28/12/2023

Projet SSI :

Analyse de risques avec la méthode MEHARI

Réalisé par :

- **CHAHET SID ALI (20225214)**
- **SORO SOPEGUE YAYA (20216016)**

2023-2024

I- Contexte Métier

1- L'entreprise Château des Saveurs

L'entreprise **Château des Saveurs** est une pâtisserie qui souhaite se spécialiser dans la vente en ligne de produits de pâtisserie. Pour ce faire, elle envisage d'utiliser un système de gestion d'entreprise pour la recommandation de produits basée sur les préférences du client, l'optimisation des itinéraires de livraison pour réduire les délais, ou encore la gestion automatisée des stocks pour garantir la disponibilité des produits les plus demandés.
Le processus métier étudié est celui relatif à la vente/livraison de produits de pâtisserie via internet.

2- Charte d'organigramme

Château des Saveurs est une PME de 6 personnes.

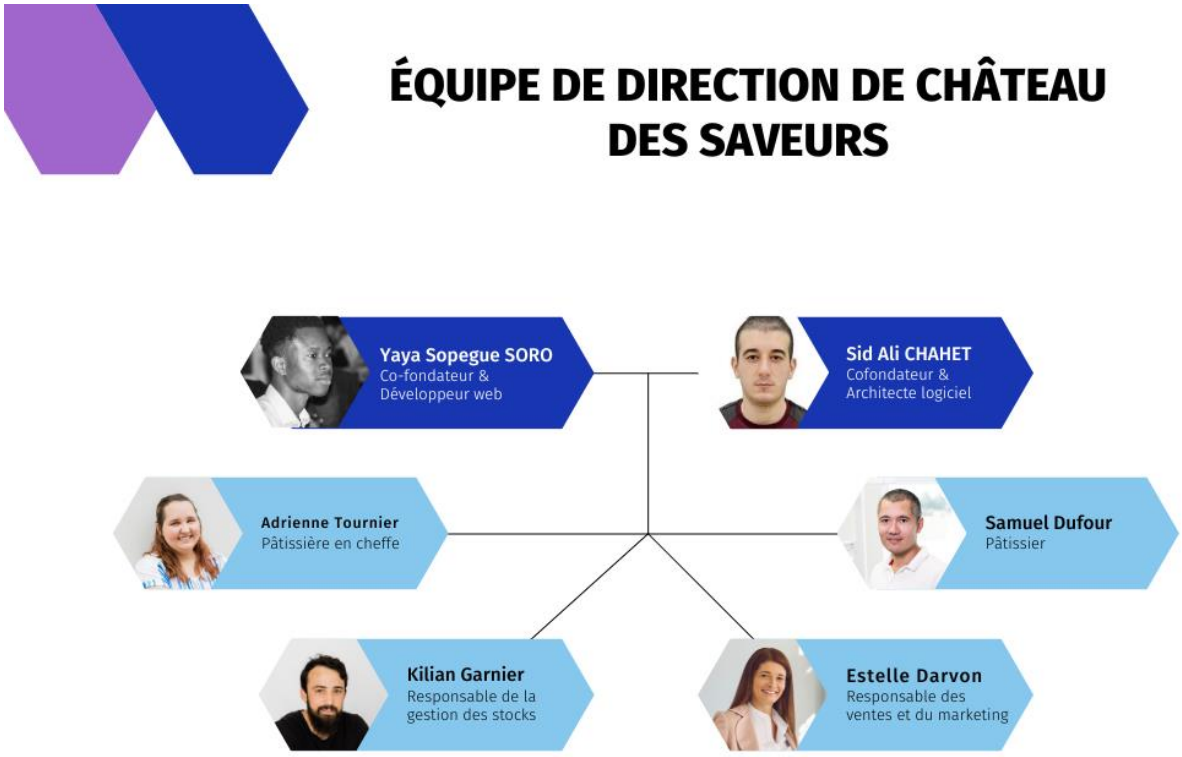


Fig. 1 : Organigramme de Chateau des saveurs

- **Cofondateur :** responsable de la création et de la gestion de l'entreprise**.**
- **Architecte logiciel :** conçoit les systèmes informatiques nécessaires à la gestion des opérations, de l'inventaire, et de la commande en ligne.
- **Pâtissier :** crée des délices sucrés en utilisant son expertise en cuisine pour confectionner des desserts exquis et délicieux.

- **Pâtissier en chef :** supervise et dirige le pâtissier, en élaborant des recettes innovantes, en maintenant des normes de qualité élevées et en assurant la gestion efficace de la pâtisserie
- **Responsable des ventes et du marketing :** élabore des stratégies de vente et de promotion efficaces pour attirer les clients, stimuler les ventes et renforcer la visibilité de la pâtisserie.
- **Responsable de la gestion et des stocks :** supervise et optimise la gestion des produits, des fournitures et de l'inventaire, garantissant ainsi une efficacité opérationnelle et une disponibilité constante des produits.
- **Développeur web :** chargé de concevoir, développer et maintenir le site Web de la pâtisserie, ainsi que de mettre en place des fonctionnalités en ligne pour les commandes, etc.

3- Principales missions, processus, activités et informations, ainsi que leurs finalités

a. Collecte des préférences du client :

- **Mission** : Collecter et enregistrer les préférences de chaque client en matière de produits de pâtisserie.
- **Finalité** : Personnaliser les recommandations de produits pour chaque client, améliorant ainsi l'expérience d'achat et la fidélisation.

b. Recommandation de produits personnalisés :

- **Processus** : Utilisation des préférences clients pour recommander des produits spécifiques.
- **Finalité** : Augmenter les ventes en proposant des produits qui correspondent aux goûts et aux préférences individuelles de chaque client.

c. Optimisation des itinéraires de livraison :

- **Activités** : Analyse des commandes en cours, de la localisation des clients et de la disponibilité des produits.
- **Finalité** : Réduire les délais de livraison en optimisant les itinéraires des livreurs, minimisant les coûts de transport et améliorant la satisfaction client.

d. Gestion automatisée des stocks :

- **Processus** : Suivi en temps réel des niveaux de stock des produits de pâtisserie.
- **Finalité** : Assurer la disponibilité des produits les plus demandés, éviter les ruptures de stock, minimiser les coûts de stockage et maximiser les ventes.

e. Gestion des commandes en ligne :

- **Activités** : Réception, traitement et suivi des commandes en ligne.

- **Finalité** : Assurer la satisfaction client en traitant efficacement les commandes, en fournissant des informations sur l'état de la commande et en garantissant des livraisons à délai raisonnable ou même rapide.

f. Gestion des retours et des remboursements :

- **Processus** : Traitement des retours de produits et des demandes de remboursement.
- **Finalité** : Maintenir la satisfaction client en gérant les retours de manière efficace et en garantissant des remboursements rapides et appropriés.

g. Suivi de la performance des ventes en ligne :

- **Activités** : Analyse des données de ventes, des taux de conversion, des taux d'abandon de panier, etc.
- **Finalité** : Identifier les tendances de vente, les opportunités d'amélioration et prendre des décisions stratégiques basées sur les données.

h. Gestion des promotions et des offres spéciales :

- **Processus** : Création et gestion de promotions et d'offres spéciales.
- **Finalité** : Stimuler les ventes en ligne en proposant des promotions attractives aux clients.

i. Service client en ligne :

- **Activités** : Fournir une assistance aux clients via chat en direct, e-mail ou téléphone.
- **Finalité** : Offrir un support client réactif pour résoudre les problèmes, répondre aux questions et améliorer la satisfaction client.

j. Sécurité des données clients :

- **Activités** : Mise en place de mesures de sécurité pour protéger les données personnelles des clients.
- **Finalité** : Assurer la confidentialité et la sécurité des informations client conformément aux réglementations en vigueur.

4- Impacts sur un dysfonctionnement de chacune de ces missions

Métrique de criticité : 1 = « pas important » et 4 = « critique »

Un dysfonctionnement de chacune des missions peut avoir des impacts significatifs sur différents aspects de l'entreprise. Voici comment chaque mission peut affecter les domaines financiers, d'image, humains, réglementaires et environnementaux en cas de dysfonctionnement :

a. Collecte des préférences du client/Recommandation de produits personnalisés :

- **Impact financier (2)** : Un dysfonctionnement peut entraîner une perte de ventes, car les clients ne reçoivent pas de recommandations personnalisées, ce qui peut réduire les ventes potentielles.
- **Impact sur l'image (2)** : Cela peut donner l'impression que l'entreprise ne comprend pas les besoins de ses clients, ce qui pourrait ternir l'image de la marque.
- I**mpact humain (1)** : Le personnel chargé de la gestion des recommandations peut devoir intervenir manuellement, augmentant la charge de travail.
- **Impact réglementaire (2)** : Les réglementations sur la protection de la vie privée des données des clients doivent être respectées.
- **Impact environnemental (1)** : Cela peut entraîner des livraisons moins efficaces si les produits recommandés ne sont pas en stock, ce qui peut augmenter les émissions de gaz à effet de serre.

b. Optimisation des itinéraires de livraison :

- **Impact financier (2)** : Des itinéraires de livraison inefficaces peuvent augmenter les coûts de livraison, réduire la rentabilité et potentiellement entraîner des retards de livraison.
- **Impact sur l'image (3)** : Les retards de livraison peuvent nuire à la satisfaction client et à la réputation de l'entreprise.
- **Impact humain (1)** : Les livreurs peuvent être stressés ou surchargés en cas d'itinéraires inadaptés.
- **Impact réglementaire (2)** : Les réglementations sur les délais de livraison doivent être respectées, notamment en matière de sécurité alimentaire.
- **Impact environnemental (1)** : Des itinéraires inefficaces peuvent entraîner une consommation de carburant supérieure et augmenter les émissions de CO2.

c. Gestion automatisée des stocks :

- **Impact financier (2)** : Une mauvaise gestion des stocks peut entraîner des coûts de stockage excessifs ou des ruptures de stock, réduisant ainsi la rentabilité.
- **Impact sur l'image (3)** : Les ruptures de stock peuvent frustrer les clients et ternir l'image de la marque.
- **Impact humain (1)** : Le personnel peut devoir gérer manuellement les problèmes de stocks, ce qui peut être chronophage (demande beaucoup de temps).
- **Impact réglementaire (1)** : La gestion des stocks de produits alimentaires doit se conformer à des réglementations strictes en matière de sécurité et de qualité.
- **Impact environnemental (1)** : Les excès de stocks peuvent entraîner du gaspillage alimentaire, ce qui a un impact environnemental négatif.

d. Gestion des commandes en ligne : Important (Le plus important)

- **Impact financier (3)** : Des erreurs de traitement des commandes peuvent entraîner des coûts supplémentaires pour l'entreprise, tels que des remboursements ou des frais de retour.
- **Impact sur l'image (4)** : Les erreurs de traitement des commandes peuvent frustrer les clients et nuire à la réputation de l'entreprise.
- **Impact humain (1)** : Les employés chargés du traitement des commandes peuvent être surchargés en cas de dysfonctionnement.

- **Impact réglementaire (1)** : La gestion des commandes en ligne doit respecter les lois sur la protection des consommateurs.
- **Impact environnemental (1)** : Des erreurs de traitement des commandes peuvent entraîner des livraisons inutiles, augmentant ainsi l'empreinte environnementale.

e. Gestion des remboursements :

- **Impact financier (2)** : Les remboursements peuvent entraîner des pertes financières.
- **Impact sur l'image (3)** : Une gestion inefficace des remboursements peut nuire à la réputation de l'entreprise.
- **Impact humain (1)** : Le personnel doit gérer les remboursements, ce qui peut être chronophage.
- **Impact réglementaire (1)** : Les politiques de remboursement doivent être conformes aux réglementations locales.
- **Impact environnemental (1)** : Les produits retournés peuvent être perdus ou gaspillés, ce qui a un impact sur l'environnement.

f. Suivi de la performance des ventes en ligne :

- **Impact financier (3)** : Un dysfonctionnement dans le suivi des ventes en ligne peut entraîner des décisions commerciales inefficaces, affectant ainsi les revenus.
- **Impact sur l'image (2)** : Les erreurs dans le suivi des ventes peuvent entraîner une perte de confiance de la part des investisseurs, des partenaires commerciaux et des clients.
- **Impact humain (1)** : Le personnel chargé de l'analyse des données peut devoir passer plus de temps à résoudre des problèmes liés au suivi des ventes.
- **Impact réglementaire (1)** : Les rapports de ventes doivent être précis pour respecter les réglementations financières.
- **Impact environnemental (1)** : Les erreurs dans le suivi des ventes peuvent entraîner des décisions logistiques inefficaces, augmentant potentiellement l'empreinte environnementale.

g. Gestion des promotions et des offres spéciales :

- **Impact financier (2)** : Un dysfonctionnement peut entraîner des pertes financières si les promotions ne sont pas correctement appliquées ou si les clients ne sont pas incités à acheter.
- **Impact sur l'image (2)** : Des problèmes avec les promotions peuvent donner l'impression que l'entreprise n'est pas fiable, ce qui peut nuire à son image de marque.
- **Impact humain (1)** : Le personnel chargé de la gestion des promotions peut devoir intervenir manuellement pour corriger les erreurs, ce qui peut augmenter la charge de travail.
- **Impact réglementaire (2)** : Il faut s'assurer que les promotions respectent les réglementations en matière de publicité et de vente.
- **Impact environnemental (1)** : Les promotions mal gérées peuvent entraîner des commandes inutiles, ce qui peut avoir un impact sur l'environnement en augmentant les émissions de gaz à effet de serre.

h. Service client en ligne : Important

- **Impact financier (2)** : Un service client inefficace peut entraîner la perte de clients et de ventes.
- **Impact sur l'image (3)** : Un mauvais service client peut nuire à la réputation de l'entreprise.
- **Impact humain (1)** : Les agents de service client peuvent être stressés en cas d'augmentation des requêtes.
- **Impact réglementaire (2)** : Les communications avec les clients doivent respecter les réglementations sur la confidentialité et la protection des données.
- **Impact environnemental (2)** : Les demandes de support en ligne peuvent être plus eco-friendly que les interactions en personne ou par téléphone.

i. Sécurité des données clients :

- **Impact financier (2)** : Une violation de la sécurité des données peut entraîner des amendes, des coûts de notification et des pertes de clientèle.
- **Impact sur l'image (2)** : Une violation de la sécurité des données peut gravement nuire à la réputation de l'entreprise.
- **Impact humain (2)** : La gestion de la sécurité des données nécessite un personnel qualifié pour mettre en place et maintenir des mesures de sécurité.
- **Impact réglementaire (2)** : La sécurité des données des clients doit respecter des lois et réglementations strictes sur la protection de la vie privée.
- **Impact environnemental (1)** : Bien que moins directe, une mauvaise gestion de la sécurité des données peut indirectement conduire à des problèmes environnementaux, par exemple, si des données sont compromises et que des ressources sont utilisées pour remédier à la situation.

II- Contexte SI

L'activité priorisée ici est la **gestion des commandes en ligne** car elle représente plus de risques que les autres. Sans cette activité, il n'y aurait pas de vente alors que la vente est l'objectif premier de l'entreprise.
Remarque **:** Hébergement : Shopify, Stripe : PaaS

1- Actifs de type "information"

- **Données applicatives :** Données structurées (SQL) de ventes, de clients, de produits stockés dans des bases de données en ligne (MySQL).
- **Données isolées/en transit :** Informations de carte de crédit, historique de commandes**,** envoi de récapitulatif de commande passées sous forme d'email, de SMS etc.
- **Fichiers bureautiques partagés :** Non
- **Fichiers bureautiques personnels :** Non
- **Documents personnels :** Non
- **Listings ou états imprimés** : Non
- **Courrier électronique :** Non
- **Courrier postal :** Non

- **Fax Archives documentaires :** Non
- **Archives informatiques** : Oui
- **Données publiées (web ou interne) :** Non

2- Actifs de type "services"

- **Services du réseau étendu :** Oui**,** Internet
- **Services du réseau local :** Oui
- **Services applicatifs :** Serveur Apache (PHP)
- **Services bureautiques communs :** Non
- **Équipements mis à la disposition des utilisateurs :** Non
- **Services systèmes Communs :** Non
- **Services de publication sur site web :** Non
- **Services généraux environnement de travail :** Oui (Poste de travail qui affiche les commandes reçues via internet)
- **Services télécom :** Oui

3- Actifs de type " lois et règlements"

- **Protection des renseignements personnels :** Oui
- **Communication financière** : Oui
- **Vérification de la comptabilité informatisée :** Non
- **Protection de la propriété intellectuelle :** Non
- **Protection des systèmes informatisés :** Oui
- **Sécurité des personnes et protection de l'environnement :** Oui

III- Métriques DIC et signification des niveaux

Activité : **gestion des commandes en ligne**

1- Actifs de type "information" *(voir fichier Mehari_chateau_des_saveurs.xlsm* ***T1)***

Données applicatives

A- Disponibilité

Une indisponibilité des données applicatives est bloquante pour l'activité des commandes en ligne, d'où le choix de la métrique 4.

B- Intégrité

Une information erronée dans la base de données ne sera pas récupérable (pas de backup initialement), d'où le choix de la métrique 4.

C- Confidentialité

Une information erronée dans la base de données ne sera pas récupérable (pas de backup initialement), d'où le choix de la métrique 4.

Le même raisonnement est effectué pour les autres actifs.

2- Actifs de type "services" (voir fichier Mehari_chateau_des_saveurs.xlsm T2)

Services du réseau étendu :

A- Disponibilité

Une indisponibilité des services du réseau étendu est bloquante pour l'activité des commandes en ligne, d'où le choix de la métrique 4.

B- Intégrité

Une information erronée des services du réseau étendu ne sera pas récupérable, d'où le choix de la métrique 4.

Le même raisonnement est effectué pour les autres actifs.

3- Actifs de type " lois et règlements" (voir fichier Mehari_chateau_des_saveurs.xlsm T3)

Protection de la propriété intellectuelle

Efficacité :

L'efficacité est la mesure utilisée pour déterminer le niveau de criticité concernant les actifs de type "lois et règlements".
On considère que la protection de la propriété intellectuelle doit être le plus efficace possible d'où le choix de la métrique 4.

Le même raisonnement est effectué pour les autres actifs.

IV- Tableau d'impacts intrinsèque :

Ce tableau permet de sélectionner les actifs de différents types sur lesquels on souhaite travailler. Dans notre cas, nous avons décidé de sélectionner les actifs avec une métrique au moins égale à 3.

Les actifs choisis sont :

1- Actifs de type "information"

- D01 - Fichiers de données ou bases de données applicatives
- D06 - Données échangées, écrans applicatifs, données individuellement sensibles

<u>1- Actifs de type “données et information”</u>

- G01 - Environnement de travail des utilisateurs
- R01 - Service du réseau étendu
- R02 - Service du réseau local
- S01 - Services applicatifs

<u>1- Actifs de type “processus de gestion”</u>

- C01 - Conformité à la loi ou aux réglementations relatives à la protection des renseignements personnels
- C05 - Conformité à la loi relative à la protection des systèmes informatisés

V- Risques actifs

Nous avons décidé d’étudier les gravités de scénarios de disponibilité pour les actifs de type services, plus précisément les **services applicatifs.**

<u>Justification</u> : En termes de gravité, les services applicatifs affichent le plus grand nombre de gravités de scénarios de niveau 4.

Mehari_chateau_des_saveurs .XLSM

Fichier Édition Affichage Insertion Format Données Outils Aide

Partager

A1:B1 | Panorama des gravités de scénarios

	Panorama des gravités de scénarios	Disponibilité				Intégrité				Confidentialité			
		Gr. 1	Gr. 2	Gr. 3	Gr. 4	Gr. 1	Gr. 2	Gr. 3	Gr. 4	Gr. 1	Gr. 2	Gr. 3	Gr. 4
Actifs de type Données et informations													
Données et informations													
D01	Fichiers de données ou bases de données applicatives	0	0	0	32	0	0	0	16	0	20	0	0
D02	Fichiers bureautiques partagés	0	0	0	0	0	0	0	0	0	0	0	0
D03	Fichiers bureautiques personnels (gérés dans environnement personnel)	0	0	0	0	0	0	0	0	0	0	0	0
D04	Informations écrites ou imprimées détenues par les utilisateurs, archives personnelles	0	0	0	0					0	0	0	0
D05	Listings ou états imprimés des applications informatiques									0	0	0	0
D06	Données échangées, écrans applicatifs, données individuellement sensibles	0	0	0	4	0	0	0	14	0	13	0	0
D07	Courrier électronique	0	0	0	0	0	0	0	0	0	0	0	0
D08	Courrier postal et télécopies	0	0	0	0	0	0	0	0	0	0	0	0
D09	Archives patrimoniales ou documentaires	0	0	0	0				•	0	0	0	0
D10	Archives informatiques	0	0	0	0	0	0	0	0	0	0	0	0
D11	Données et informations publiées sur des sites publics ou internes	0	0	0	0	0	0	0	0				
Actifs de type Services													
Services généraux communs													
G01	Environnement de travail des utilisateurs	0	0	1	0								
G02	Services de télécommunication (voix, télécopies, visioconférence, etc.)	0	0	0	0	0	0	0	0				
Services informatiques et télécom													
R01	Service du réseau étendu	0	0	3	16	0	0	0	5				
R02	Service du réseau local	0	0	13	0	0	0	5	0				
S01	Services applicatifs	0	0	4	37	0	0	0	16	0	0	16	0
S02	Services bureautiques communs (serveurs de données, gestionnaires de documents, imprimantes partagées, etc.)	0	0	0	0	0	0	0	0				
S03	Equipements mis à la disposition des utilisateurs (PC, imprimantes locales, périphériques, interfaces spécifiques, etc.)	0	0	0	0								
S04	Services systèmes communs : messagerie, archivage, impression, édition, etc.	0	0	0	0	0	0	0	0				
S05	Services de publication d'informations sur un site web interne ou public	0	0	0	0	0	0	0	0				
Actifs de type Processus de management		**Efficience**											
Non conformité à la loi ou à la réglementation													
C01	Conformité à la loi ou aux réglementations relatives à la protection des renseignements personnels	0	0	4	0								
C02	Conformité à la loi ou aux réglementations relatives à la communication financière	0	0	0	0								
C03	Conformité à la loi ou aux réglementations relatives à la vérification de la comptabilité informatisée	0	0	0	0								
C04	Conformité à la loi ou aux réglementations relatives à la propriété intellectuelle	0	0	0	0								
C05	Conformité à la loi relative à la protection des systèmes informatisés	0	0	4	0								
C06	Conformité aux réglementations relatives à la sécurité des personnes et à la protection de l'environnement	0	0	0	0								

Fig. 2 : Panorama des gravités de scénarios

V- Tableau des événements :

Puisque nous avons décidé de continuer avec la disponibilité des services applicatifs, les évènements choisis du tableau sont les suivants :

- Absence de maintenance applicative ou maintenance app. impossible
- Absence de maintenance système ou maintenance système impossible
- Panne d'équipement informatique ou télécom
- Panne d'équipement de servitude
- Bug bloquant dû à une erreur de conception ou d'écriture de programme (interne)
- Incident d'exploitation
- Effacement volontaire ou pollution massive de configurations systèmes
- Saturation malveillante d'équipements informatiques ou réseaux
- Manipulation ou falsification matérielle d'équipement
- Vol physique

VI- Scénarios

Dans cette partie, on traitera des scénarios en rapport avec les évènements choisis ci-dessus et décidera si le risque est accepté ou transféré.

Etant donné que nous avons choisi de travailler sur la disponibilité des services applicatifs, on a eu donc à traiter les 64 scénarios liés à l'indisponibilité des services applicatifs. Pour chacun de ces scénarios on aura à les traiter de 4 stratégies possibles.

- La réduction de risque (R) : pour cela on aura besoin de mettre un plan d'action en place pour réduire les risques
- Le transfert de risques (T) : à une organisation externe (un tiers).
- L'acceptation du risque (A) : on vise à accepter le risque et à travailler avec ;
- L'évitement du risque (E) : on vise à éviter le risque, car il est trop grand.

Dans ce qui suit, On a décidé que :

- Pour tous les scénarios malveillants qui relèvent d'erreurs, vol, d'accidents liés à une surcharge électrique et d'incidents malveillants provoqués par des utilisateurs illégitimes et/ou non autorisés, on a décidé qu'on devait transférer le risque car on cherche à réduire l'impact financier en cas de la réalisation du risque sur l'activité de "gestion de commandes en ligne".
- Pour tous les scénarios qui n'ont pas d'impacts ou peu on a décidé qu'on devait accepter le risque car on estime qu'ils ne sont pas bloquants pour l'activité de l'entreprise, ce qui fait qu'on peut continuer travailler même si on est confronté à ce genre de risques qui relèvent d'erreurs, d'accidents, d'incidents provoqués légitimement (c'est-à-dire indépendamment de notre volonté).
- Pour les scénarios restants qui ne sont pas malveillants on aura à soit les réduire ou soit les éviter.

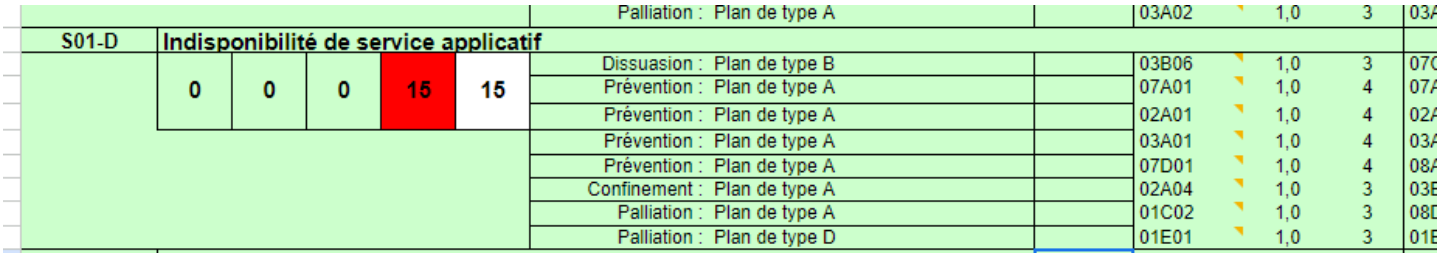
- Quelques scénarios de risques :

Scénarios	**Accepté ou Transféré ou Traité (champ vide dans le Mehari)**
Effacement accidentel de programmes de services applicatifs, suite à un incident d'exploitation.	**Traité**
Effacement par erreur de programmes de services applicatifs, par un utilisateur autorisé légitime	**Traité**
Effacement par erreur de programmes de services applicatifs, par un utilisateur autorisé illégitime	**Traité**
Effacement par erreur de programmes de services applicatifs, par un utilisateur non autorisé	**T**
Effacement malveillant de programmes de services applicatifs, par un utilisateur autorisé légitime	**T**
Effacement malveillant de programmes de services applicatifs, par un utilisateur autorisé illégitime	**T**
Indisponibilité temporaire accidentelle de système hôte de services applicatifs, due à une panne d'équipement	**A**
Indisponibilité temporaire accidentelle de système hôte de services applicatifs, due à une défaillance ou à une indisponibilité de moyens de servitude	**A**
Inexploitabilité accidentelle de média support de programmes de services applicatifs, en médiathèque, due au vieillissement	**A**

Fig. 3 : Quelques risques liés à l'indisponibilité des services applicatifs

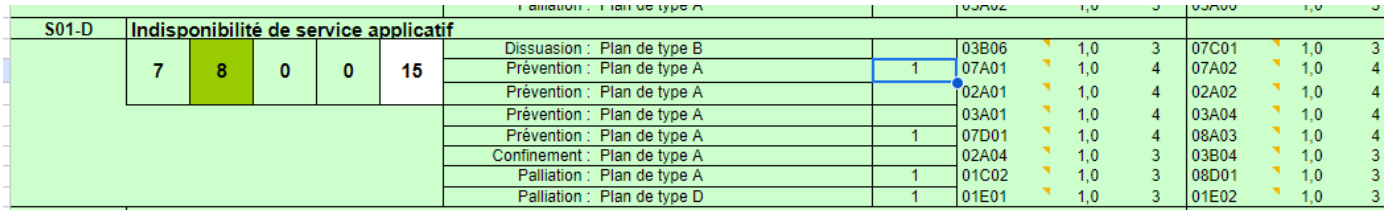
VII- Plan d’actions :

Dans cette étape on va définir l’ensemble de méthodes, mesures correctives et préventives à mettre en œuvre pour les risques identifiés au cours de l'analyse des risques qu’on a décidé de traiter.



						Palliation : Plan de type A		03A02	1,0	3	03A		
S01-D	Indisponibilité de service applicatif												
	0	0	0	15	15	Dissuasion : Plan de type B		03B06	1,0	3	07C		
						Prévention : Plan de type A		07A01	1,0	4	07A		
						Prévention : Plan de type A		02A01	1,0	4	02A		
						Prévention : Plan de type A		03A01	1,0	4	03A		
						Prévention : Plan de type A		07D01	1,0	4	08A		
						Confinement : Plan de type A		02A04	1,0	3	03E		
						Palliation : Plan de type A		01C02	1,0	3	08D		
						Palliation : Plan de type D		01E01	1,0	3	01E		

*Fig. 4 : Gravité scénarios **avant** choix de plan d’actions*



S01-D	Indisponibilité de service applicatif												
	7	8	0	0	15	Dissuasion : Plan de type B		03B06	1,0	3	07C01	1,0	3
						Prévention : Plan de type A	1	07A01	1,0	4	07A02	1,0	4
						Prévention : Plan de type A		02A01	1,0	4	02A02	1,0	4
						Prévention : Plan de type A		03A01	1,0	4	03A04	1,0	4
						Prévention : Plan de type A	1	07D01	1,0	4	08A03	1,0	4
						Confinement : Plan de type A		02A04	1,0	3	03B04	1,0	3
						Palliation : Plan de type A	1	01C02	1,0	3	08D01	1,0	3
						Palliation : Plan de type D	1	01E01	1,0	3	01E02	1,0	3

*Fig. 5 : Gravité de scénarios **après** choix de plan d’actions*

Avant l'application d'un plan d'action quelconque, nous avions 15 scénarios de risques de gravité 4 concernant l'indisponibilité des services applicatifs. *(Voir fig. 4)*
L'application de deux plans de prévention de type A, d'un plan de palliation de type A et d'un plan de palliation de type D ont permis de réduire les gravités de risques de ces scénarios à 7 scénarios de gravité 1 et 8 scénarios de gravité 2. *(Voir fig. 5)*

Remarque : L'application des autres types de plan n'avait aucun impact sur la réduction de La gravité des risques.

➢ ***Choix de quelques services à améliorer pour chaque type de plan choisi***

Pour chaque service, il s'agirait de poser la question de savoir si le service a été mis en œuvre(partiellement/entièrement) et sinon quelles parties du service restent à implémenter. On ne traitera que d'un service pour chaque type de plan.

1. *1er plan de prévention de type A*

07A01 : Gestion des profils d'accès (droits et privilèges accordés en fonction des profils de fonction)

	A	B	C	D	E	F	G	H	I	J	K
1	**Questionnaire d'audit : Sécurité des Systèmes et de leur architecture**		**1**	**variante**							
2	Référence	Question	R-V1	R-V2	R-V3	R-V4	P	Max	Min	Typ	ISO 27002
3	**07A**	**Contrôle d'accès aux systèmes**									
4	***07A01***	***Gestion des profils d'accès (droits et privilèges accordés en fonction des profils de fonction)***									
5	07A01-01	A-t-on établi une politique de gestion des droits d'accès aux systèmes s'appuyant sur une analyse préalable des exigences de sécurité, basées sur les enjeux de l'activité ?	1				2			E1	11.1.1
6	07A01-02	Les droits d'accès aux différentes parties du SI (applications, bases de données, systèmes, équipements etc.) sont-ils définis par rapport à des "profils" métiers regroupant des "rôles" ou des "fonctions" dans l'organisation (un profil définissant les droits dont disposent les titulaires de ce profil) ? *Nota : La notion de profil peut, dans certaines circonstances, être remplacée par une notion de "groupe".*	1				4	2		E1	11.2.2
7	07A01-03	Est-il possible d'introduire, dans les règles de définition des droits d'accès (qui déterminent les droits attribués à un profil), des paramètres variables en fonction du contexte tels que la localisation du demandeur ou les réseaux utilisés, ou en fonction des moyens utilisés (protocoles, chiffrement, etc.) ou de la classification des ressources auxquelles les droits donnent accès ?	0				4			E2	
8	07A01-04	Les profils permettent-ils également de définir des créneaux horaires et des calendriers de travail (heures début et fin de journée, week-end, vacances, etc.) ?	1				2			E3	11.5.6
9	07A01-05	Ces profils et l'attribution de droits aux différents profils ont-ils reçu l'approbation des propriétaires d'information et/ou du RSSI ?	0				4	2		E2	11.5.6
10	07A01-06	Les processus de définition et de gestion des droits attribués aux profils sont-ils sous contrôle strict ? *Un contrôle strict requiert que la liste des personnes habilitées à changer les droits attribués aux profils soit très limitée, que la matérialisation de ces droits sous forme de tables soit strictement sécurisée lors de leur transmission et de leur stockage et qu'il existe un contrôle d'accès renforcé pour pouvoir les modifier, et que les modifications soient journalisées et auditées.*	0				4	3		R1	
11	07A01-07	Peut-on contrôler à tout moment la liste des profils et l'ensemble des droits attribués à chaque profil ?	1				2	2		C1	
12	07A01-08	Y a-t-il un audit régulier, au moins une fois par an, de l'ensemble des droits attribués à chaque profil et des procédures de gestion des profils ?	0				4	2		C1	11.2.4

Fig. 6 : 07A01 Gestion des profils d'accès (droits et privilèges accordés en fonction des profils de fonction)

Réponses aux sous questions :

07A01-01

Réponse : Oui
Solution : Aucune

07A01-02
Réponse : Oui

Solution : Aucune

07A01-03

Réponse : Non
Solution : Mettre en place un modèle RBAC qui limite strictement les droits attribués à chaque profil en fonction des responsabilités et des besoins fonctionnels.

07A01-04

Réponse : Oui
Solution : Aucune

07A01-05

Réponse : Non
Solution : Dans le contexte qu'on a défini, il n'y a pas de de RSSI / Propriétaire de l'information. Le mieux serait de nommer une personne qui va occuper cette tâche.

07A01-06

Réponse : Non
Solution : Mise en place d'un contrôle strict pour définir et gérer les différents droits attribués aux profils, en ayant un administrateur qui aura à gérer l'attribution de ces droits. Il faut encore en plus de tout cela, mettre en place une politique d'authentification forte pour l'administrateur.

07A01-07
Réponse : Oui
Solution : Aucune

07A01-08

Réponse : Non
Solution : Il y a une vraie nécessité à mettre en place des audits réguliers au moins une fois par an pour permettre d'avoir une visibilité régulière sur les droits attribués et d'identifier rapidement tout écart par rapport aux politiques de sécurité.

2. ***Dernier plan de prévention de type A :***

08E01 : Détection et traitement (en temps réel) des anomalies et incidents d'exploitation

278	**08E**	**Gestion et traitement des incidents**										
279	***08E01***	***Détection et traitement (en temps réel) des anomalies et incidents d'exploitation***										
280	08E01-01	A-t-on analysé les événements ou successions d'événements pouvant être révélateurs de comportements anormaux ou d'actions illicites et a-t-on mis en place des points ou indicateurs de surveillance en conséquence ?	0				4			E2		
281	08E01-02	Le système dispose-t-il d'une fonction automatique de surveillance en temps réel en cas d'accumulation d'événements anormaux (par exemple tentatives infructueuses de connexion sur stations voisines ou sur des transactions sensibles) ?	0				4					
282	08E01-03	Existe-t-il une application capable d'analyser les diagnostics individuels d'anomalie et de déclencher une alerte à destination du personnel d'exploitation ?	0				4			E3		
283	08E01-04	Existe-t-il, parmi le personnel d'exploitation, une équipe permanente ou disponible sur appel (astreinte) capable de réagir en cas d'alerte de la détection d'anomalie ?	0				4	2		E3		
284	08E01-05	A-t-on défini, pour chaque cas d'alerte, la réaction attendue de l'équipe d'intervention et sa disponibilité est-elle suffisante pour faire face à cette attente ?	0				4			E3		
285	08E01-06	Les paramètres définissant les alarmes sont-ils strictement protégés (droits limités et authentification forte) contre tout changement illicite ?	0				4	3		R1		
286	08E01-07	Tout arrêt du système d'alerte déclenche-t-elle une alarme auprès de l'équipe de surveillance ?	0				4	3		R1		
287	08E01-08	Existe-t-il un archivage (sur disque, cassette, DON, etc.) de tous les éléments ayant permis de détecter une anomalie ou un incident ?	0				2			E2		
288	08E01-09	Les procédures de détection d'anomalies et la disponibilité de l'équipe de surveillance font-elles l'objet d'un audit régulier ?	0				2	3		C1		

Fig. 7 : 08E01 : Détection et traitement (en temps réel) des anomalies et incidents d'exploitation

Réponses aux sous questions :

08E01-01

Réponse : Non
Solution : C'est la plateforme d'hébergement qui s'en occupe.

08E01-02

Réponse : Non
Solution : C'est la plateforme d'hébergement qui s'en occupe.

08E01-03

Réponse : Non
Solution : C'est la plateforme d'hébergement qui s'en occupe.

08E01-04

Réponse : Non
Solution : C'est la plateforme d'hébergement qui s'en occupe.

08E01-05

Réponse : Non
Solution : C'est la plateforme d'hébergement qui s'en occupe.

08E01-06

Réponse : Non
Solution : C'est la plateforme d'hébergement qui s'en occupe.

08E01-07

Réponse : Non
Solution : C'est la plateforme d'hébergement qui s'en occupe.

08E01-08

Réponse : Non
Solution : C'est la plateforme d'hébergement qui s'en occupe.

08E01-09

Réponse : Non
Solution : C'est la plateforme d'hébergement qui s'en occupe.

3. Plan de palliation de type A :

01C02 : Gestion du personnel et des partenaires ou prestataires stratégiques

109	*01C02*	*Gestion du personnel et des partenaires ou prestataires stratégiques*								
110	01C02-01	Les compétences stratégiques sont-elles régulièrement identifiées ?	0				4	2		E2
111	01C02-02	Des solutions de secours existent-elles en cas d'indisponibilité de compétences stratégiques ?	0				4	3		E3
112	01C02-03	Les partenaires ou prestataires stratégiques sont-ils régulièrement identifiés ?	0				4	2		E2
113	01C02-04	Des solutions de secours existent-elles en cas d'indisponibilité de partenaires ou prestataires stratégiques ?	0				4	3		E3
114	01C02-05	Ces solutions de secours (concernant le personnel interne ou les prestataires) permettent-elles de garantir une poursuite de l'activité de l'entreprise sans perturbation majeure ?	0				4	3		E3
115	01C02-06	Le personnel stratégique fait-il l'objet d'une gestion de carrière spécifique ?	0				2			E3
116	01C02-07	Les prestataires stratégiques font-ils l'objet d'une gestion contractuelle spécifique ?	0				2			E3
117	01C02-08	Existe-t-il une procédure de contrôle de la pertinence et de la mise à jour des mesures précédentes ?	0				2		3	R1

Fig. 8 : 01C02 : Gestion du personnel et des partenaires ou prestataires stratégiques

Réponses aux sous questions :

01C02-01

Réponse : Non
Solution : Les compétences stratégiques évoluent avec le temps, ce qui nous pousse à toujours faire une veille stratégique de compétences stratégiques.

01C02-02

Réponse : Non
Solution : Recourir à des services de conseil externe ou à des experts en gestion des risques et en sécurité de l'information en cas de besoin

01C02-03

Réponse : Non
Solution : Établir une cartographie complète des parties prenantes, y compris les partenaires et prestataires, qui ont un impact direct ou indirect sur la sécurité de l'information.

01C02-04

Réponse : Non
Solution : Évitez de dépendre excessivement d'un seul fournisseur en faisant en sorte de diversifier les fournisseurs pour réduire les risques associés à l'indisponibilité.

01C02-05

Réponse : Non
Solution : Il faut d'abord mettre en place ces solutions pour voir si elles permettent une reprise d'activité dans chaque situation, car chaque situation est unique.

01C02-06

Réponse : Non
Solution : la solution consiste à identifier les compétences spécifiques nécessaires pour jouer un rôle stratégique dans l'entreprise. Cela peut inclure des compétences en leadership, en prise de décision stratégique, en gestion du changement, et une compréhension approfondie des enjeux commerciaux.

01C02-07

Réponse : Non
Solution : il faut établir des accords clairs, définir des attentes mutuelles, garantir la qualité des services et minimiser les risques associés à la dépendance envers ces partenaires. Les contrats devraient inclure des SLA détaillés décrivant les niveaux de service attendus, les délais, les performances, et d'autres indicateurs clés de qualité. Ces SLA aident à mesurer et à garantir la qualité des services fournis par le prestataire

01C02-08 :

Réponse : Non
Solution : Faire une évaluation régulière des risques pour identifier les menaces émergentes et une simulation d'incidents qui permet de tester la capacité de l'organisation à réagir et à récupérer en cas d'incident de sécurité.

4. ***Plan de palliation de type D :***

01E01 : Prise en compte des besoins de continuité de l'activité

194	*01E01*	***Prise en compte des besoins de continuité de l'activité***									
195	01E01-01	A-t-on analysé la criticité des différentes activités pour mettre en évidence les besoins de continuité de service ? *Une analyse approfondie suppose que l'on établisse une liste de scénarios d'incidents et qu'on en analyse toutes les conséquences prévisibles.*	0				4	2		E1	14.1.2
196	01E01-02	Cette analyse a-t-elle permis de formaliser les performances minimales à assurer au niveau des systèmes d'information et ces performances minimales ont-elles été acceptées par les utilisateurs (propriétaires d'information) ?	0				4	2		E1	14.1.2
197	01E01-03	Existe-t-il des processus, régulièrement mis en oeuvre, d'analyse des risques, liés à l'information, pouvant conduire à une interruption des activités de l'entreprise, débouchant sur une définition des exigences de sécurité, des responsabilités, des procédures à appliquer et moyens à mettre en oeuvre afin de permettre l'élaboration des plans de continuité ?	0				2			E2	14.1.1

Fig. 9 : 01E01 Prise en compte des besoins de continuité de l'activité

Réponses aux sous questions :

01E01-01

Réponse : Non
Solution : Établir une liste des scénarios d'incidents, pour chaque scénario une analyse approfondie des conséquences prévisibles doit être réalisée. Cela pourrait inclure la durée prévue de l'indisponibilité, les pertes financières estimées et les impacts sur les clients et les partenaires.

01E01-02

Réponse : Non
Solution : Les performances minimales sont définies en fonction des résultats de l'analyse de la criticité des activités. Cela peut inclure des délais de reprise acceptables, des objectifs de disponibilité des systèmes, des niveaux de performance spécifiques

01E01-03

Réponse : Non
Solution : Appliquer une méthodologie d'analyse des risques conforme aux directives de la norme ISO 27001