zone de l'annexe A est d'enregistrer les événements et de générer des preuves.

L'annexe A.12.5 concerne le contrôle du logiciel opérationnel. L'objectif de cette zone de l'annexe A est de garantir l'intégrité des systèmes opérationnels.

L'annexe A.12.6 concerne la gestion des vulnérabilités techniques. L'objectif de ce contrôle de l'annexe A est d'empêcher l'exploitation des vulnérabilités techniques.

L'annexe A.12.7 concerne les systèmes d'information et les considérations d'audit. L'objectif de cette zone de l'annexe A est de minimiser l'impact des activités d'audit sur les systèmes opérationnels.

Annexe A.13 - Sécurité des communications

L'annexe A.13.1 concerne la gestion de la sécurité du réseau. L'objectif de cette annexe est de garantir la protection de l'information dans les réseaux et ses installations de traitement de l'information de soutien.

L'annexe A.13.2 concerne le transfert d'information. L'objectif de cette annexe est de maintenir la sécurité de l'information transférée au sein de l'organisation et avec toute entité externe, par exemple un client, un fournisseur ou toute autre partie intéressée.

Annexe A.14 - Acquisition, développement et maintenance de systèmes

L'annexe A.14.1 concerne les exigences de sécurité des systèmes d'information. L'objectif de cette zone de l'annexe est de s'assurer que la sécurité de l'information fait partie intégrante des systèmes d'information sur tout leur cycle de vie. Cela inclut également les exigences pour les systèmes d'information qui proposent des services sur les réseaux publics.

Annexe A.15 - Relations avec les fournisseurs

L'annexe A.15.1 concerne la sécurité de l'information dans les relations avec les fournisseurs. L'objectif ici est de protéger les actifs précieux de l'organisation qui sont accessibles ou affectés par les fournisseurs.

L'annexe A.15.2 concerne la gestion du développement de services de fournisseurs. L'objectif de ce contrôle de l'annexe A est de s'assurer que le niveau convenu de sécurité de l'information et de prestation de services est maintenu en conformité avec les accords de fournisseurs.

L’information

L'annexe A.16.1 concerne la gestion des incidents, événements et faiblesses de sécurité de l'information. L'objectif de cette zone de l'annexe est de garantir une approche cohérente et efficace du cycle de vie des incidents, événements et faiblesses.

Annexe A.17 - Aspects de la sécurité de l'information de la gestion de la continuité des activités

L'annexe A.17.1 concerne la continuité de la sécurité de l'information. L'objectif de ce contrôle de l'annexe A est que la continuité de la sécurité de l'information soit intégrée aux systèmes de gestion de la continuité des activités de l'organisation.

L'annexe A.17.2 concerne les redondances. L'objectif de ce contrôle de l'annexe A est de garantir la disponibilité des installations de traitement de l'information.

Annexe A.18 - Conformité

L'annexe A.18.1 concerne la conformité aux exigences légales et contractuelles. L'objectif est d'éviter les manquements aux obligations légales, statutaires, réglementaires ou contractuelles liées à la sécurité de l'information et à toutes les exigences de sécurité.

Résultats :

Après notre étude :

ANNEX A CONTROL	TITLE	CONTROL OBJECTIVE	CONTROL APPLIED?	DATE OF IMPLEMENTATION	DATE OF LAST ASSESSMENT
5	**INFORMATION SECURITY POLICIES**				
5,1	Management direction for information security	Provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.			
5.1.1	Policies for information security	A set of policies for information security shall be defined, approved by management, published, and communicated to all employees and relevant external parties.	Yes	01/03/2020	22/01/2022
5.1.2	Review of the policies for information security	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness	Yes	01/03/2020	22/01/2022
6	**ORGANIZATION OF INFORMATION SECURITY**				
6,1	Internal organization	Establish a management framework to initiate and control the implementation and operation of information security within the organization.			
6.1.1	Information security roles and responsibilities	All information security responsibilities shall be defined and allocated	Yes	01/03/2020	22/01/2022
6.1.2	Segregation of duties	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets	Yes	01/03/2020	22/01/2022
6.1.3	Contact with authorities	Appropriate contacts with relevant authorities shall be maintained	Yes	01/03/2020	22/01/2022
6.1.4	Contact with sepcial interest groups	Appropriate contacts with special interest groups or other specialist ssecurity forums and professional associations shall be maintained	Yes	01/03/2020	22/01/2022
6.1.5	Information security in project management	Information security shall be addressed in project management, regardless of the type of project.	Yes	01/03/2020	22/01/2022
6,2	Mobile devices and teleworking	Ensure the security of teleworking and the use of mobile devices.			

6.2.1	Mobile device policy	A policy and supporting security measures shall be adopted to manage the risks introduced by mobile devices	Yes	01/03/2020	22/01/2022
6.2.2	Teleworking	A policy supporting security measures shall be implemented to protect information accessed, processed, or stored at teleworking sites	Yes	01/03/2020	22/01/2022
7	**HUMAN RESOURCE SECURITY**				
7,1	Prior to employment	Ensure that employees and contractors understand their responsibilities and are suitable for the rules for which they are considered.			
7.1.1	Screening	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations, and ethics and shall be proportional to the business requirements, the classification of the information to be accessed, and the perceived risks	Yes	01/03/2020	22/01/2022
7.1.2	Terms and conditions of employement	The contractual agreements with employees and contractors shall state their and the organization's responsibilites for information security	Yes	01/03/2020	22/01/2022
7,2	During employment	Ensure that employees and contractors are aware of and fulfil their information security responsibilities.			
7.2.1	Management responsibilities	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization	Yes	01/03/2020	22/01/2022
7.2.2	Information security awareness, education, and training	All employees of the organization and relevant contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures as relevant to their job function	Yes	01/03/2020	22/01/2022
7.2.3	Disciplinary process	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach	Yes	01/03/2020	22/01/2022

7,3	Termination or change of employment	Protect the organization's interests as part of the process of changing or terminating employment.			
7.3.1	Termination of rchange of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor, and enforced	Yes	01/03/2020	22/01/2022
8	**ASSET MANAGEMENT**				
8,1	Responsibility for assets	Identify organizational assets and define appropriate protection responsibilities.			
8.1.1	Inventory of assets	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained	Yes	01/03/2020	22/01/2022
8.1.2	Ownership of assets	Assets maintained in the inventory shall be owned	Yes	01/03/2020	22/01/2022
8.1.3	Acceptable use of assets	Rules for the acceptable use of information and assets associated with information and information processing facilities shall be identified, documented, and implemented	Yes	01/03/2020	22/01/2022
8.1.4	Return of assets	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract, or agreement	Yes	01/03/2020	22/01/2022
8,2	Information classification	Ensure that information received an appropriate level of protection in accordance with its importance to the organization.			
8.2.1	Classification of information	Information shall be classified in terms of legal requirements, value, criticality, and sensitivitiy to unauthorized disclosure or modification	Yes	01/03/2020	22/01/2022
8.2.2	Labelling of information	An appropriate set of procedures for information labeling shall be developed and implemented in accordance with the information classification scheme adopted by the organization	Yes	01/03/2020	22/01/2022
8.2.3	Handling of assets	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization	Yes	01/03/2020	22/01/2022

8,3	Media handling	Prevent unauthorized disclosure, modification, removal or destruction of information stored on media.			
8.3.1	Management of removable media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization	Yes	01/03/2020	22/01/2022
8.3.2	Disposal of media	Media shall be disposed of securely when no longer required, using formal procedures	Yes	01/03/2020	22/01/2022
8.3.3	Physical media transfer	Media containing inforation shall be protected against unauthorized access, misuse, or corruption during transportation	Yes	01/03/2020	22/01/2022
9	**ACCESS CONTROL**				
9,1	Business requirements of access control	Limit access to information and information processing facilities.			
9.1.1	Access control policy	An access control policy shall be established, documented, and reviewed based on business and information security requirements	Yes	01/03/2020	22/01/2022
9.1.2	Access to networks and network services	Users shall only be provided with access to the network and network services that they have been specifically authorized to use	Yes	01/03/2020	22/01/2022
9,2	User access management	Ensure authorized user access and to prevent unauthorized access to systems and services.			
9.2.1	User registration and de-registration	A formal user registration and de-registration process shall be implemented to enable assignment of access rights	Yes	01/03/2020	22/01/2022
9.2.2	User access provisioning	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services	Yes	01/03/2020	22/01/2022
9.2.3	Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled	Yes	01/03/2020	22/01/2022
9.2.4	Management of secret authentication information of users	The allocation of secret authentication information shall be controlled through a formal management proces	Yes	01/03/2020	22/01/2022
9.2.5	Review of user access rights	Asset owners shall review users' access rights at regular intervals	Yes	01/03/2020	22/01/2022

9.2.6	Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract, or agreement, or adjusted upon change	Yes	01/03/2020	22/01/2022
9,3	User responsibilities	Make users accountable for safeguarding their authentication information.			
9.3.1	Use of secret authentication information	Users shall be required to follow the organization's practices in the use of secret authentication informatioin	Yes	01/03/2020	22/01/2022
9,4	System and application access control	Prevent unauthorized access to systems and applications.			
9.4.1	Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy	Yes	01/03/2020	22/01/2022
9.4.2	Secure log-on procedures	Where required by the access control policy, access to systems and applications shall be controlled by a secure log on procedure	Yes	01/03/2020	22/01/2022
9.4.3	Password management system	Password management systems shall be interactive and shall ensure quality passwords	Yes	01/03/2020	22/01/2022
9.4.4	Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled	Yes	01/03/2020	22/01/2022
9.4.5	Access control to program source code	Access to program source code shall be restricted	Yes	01/03/2020	22/01/2022
10	**CRYPTOGRAPHY**				
10,1	Cryptographic controls	Ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.			
10.1.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented	Yes	01/03/2020	22/01/2022
10.1.2	Key management	A policy on the use, protection, and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle	Yes	01/03/2020	22/01/2022
11	**PHYSICAL AND ENVIRONMENTAL SECURITY**				

11,1	Secure areas	Prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.			
11.1.1	Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilites	Yes	01/03/2020	22/01/2022
11.1.2	Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access	Yes	01/03/2020	22/01/2022
11.1.3	Securing offices, rooms and facilities	Physical security for offices, rooms, and facilities shall be designed and applied	Yes	01/03/2020	22/01/2022
11.1.4	Protecting against external end environmental threats	Physical protection gainst natural disasters, malicious attacks, or accidents shall be designed and applied	Yes	01/03/2020	22/01/2022
11.1.5	Working in secure areas	Procedures for working in secure areas shall be designed and appiled	Yes	01/03/2020	22/01/2022
11.1.6	Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized personsl could enter the premises shall be controlled, and if possible, isolation from information processing facilities to prevent unauthorized access	Yes	01/03/2020	22/01/2022
11,2	Equipment	Prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.			
11.2.1	Equipment siting and protection	Equipment shall be sited and protected to reduce risks of environmental threats and hazards, and opportunities for unauthorized acces	Yes	01/03/2020	22/01/2022
11.2.2	Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities	Yes	01/03/2020	22/01/2022
11.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference, or damage	Yes	01/03/2020	22/01/2022
11.2.4	Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity	Yes	01/03/2020	22/01/2022
11.2.5	Removal of assets	Equipment, information, or software shall not be taken off-site without prior authorization	Yes	01/03/2020	22/01/2022

11.2.6	Security of equipment and assets off-premises	Security shall be aplied to off-site assets taking into account the different risks of working outside the organization's premises	Yes	01/03/2020	22/01/2022
11.2.7	Secure disposal or reuse of equipment	All equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use	Yes	01/03/2020	22/01/2022
11.2.8	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection	Yes	01/03/2020	22/01/2022
11.2.9	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted	Yes	01/03/2020	22/01/2022
12	**OPERATIONS SECURITY**				
12,1	Operational procedures and responsibilities	Ensure correct and secure operations of information processing facilities.			
12.1.1	Documented operating procedures	Operating procedures shall be documented and made available to all users who need them	Yes	01/03/2020	22/01/2022
12.1.2	Change management	Changes to the organization, business processes, information processing facilities, and systems that affect information security shall be controlled	Yes	01/03/2020	22/01/2022
12.1.3	Capacity management	The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance	Yes	01/03/2020	22/01/2022
12.1.4	Separation of development, testing and operational environments	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment	Yes	01/03/2020	22/01/2022
12,2	Protection from malware	Ensure that information and information processing facilities are protected against malware.			
12.2.1	Controls against malware	Detection, prevention, and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness	Yes	01/03/2020	22/01/2022
12,3	Backups	Protect against loss of data.			

12.3.1	Information backup	Backup copies of information, software, and system images shall be taken and tested regularly in accordance with an agreed backup policy	Yes	01/03/2020	22/01/2022
12,4	Logging and monitoring	Record events and generate evidence.			
12.4.1	Event logging	Event logs recording user activities, exceptions, faults, and information security events shall be produced, kept, and regularly reviewed	Yes	01/03/2020	22/01/2022
12.4.2	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access	Yes	01/03/2020	22/01/2022
12.4.3	Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed	Yes	01/03/2020	22/01/2022
12.4.4	Clock synchronisation	The clocks of all relevant information processing systems within an organization or security domain shall be synchornized to a single reference time source	Yes	01/03/2020	22/01/2022
12,5	Control of operational software	Ensure the integrity of operational systems.			
12.5.1	Installation of software on operational systems	Procedures should be implemented to control the installation of software on operational systems	Yes	01/03/2020	22/01/2022
12,6	Technical vulnerability management	Prevent exploitation of technical vulnerabilities.			
12.6.1	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk	Yes	01/03/2020	22/01/2022
12.6.2	Restrictions on software installation	Rules governing the installation of software by users should be established and implemented	Yes	01/03/2020	22/01/2022
12,7	Information systems audit considerations	Minimize the impact of audit activities on operational systems.			
12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems should be carefully planned and agreed to minimize disruptions to business processes	Yes	01/03/2020	22/01/2022
13	**COMMUNICATIONS SECURITY**				

13,1	Network security management	Ensure the protection of information in networks and its supporting information processing facilities.			
13.1.1	Network controls	Networks shall be manged and controlled to protect information in systems and applications	Yes	01/03/2020	22/01/2022
13.1.2	Security of network services	Security mechanisms, service levels, and management requirements of all network services shall be identified and included in network service agreements, whether these services are provided in-house or outsourced	Yes	01/03/2020	22/01/2022
13.1.3	Segregation in networks	Groups of information services, users, and information systems shall be segregated on networks	Yes	01/03/2020	22/01/2022
13,2	Information transfer	Maintain the security of information transferred within an organization and with any external entity.			
13.2.1	Information transfer policies and procedures	Formal transfer policies, procedures, and controls shall be in plce to protect the transfer of information through the use of all types of communication facilities	Yes	01/03/2020	22/01/2022
13.2.2	Agreements on information transfer	Agreements shall address the secure transfer of business information between the organization and external parties	Yes	01/03/2020	22/01/2022
13.2.3	Electronic messaging	Information involved in electronic messaging shall be appropriately protected	Yes	01/03/2020	22/01/2022
13.2.4	Confidentiality or non-disclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed, and documented	Yes	01/03/2020	22/01/2022
14	**SYSTEM ACQUISITION, DEVELOPMENT, AND MAINTENANCE**				
14,1	Security requirements of information systems	Ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.			
14.1.1	Information security requirements analysis and specification	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems	Yes	01/03/2020	22/01/2022

14.1.2	Securing application services on public networks	Information involved in application services passing over pubic networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclousre and modification	Yes	01/03/2020	22/01/2022
14.1.3	Protecting application services transactions	Information involved in application service transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication, or replay	Yes	01/03/2020	22/01/2022
14,2	Security in development and support processes	Ensure that information security is designed and implemented within the development lifecycle of information systems.			
14.2.1	Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organization	Yes	01/03/2020	22/01/2022
14.2.2	System change control procedures	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures	Yes	01/03/2020	22/01/2022
14.2.3	Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impct on organization operations or security	Yes	01/03/2020	22/01/2022
14.2.4	Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled	Yes	01/03/2020	22/01/2022
14.2.5	Secure system engineering principles	Principles for engineering secure systems shall be established, documented, maintained, and applied to any information system implementation efforts	Yes	01/03/2020	22/01/2022
14.2.6	Secure development environment	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle	Yes	01/03/2020	22/01/2022
14.2.7	Outsourced development	The organization shall supervise and monitor the activity of outsourced system development	Yes	01/03/2020	22/01/2022
14.2.8	System security testing	Testing of security functionality shall be carried out during development	Yes	01/03/2020	22/01/2022

14.2.9	System acceptance testing	Acceptance testing programs and related criteria shall be established for new information systems, upgrades, and new verisons	Yes	01/03/2020	22/01/2022
14,3	Test data	Ensure the protection of data used for testing.			
14.3.1	Protection of test data	Test data shall be selected carefully, protected, and controlled	Yes	01/03/2020	22/01/2022
15	**SUPPLIER RELATIONSHIPS**				
15,1	Information security in supplier relationships	Ensure protection of the organization's assets that is accessible by suppliers.			
15.1.1	Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier access to the organization's assets shall be agreed on with the supplier and documented	Yes	01/03/2020	22/01/2022
15.1.2	Addressing security within supplier agreements	All relevant information security requirements should be established and agreed upon with each supplier that may access, process, store, communicate, or provide IT infrastructure components for the organization's information	Yes	01/03/2020	22/01/2022
15.1.3	Information and communication technology supply chain	Agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and product supply chains	Yes	01/03/2020	22/01/2022
15,2	Supplier service delivery management	Maintain an agreed level of information security and service delivery in line with supplier agreements.			
15.2.1	Monitoring and review of supplier services	Organizations should regularly monitor, review, and audit supplier service delivery	Yes	01/03/2020	22/01/2022
15.2.2	Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures, and controls, should be managed, taking account of the criticality of business information, systems, and processes involved and re-assessment of risks	Yes	01/03/2020	22/01/2022
16	**INFORMATION SECURITY INCIDENT MANAGEMENT**				

16,1	Management of information security incidents and improvements	Ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.			
16.1.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents	Yes	01/03/2020	22/01/2022
16.1.2	Reporting information security events	Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents	Yes	01/03/2020	22/01/2022
16.1.3	Reporting information security weaknesses	Information security events should be reported through appropriate management channels as quickly as possible	Yes	01/03/2020	22/01/2022
16.1.4	Assessment of and decision on information security events	Information security events should be assessed and it should be decided if they are to be classified as information security incidents	Yes	01/03/2020	22/01/2022
16.1.5	Response to information security incidents	Information security incidents should be responded to in accordance with the documented procedures	Yes	01/03/2020	22/01/2022
16.1.6	Learning from information security incidents	Knowledge gained from analyzing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents	Yes	01/03/2020	22/01/2022
16.1.7	Collection of evidence	The organization should define and apply procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence	Yes	01/03/2020	22/01/2022
17	**INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT**				
17,1	Information security continuity	Information security continuity shall be embedded in the organization's business continuity management systems.			
17.1.1	Planning information security continuity	The organization should determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster	Yes	01/03/2020	22/01/2022
17.1.2	Implementing information security continuity	The organization should establish, document, implement and maintain processes, procedures, and controls to ensure the required	Yes	01/03/2020	22/01/2022

		level of continuity for information security during an adverse situation			
17.1.3	Verify, review and evaluate information security continuity	The organization must verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during these situations	Yes	01/03/2020	22/01/2022
17,2	Redundancies	Ensure availability of information processing facilities.			
17.2.1	Availability of information processing facilities	Information processing facilities should be implemented with redundancy sufficient to meet availability requirements	Yes	01/03/2020	22/01/2022
18	**COMPLIANCE**				
18,1	Compliance with legal and contractual requirements	Avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.			
18.1.1	Identification of applicable legislation and contractual requirements	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements should be explicitly identified, documented and kept up to date for each information system and the organization	Yes	01/03/2020	22/01/2022
18.1.2	Intellectual property rights	Appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products	Yes	01/03/2020	22/01/2022
18.1.3	Protection of records	Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislator, regulatory, contractual and business requirements	Yes	01/03/2020	22/01/2022
18.1.4	Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information should be ensured as required in relevant legislation and regulation where applicable	Yes	01/03/2020	22/01/2022
18.1.5	Regulation of cryptographic controls	Cryptographic controls should be used in compliance with all	Yes	01/03/2020	22/01/2022

		relevant agreements, legislation and regulations			
18,2	Information security reviews	Ensure that information security is implemented and operated in accordance with the organizational policies and procedures.			
18.2.1	Independent review of information security	The organization’s approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) should be reviewed independently at planned intervals or when significant changes occur	Yes	01/03/2020	22/01/2022
18.2.2	Compliance with security policies and standards	Managers should regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements	Yes	01/03/2020	22/01/2022
18.2.3	Technical compliance review	Information systems should be regularly reviewed for compliance with the organization’s information security policies and standards	Yes	01/03/2020	22/01/2022

Conclusion :

D'après notre évaluation, le site de vente de billets de voyage en ligne de la RAM est soumis aux exigences de l’annexe A des mesures de sécurité.

VI. Processus de gestion des incidents :

La gestion des incidents concerne la prise en charge de tous les incidents informatiques tout au long de leurs cycles de vie.

Sa mission est d'assurer un fonctionnement normal des services conformément avec l'engagement pris contractuellement sur les niveaux de services garantis.

La mise en œuvre d'un processus de gestion des incidents est une étape incontournable pour :

-La réactivité : l'utilisateur peut joindre rapidement un technicien pour l'assister. Cela occasionnera moins de perte de temps pour l'utilisateur, mais aussi pour ses collègues qu'il ne dérange plus.

-L'efficacité du technicien : il ne sera plus dérangé au cours d'une activité planifiée.

-La capitalisation du savoir : si un incident a été enregistré, en cas de renouvellement de ce type d'incident, les techniciens du service savent ce qu'il convient de faire et gagneront du temps dans le traitement de l'incident.

-La prévention : il sera possible d'identifier correctement un incident mineur avant qu'il ne devienne critique et que cela aboutisse à une situation de crise.

La gestion des incidents selon le référentiel ITIL :

La gestion des incidents est un processus faisant partie du management des systèmes d'information parmi lesquels l'ensemble de bonnes pratiques ITIL1 (: Information Technology Infrastructure Library)

ITIL est un ensemble de bonnes pratiques, procédures et méthodes qui servent de lignes directrices pour l'amélioration de la gestion des services dans l'environnement informatique.

C'est en fonction de son organisation, de son activité, de sa taille et de ses objectifs stratégiques que l'entreprise mettra en œuvre, en partie ou en totalité, les processus décrits dans ITIL.

Les Bonnes pratiques ITIL :

De manière générale, les technologies de l'information peuvent être très complexes. Afin de gérer cette complexité, il est important de définir des processus clairs, consistants et bien définis.

ITIL permet d'identifier, d'améliorer et de documenter les processus mis en œuvre, ce qui peut résulter en une amélioration de l'organisation de l'entreprise.

ITIL regroupe un ensemble de bonnes pratiques largement répandues qui découlent de l'expertise et de l'expérience de ses contributeurs et membres de la communauté ITSM (Information Technology Service Management). Cela en fait un référentiel évolutif basé sur l'expérience pratique. Plus spécifiquement, ITIL est un recueil structuré de conseils et de recommandations orientés vers le service à la clientèle. Enfin, il est ouvert et s'intègre bien aux autres référentiels de l'industrie (CMMI, PMBOK, COBIT, etc.). Il est en quelque sorte le noyau de la gestion des services.

Objectif du processus de gestion des incidents :

Le but principal du processus de gestion des incidents est de « rétablir un service opérationnel aussi rapidement que possible en minimisant l'impact sur l'entreprise et en s'assurant que les niveaux de service et de disponibilité convenus soient maintenus ».

D'autres objectifs sont également à prendre en compte :

-S'assurer que des méthodes standardisées et des procédures sont utilisées afin de garantir une réponse.

-Augmenter la visibilité des incidents et la communication vers le métier.

-Maintenir la satisfaction du client en assurant une qualité des services des technologies de l'information. La gestion des incidents traite tous les incidents rapportés par les utilisateurs via le centre de service, le personnel technique et la surveillance technique. Les incidents peuvent apparaître au niveau :

Matériel :

-Poste de travail en panne, -

-Imprimante non opérationnelle,

-Ressource indisponible ou inaccessible,

-Alerte ou exception générée automatiquement par un composant du système.

Applicatif :

-Service non disponible,

-Dysfonctionnement d'une application,

-Demande d'assistance de la part des utilisateurs par rapports à un défaut de maitrise de certaines fonctionnalités applicatives.

Cycle de vie d'un incident :

Le traitement d'un incident se fait en plusieurs étapes. On parle régulièrement du cycle de vie d'un incident comme il est illustré dans la figure suivante ci-dessous. Les demandes de services, les requêtes et les événements sont traités via le centre de services et enregistrés dans le cadre du processus de gestion des incidents.

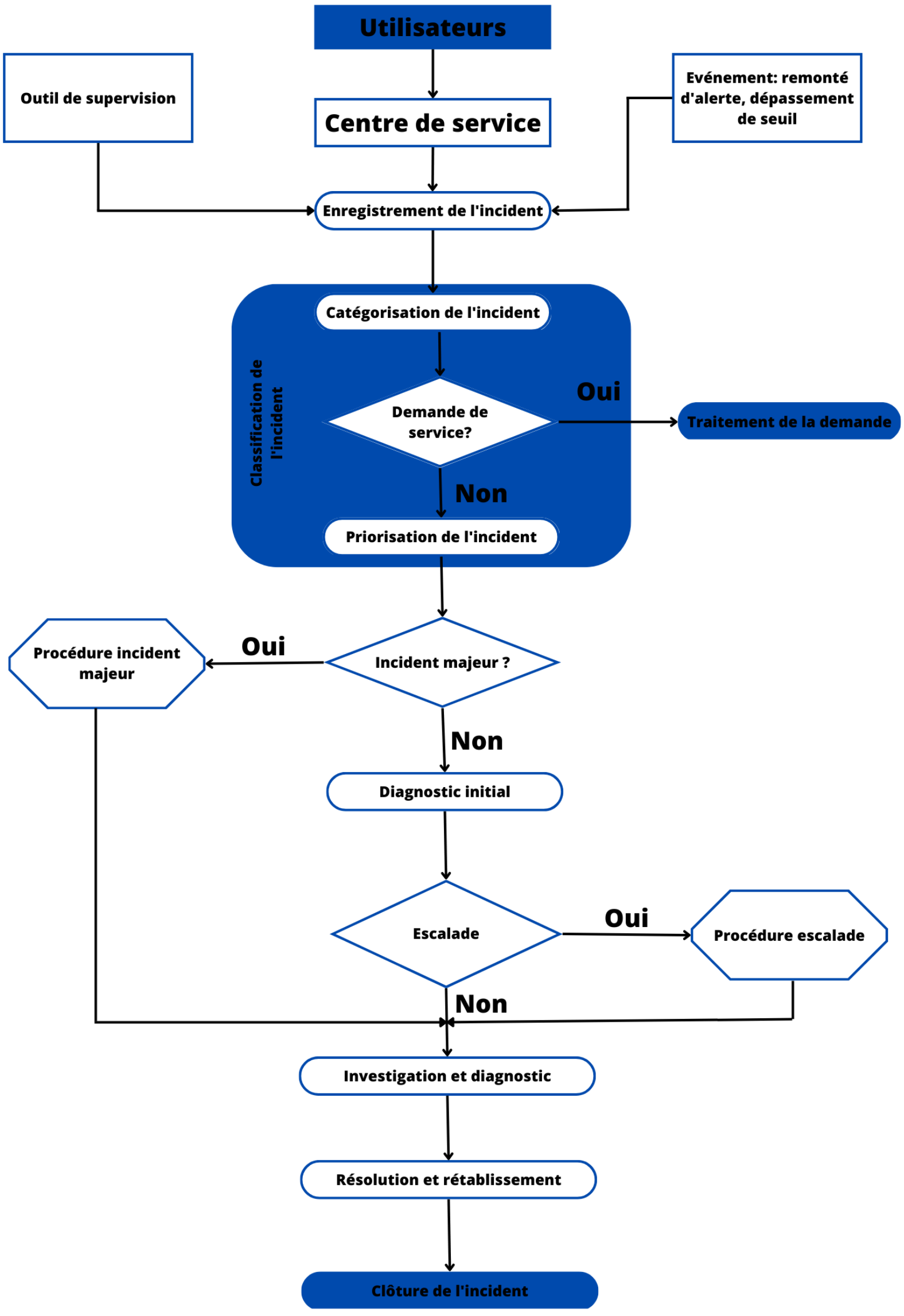


Figure (cycle de vie d’un incident)

Dans notre cas, la gestion des incidents de la RAM se basera sur la procédure d'escalade suivante :

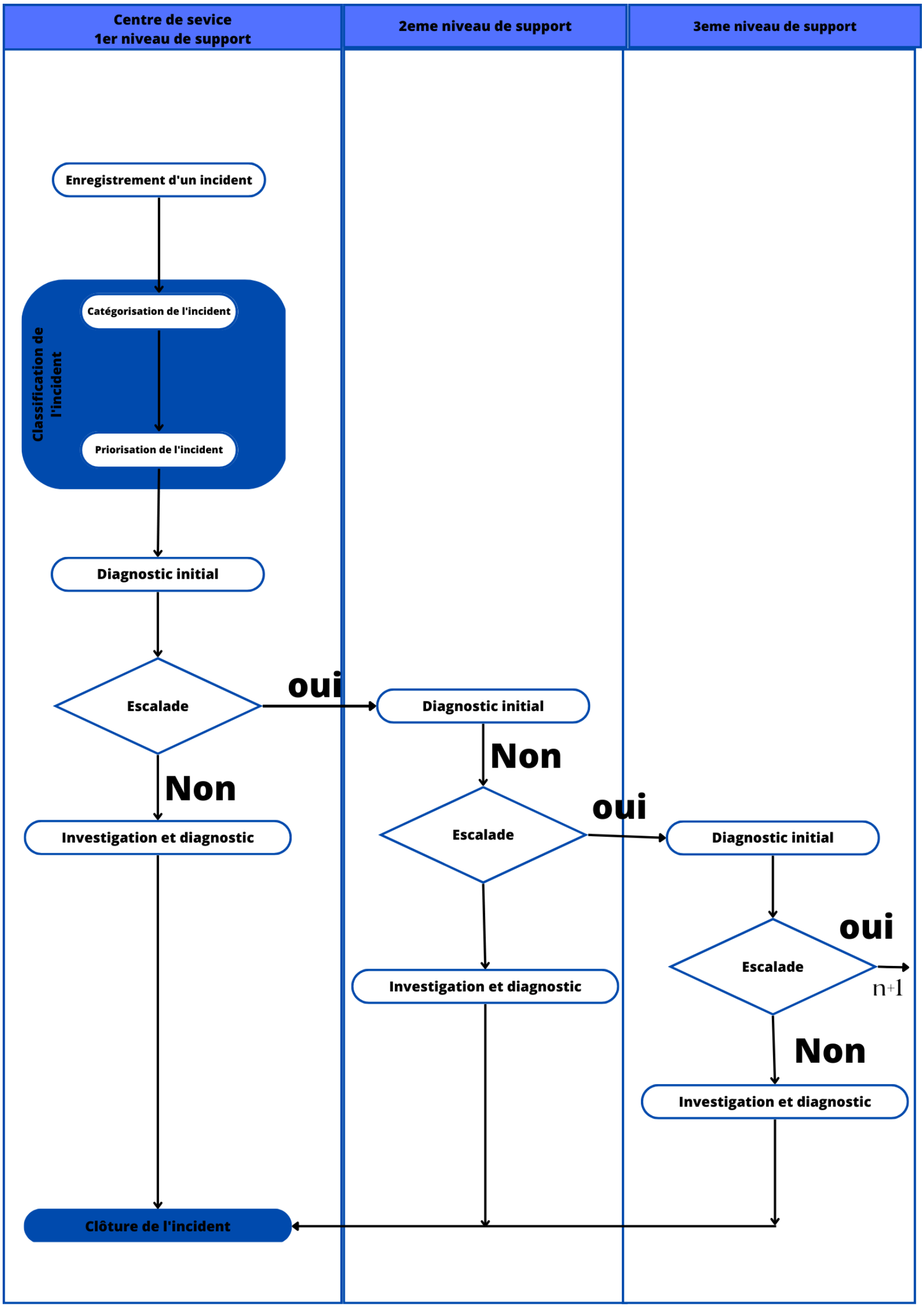


Figure (escalade d'incident)

Support de niveau 1 : centre de service sera géré par du personnel du centre d'appel qui se chargera de résoudre les incidents de premier ordre signalés par les utilisateurs du site ou les employés en internes qui auront des problèmes particulièrement basiques

Support de niveau de niveau 2 : composé de techniciens se chargeront de gérer les incidents dont le premier niveau n'arrivera pas à résoudre (notamment les incidents de panne du matériel)

Support de niveau 3 : composé d'ingénieurs en gestion et réponses d'incidents se chargeront de gérer les incidents majeurs et de hautes ampleur (notamment les attaques informatiques et des piratages des hackers)

Dans la pratique, il est nécessaire de prévoir des traitements d'exception car il n'est pas possible de conserver des incidents ouverts au-delà d'un certain délai.

Dans cette phase, le centre de services doit s'assurer que l'enregistrement des différentes actions réalisées pendant le traitement de l'incident a été correctement réalisé dans l'outil de gestion des incidents.

Etat d'un incident :

Depuis sa détection, l'incident va passer par des états successifs tout au long de son traitement.

----------Tableau de l'état d'un incident----------

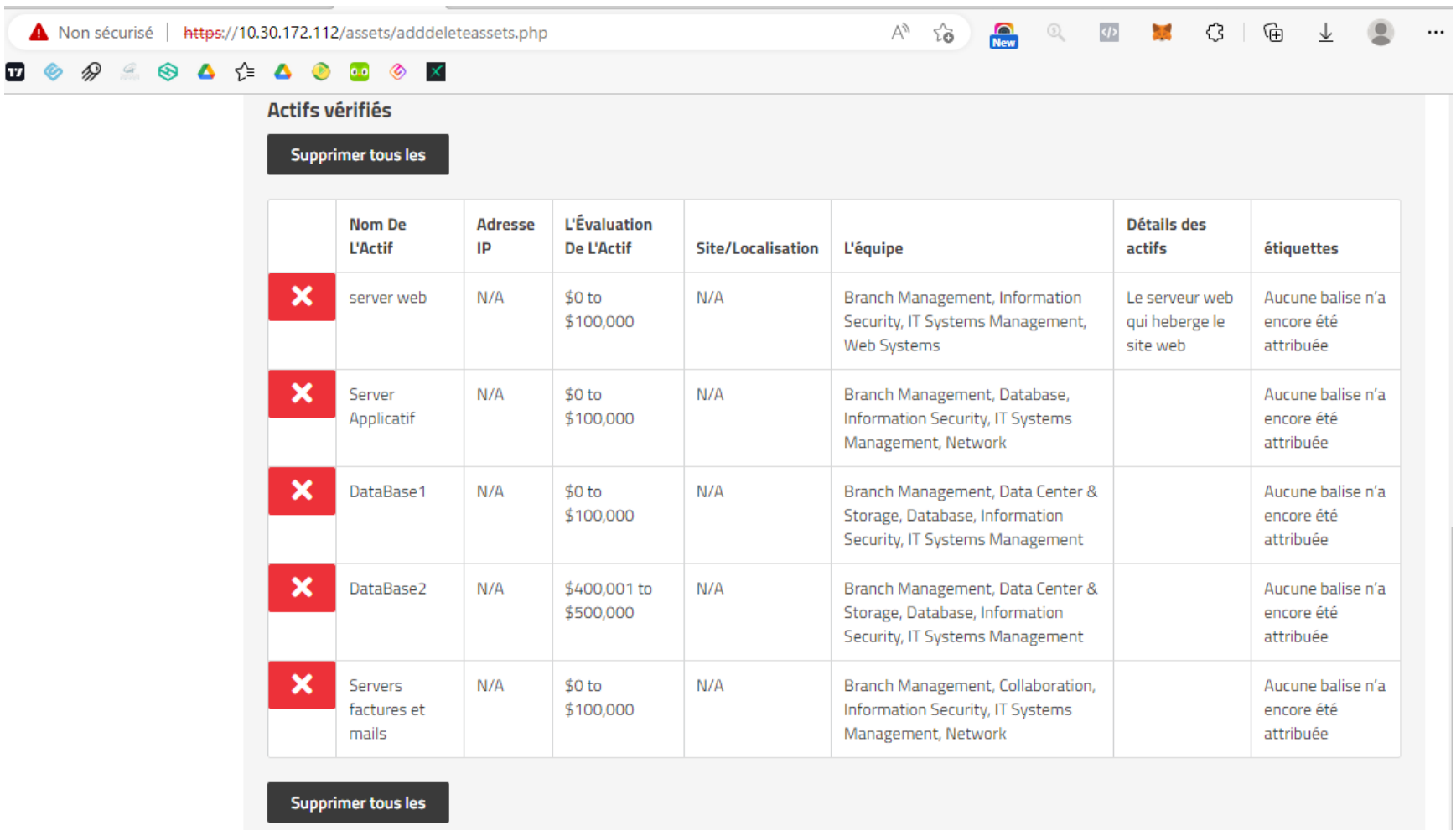
L'outil de gestion d'incident à mettre en place doit indiquer à tous les acteurs du processus de gestion des incidents (clients, technicien...) l'état d'avancement du traitement de l'incident. Pour notre société la RAM nous utiliserons l'outil simplerisk comme outil de gestion d'incident.

VII. L’outil simplerisk :

SimpleRisk est une plateforme GRC complète qui peut être utilisée pour tous vos besoins en matière de gouvernance, de gestion des risques et de conformité. Il offre des fonctionnalités suffisamment complètes pour être utilisées par certaines des plus grandes organisations de la planète tout en présentant une interface utilisateur si simple et intuitive qu'elle peut être utilisée par les personnes les moins techniques de l’organisation.

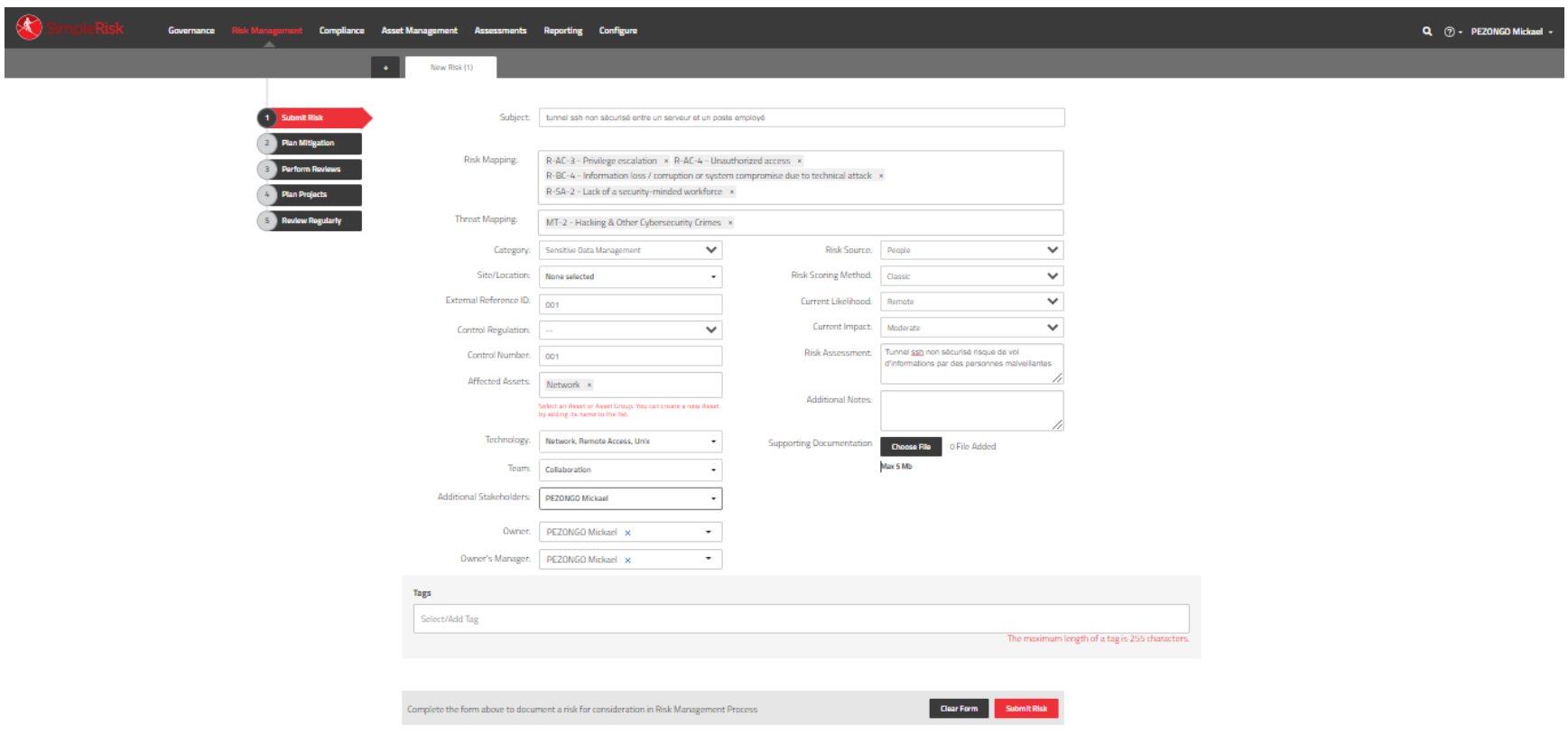
Enregistrement de nos actifs dans Simple Risk

Maintenant nous allons enregistrer l’ensemble de nos actifs sur simple risk afin de pouvoir les contrôler, les auditer et pouvoir gérer les risques liés à ces actifs. L’ensemble de nos actifs sont ceux citer dans la première partie de notre rapport. La capture suivante montre les actifs enregistrer sur simple risk

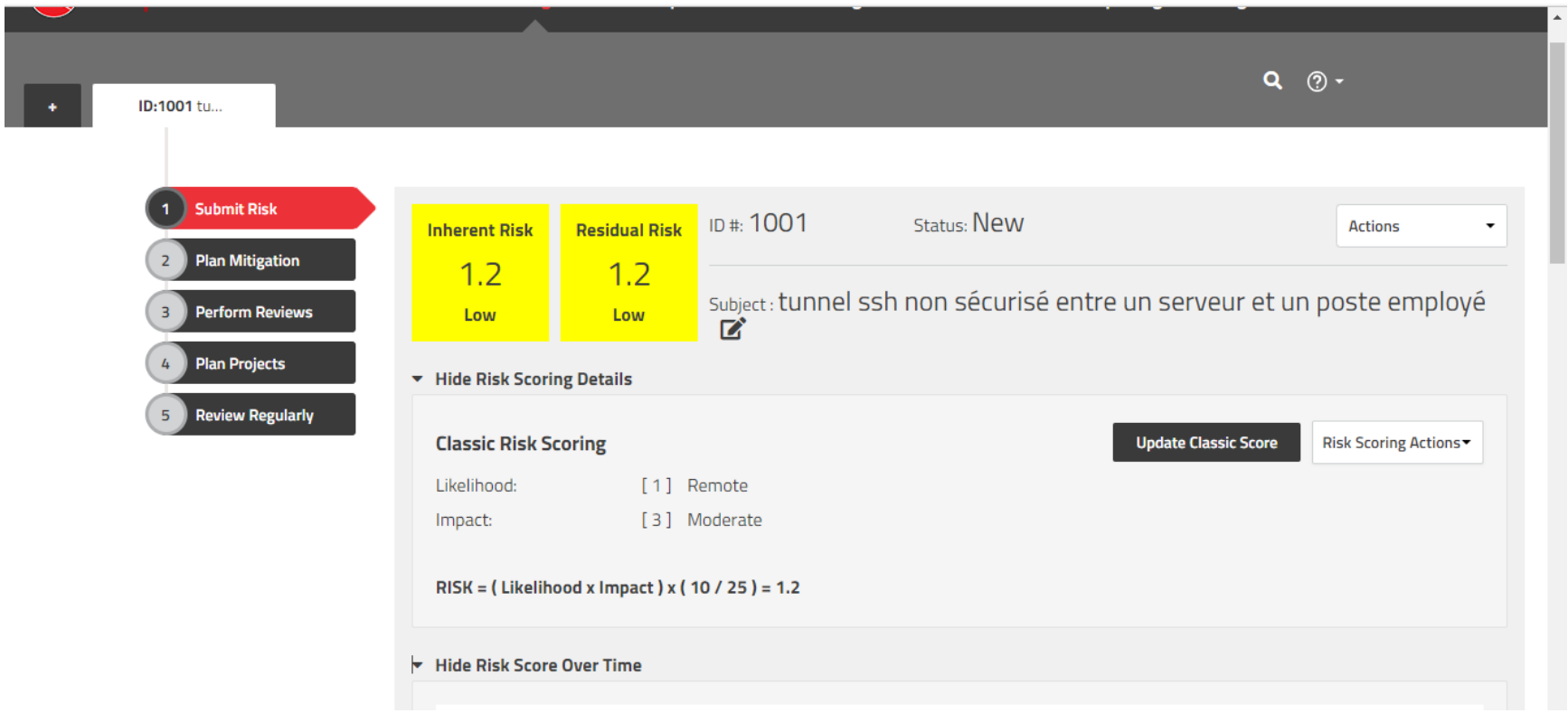


Simulation de la soumission d’un risque dans Simple Risk :

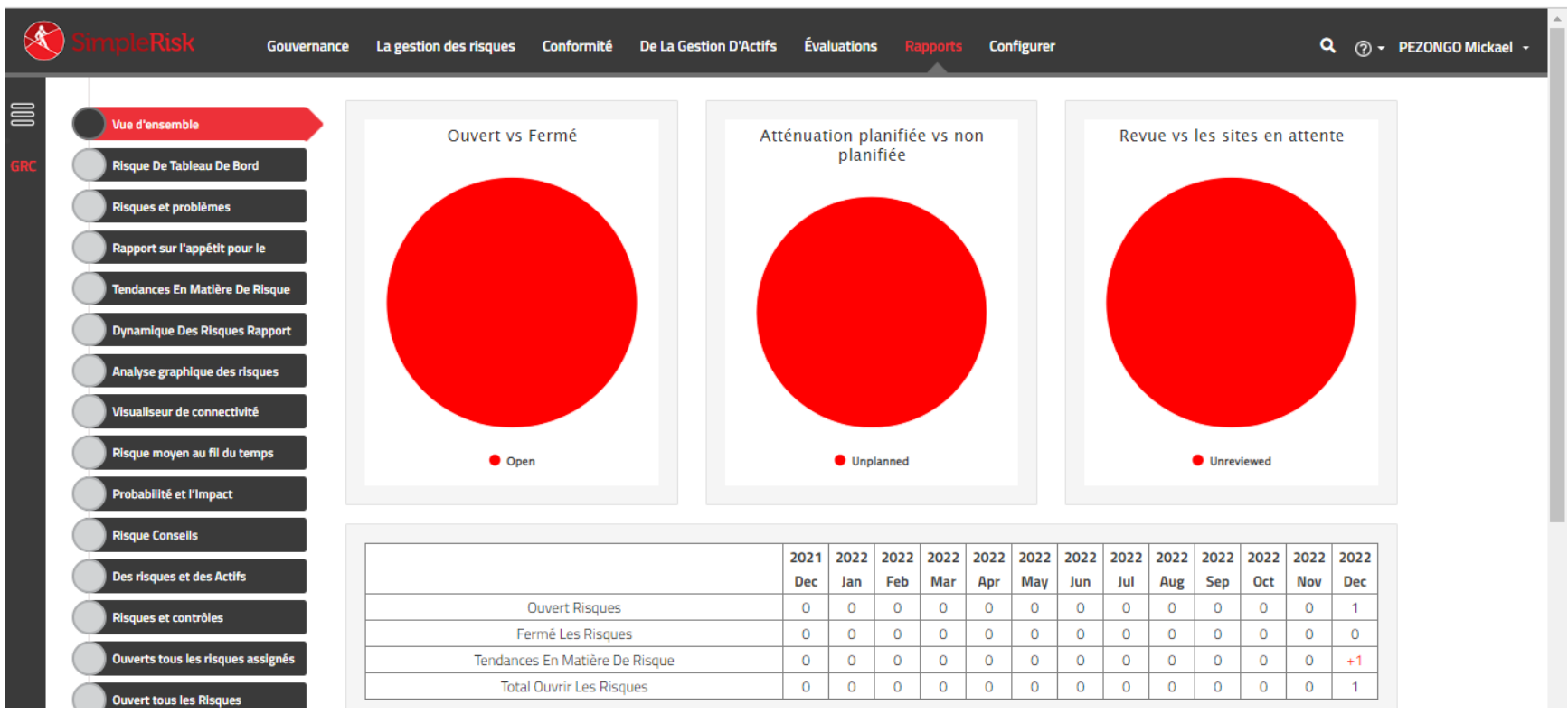
Pour la soumission d’un risque dans simplerisk, on enregistre les informations du risque comme dans la capture suivante :



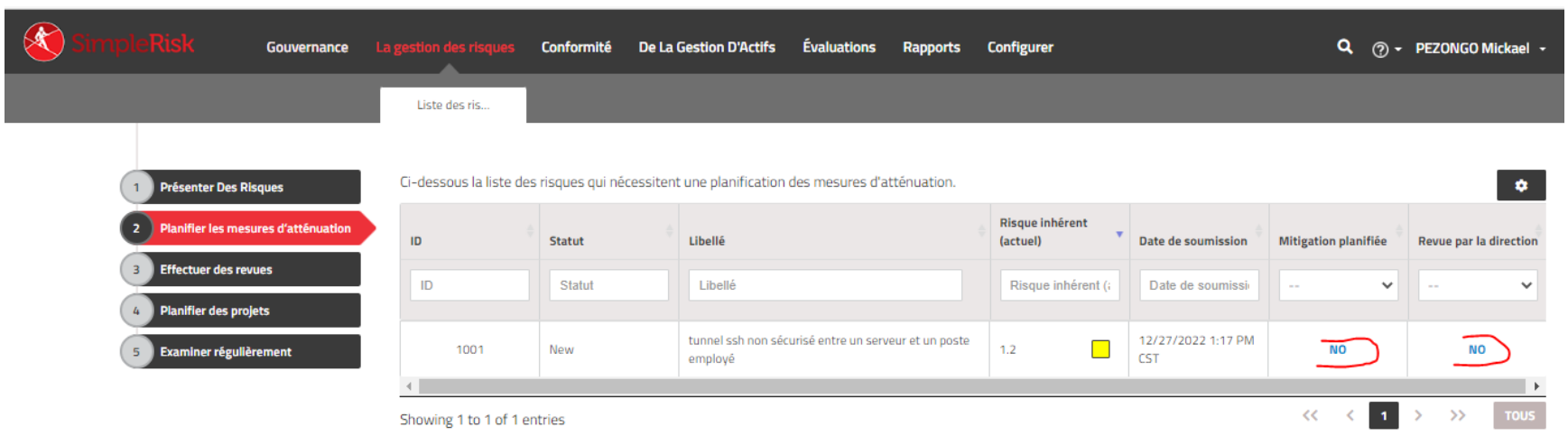
Ensuite à travers les informations rentrées, simple risk calcule lui le degré du risque comme nous pouvons le voir dans l’image ci-dessous :



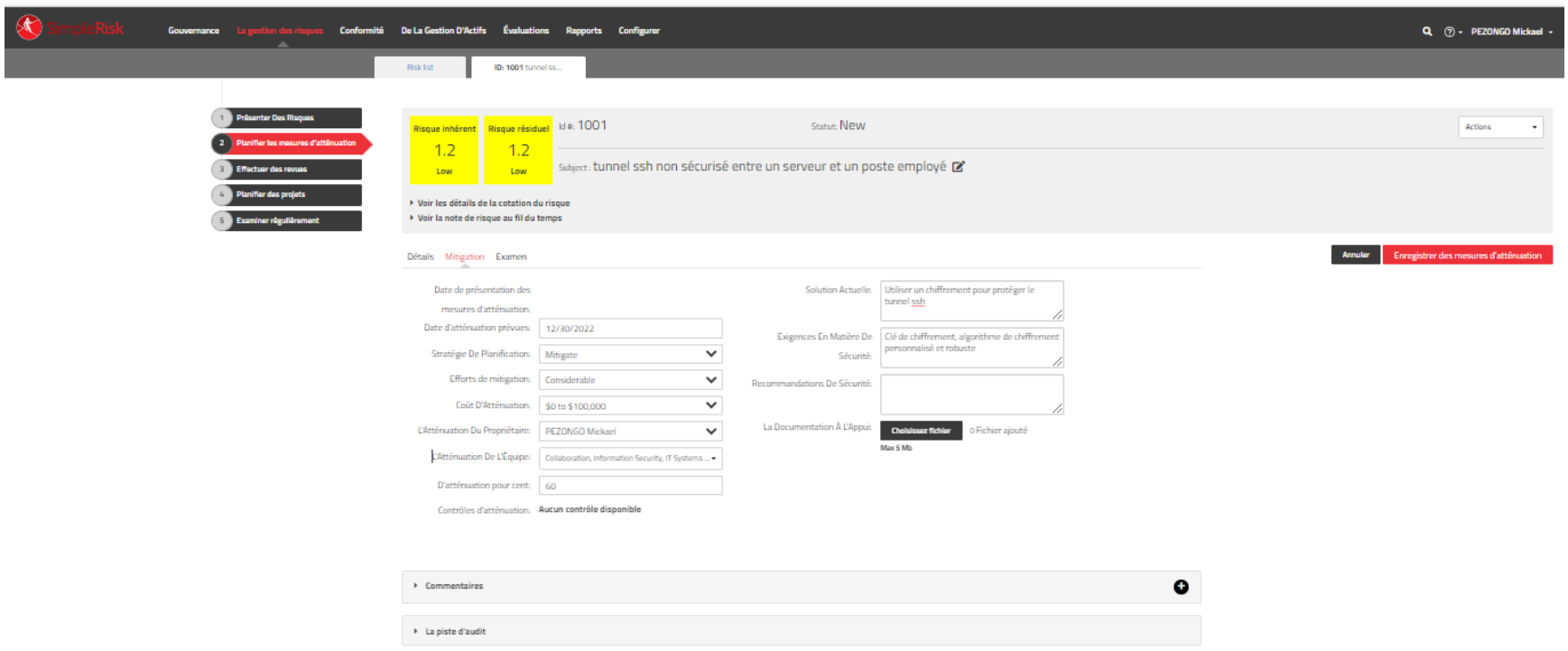
Dans rapport, nous pouvons voir qu'un y a u n risque ouvert mais non traité simple risk utilise la couleur rouge pour montrer qu'on a des risques non traités :



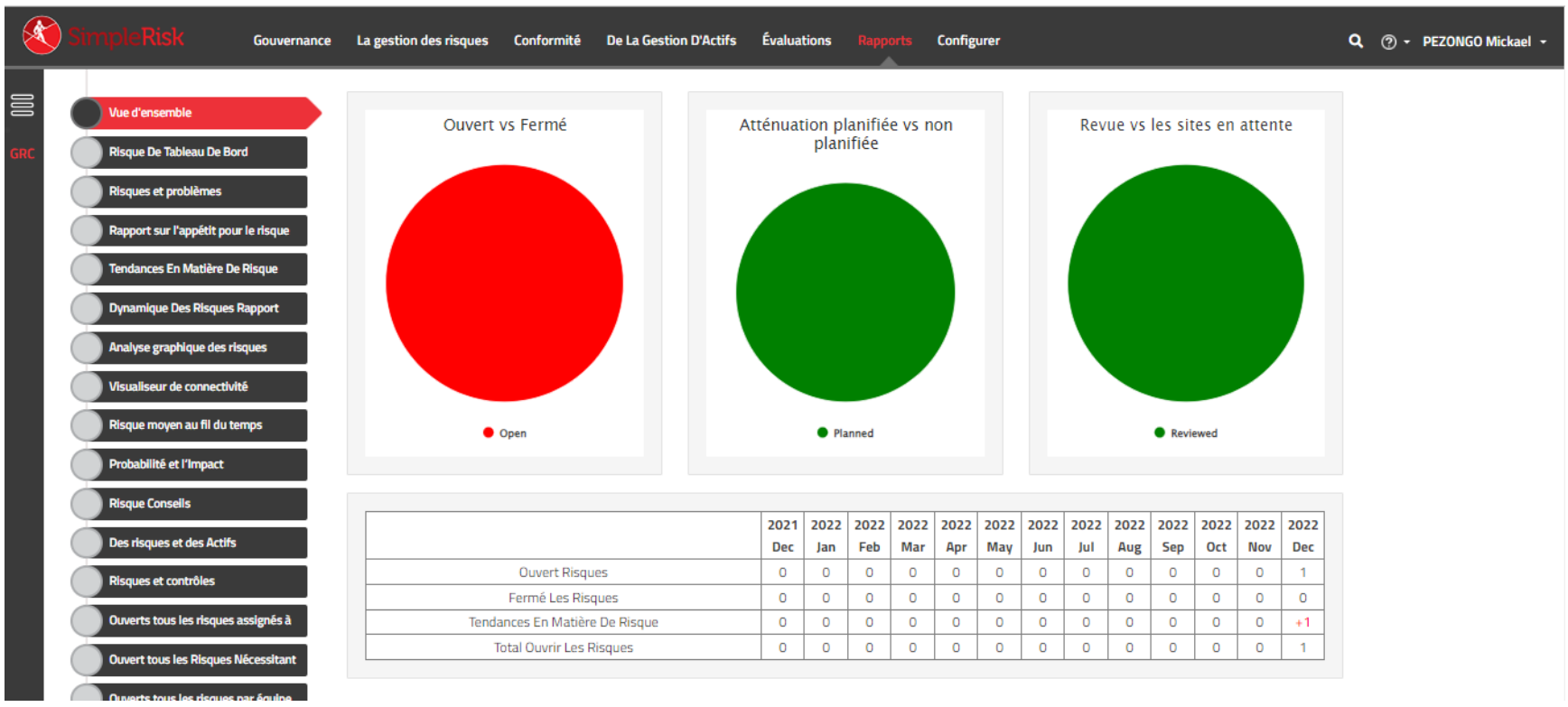
Dans gestion des risques, nous allons mettre en place un plan de mitigation de notre risque :



Pour mettre en place le plan de mitigation, nous devons remplir les champs suivants comme sur la capture qui suit :



Maintenant nus pouvons voir que dans rapports la gestion du risque est planifiée mais pas encore fermé :



	2021 Dec	2022 Jan	2022 Feb	2022 Mar	2022 Apr	2022 May	2022 Jun	2022 Jul	2022 Aug	2022 Sep	2022 Oct	2022 Nov	2022 Dec
Ouvert Risques	0	0	0	0	0	0	0	0	0	0	0	0	1
Fermé Les Risques	0	0	0	0	0	0	0	0	0	0	0	0	0
Tendances En Matière De Risque	0	0	0	0	0	0	0	0	0	0	0	0	+1
Total Ouvrir Les Risques	0	0	0	0	0	0	0	0	0	0	0	0	1