**Projet cybersécurité**

Mise en place du PRA

Louis Hans

Rudy Krauffel

Corentin Lente

Table des matières

[Plan de reprise d’activité 4](#_Toc36739268)

[Contexte 4](#_Toc36739269)

[Plan de reprise d’activité en cas de perte de données : 4](#_Toc36739270)

[Plan de sauvegardes des données : 4](#_Toc36739271)

[Mesures préventives : 4](#_Toc36739272)

[Mesures détectives : 5](#_Toc36739273)

[Mesures correctives : 5](#_Toc36739274)

[Evaluations des risques : 5](#_Toc36739275)

[Etablir les priorités de l’entreprise : 5](#_Toc36739276)

[Stratégie de récupération : 6](#_Toc36739277)

[Procédure de test de notre plan de reprise d’activité : 6](#_Toc36739278)

[Recommandations : 7](#_Toc36739279)

[La structure de la norme 7](#_Toc36739280)

[1. Politique et périmètre 8](#_Toc36739281)

[2. Appréciation des risques 8](#_Toc36739282)

[3. Traitement des risques 8](#_Toc36739283)

[4. Mesures de sécurité 9](#_Toc36739284)

# Plan de reprise d’activité

Un Plan de Reprise d’Activité Informatique met en œuvre l’ensemble des processus et des moyens humains, matériels et technologiques permettant à l’entreprise de faire face à un sinistre informatique majeur

Un PRA Informatique s’articule autour de :

* Préparation et définitions des différents processus et outils qui constitueront la base essentielle sur laquelle l’entreprise s’appuiera pour faire face à un sinistre.
* La mise en œuvre opérationnelle d’un mode « lean » ou configuration minimale permettant à l’entreprise d’assurer ses fonctions vitales immédiatement après le sinistre. La vitesse de réaction et la qualité de la préparation sont ici essentielles.

## Contexte

L’entreprise Motuc vient de subir une cyber-attaque le 26 mars 2020 et toute l’infrastructure est impactée. Il y a d’importante sommes d’argent qui sont en jeux. La conséquence de cette cyber-attaque est le chiffrement de plusieurs fichiers importants, ce qui met l’entreprise en arrêt.

## Plan de reprise d’activité en cas de perte de données :

## Plan de sauvegardes des données :

-Pour les données clients, il faudra faire des sauvegardes journalières pour éviter la perte de clients potentiel.

-Pour les données concernant le stock, il est conseiller de mettre en place des sauvegardes toutes les heures pour éviter une trop grande perte, voir raccourcir la durée s’il y a un grand nombre de commandes.

-Concernant les données comptables, il est préférable de faire deux sauvegardes par jour pour enregistrer les ventes de la matinée et de l’après-midi.

Ces sauvegardes seront faites avec un script écrit par le service informatique. Elles seront situées dans le cloud et sur les différents serveurs physiques pour plus de sécurité.

## Mesures préventives :

Les mesures préventives ont un rôle primordial pour l’entreprise lors d’un sinistre quel qu’il soit, dans notre cas une perte de données. Ces mesures auront pour but de diminuer l’inactivité de l’entreprise.

* Des sauvegardes de données régulière.

Dans notre cas une sauvegarde des données dans le cloud et sur les serveurs physiques qui permettra une continuité de l’entreprise.

* Il faudra effectuer des tests de notre plan de reprise d’activité régulièrement
* Installer des générateurs et de conduire des inspections du quotidien.
* Mettre en place un guide des bonnes pratiques pour la sécurité du SI.
* Mise en place d’un réseau intranet de secours.

## Mesures détectives :

Les mesures détective sont utiles à la détection d’éléments indésirables dans le système d’information de l’entreprise. Cela permettra d’appliquer les correctives plus efficacement.

* Installer des logiciels anti-virus à jour et les renouveler.
* Mettre en place des sessions de formation des salariés contre la détection de menace
* Installer des logiciels de contrôle/surveillance des serveurs et des réseaux.

## Mesures correctives :

Les mesures correctives visent à restaurer un système après un événement indésirable (sinistre, désastre). Ces mesures portent sur la fixation ou la restauration des systèmes d’information après l’incident.

Elles peuvent inclure la tenue de documents critiques dans le plan de reprise d’activité ou la souscription à des polices d'assurance adaptées à l’organisation. Dans toutes les organisations, un Plan de Reprise d’Activité doit permettre de répondre aux interrogations suivantes :

* Quel est son objectif et son but ?
* Quelles sont les personnes ou équipes responsables si des perturbations surviennent ?
* Que feront ces personnes quand l’incident surviendra ?

## Evaluations des risques :

Notre équipe a préalablement fais cette évaluation. Nous vous laissons aller voir le fichier « Analyse des risques détaillés »

## Etablir les priorités de l’entreprise :

Nous avons identifié les services critiques à la survie de votre entreprise. Les voici par ordre de priorité :

- Electricité

- Accès à internet (Nos fichiers dans le cloud)

- Accès aux différents ERP

- Communications entre les plateformes de ravitaillement et les magasins

- Identifier et traiter le risque

- Changement du matériel défectueux

## Stratégie de récupération :

Notre stratégie de récupération lors d’une perte de donnée est :

Employé hors service informatique :

* Contacter le service informatique si détection de la perte de donnée
* Appliquer les conseils du service informatique

Service Informatique :

* Identifier la raison de notre perte de donnée.
* Traiter le problème lié à cette perte.
* Récupération de notre sauvegarde des données dans le cloud.
* Réinitialisation des machines physique à partir des sauvegardes du cloud
* Relancement de l’activité.
* Contact des personnes impactée par la perte des données (Clients fournisseurs).

## Procédure de test de notre plan de reprise d’activité :

Lors d’une attaque ransomware, notre entreprise à perdu l’accès a ses fichiers, les pirates demandent une rançon pour la récupération de ces fichiers, voici un plan de comment récupérer ces données :

* Identifier la raison de notre perte de donnée.
* Traiter le problème lié à cette perte.
* Récupération de notre sauvegarde des données dans le cloud.
* Relancement de l’activité.
* Contact des personnes impactée par la perte des données (Clients fournisseurs).

Une fois que ces actions sont effectuées, vous aurez de nouveau accès à vos données.

Les tests de notre plan de prise d’activité devront être effectués tous les 6 mois pour pouvoir maintenir une certaine qualité. Ce test aura pour but de fournir des informations supplémentaires quant aux nouvelles étapes qui devront être incluses, aux changements des procédures qui ne sont pas efficaces et aux autres rajustements appropriés. Ceux-ci ne peuvent pas devenir évidents à moins qu'un réel test d'essai ne soit exécuté. Le plan est par la suite mis à jour pour corriger n'importe quel problème identifié pendant le test.

## Recommandations :

**Que faire pour que ce genre d’attaques ne se reproduisent plus ?**

Pour éviter que ce sinistre se réitère, nous vous proposons de suivre la norme de sécurité informatique ISO 27001, c’est la norme internationale décrivant les bonnes pratiques à suivre dans le cadre de la création d’un système de gestion de la sécurité de l'information (ISMS - Information Security management system).

La norme ISO 27001 sert à :

* Protéger les données
* Augmenter la résilience aux cyberattaques
* Réduire les coûts de sécurité de l'information
* Répondre aux menaces de sécurité changeantes
* Améliorer la culture d'entreprise

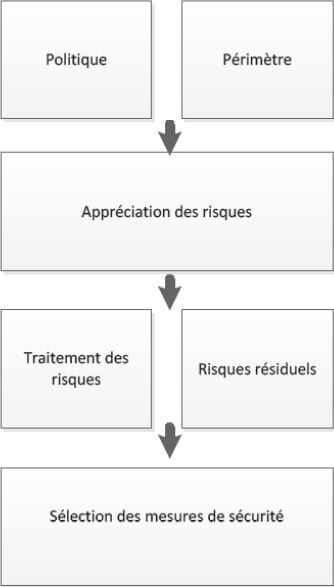
## La structure de la norme

La norme ISO 27001 est une démarche calquée sur ISO 9000, qui comprend plusieurs phases à mettre en place (Plan /Do/ Check /Act)

Phase plane :

La phase « Plan » du PDCA consiste à fixer les objectifs du SMSI en suivant quatre grandes étapes, la politique et le périmètre du SMSI, l’appréciation des risques, le traitement des risques décidé en tenant en compte des risques résiduels et la sélection des mesures de sécurité présentées dans le SoA11 (Statement of Applicability).

Dans la figure ci-dessous, une vue du déroulement de la phase Plan.



### Politique et périmètre

La première étape consiste à définir la politique et le périmètre du SMSI.

La politique est là pour préciser le niveau de sécurité qui sera appliqué au sein du périmètre du SMSI. La norme ne fixe pas d’exigences sur le périmètre, il peut être restreint où couvrir l’ensemble des activités de l’organisme.

L’objectif est d’y inclure les activités pour lesquelles les parties prenantes exigent un certain niveau de confiance.

### Appréciation des risques

La norme ISO 27001 ne donne pas de directives sur la méthode d’appréciation des risques à adopter. Les entreprises peuvent donc en inventer une en veillant à bien respecter le cahier des charges ou en choisir une parmi les plus courantes notamment la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) mise en place en France par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d’Information). Le cahier des charges relatif à l’appréciation des risques se développe en 7 points :

* Identifier les actifs ;
* Identifier les personnes responsables ;
* Identifier les vulnérabilités ;
* Identifier les menaces ;
* Identifier leurs impacts sur les actifs à défendre ;
* Évaluer la vraisemblance ou potentialité du risque ;
* Estimer les niveaux de risque, fonction de leur potentialité et de leur impact.

### Traitement des risques

Il existe quatre traitements possibles de chacun des risques identifiés, présentés par ordre décroissant d'intérêt pour l'organisme :

* L’évitement : politique mise en place si l’incident est jugé inacceptable ou si les mesures sont aisément accessibles. Il s'agit de réorganiser le système d'information à protéger de façon à éliminer totalement la potentialité du risque.
* La réduction : on ramène la potentialité et/ou l'impact du risque à un niveau acceptable par la mise en œuvre de mesures techniques et organisationnelles. C'est la solution la plus utilisée.
* Le transfert (ou partage) : la part de risque qui ne peut pas être évitée ou réduite est dénommée risque résiduel. L'organisme peut transférer la responsabilité technique de tout ou partie de ce risque résiduel en recourant à une solution d'externalisation de sécurité. Il peut aussi souscrire une assurance pour diminuer l'impact financier du risque.
* L’acceptation (ou maintien) : ne mettre en place aucune mesure de sécurité supplémentaire car les conséquences du risque résiduel non transférable sont acceptables. Par exemple, le vol d’un ordinateur portable ne comportant pas de données primordiales pour l’entreprise est sans grand impact. Cette solution peut n'être que ponctuelle.

Lorsque la décision de traitement du risque est prise, l’entreprise doit identifier les risques résiduels c’est-à-dire ceux qui persistent après la mise en place des mesures de sécurité. S'ils sont jugés inacceptables, il faut définir des mesures de sécurité supplémentaires. Cette phase d'acceptation formelle des risques résiduels s'inscrit souvent dans un processus d'homologation. Le système étant homologué en tenant compte de ces risques résiduels.

### Mesures de sécurité

La norme ISO 27001 contient une annexe A qui propose 114 mesures de sécurité classées en 14 catégories (politique de sécurité, sécurité du personnel, contrôle des accès…) Cette annexe normative, n'est qu’une liste qui ne donne aucun conseil de mise en œuvre au sein de l’entreprise. Les mesures sont présentées dans la norme ISO 27002.

Phase Do : mise en œuvre et exploitation des mesures de la politique :

Met en place les objectifs. Elle comporte plusieurs étapes :

* Établir un plan de traitement des risques
* Déployer les mesures de sécurité
* Générer des indicateurs
  + De performance pour savoir si les mesures de sécurité sont efficaces
  + De conformité qui permettent de savoir si le SMSI est conforme à ses spécifications
* Former et sensibiliser le personnel

Phase check : mesurer les résultats issus des actions mises en œuvre :

* Audits internes de conformité et d'efficacité du SMSI (ponctuels et planifiés)
* Réexaminer l'adéquation de la politique SSI avec son environnement
* Suivre l'efficacité des mesures et la conformité du système
* Suivre les risques résiduels

Phase Act : Planifier et suivre les actions correctives et préventives

Mettre en place des actions correctives, préventives ou d’amélioration pour les incidents et écarts constatés lors de la phase Check

* Actions correctives : agir sur les effets pour corriger les écarts puis sur les causes pour éviter que les incidents ne se reproduisent
* Actions préventives : agir sur les causes avant que l’incident ne se produise
* Actions d’amélioration : améliorer la performance d’un processus du SMSI.