Guide de reprise informatique

Secrétariat
du Conseil du trésor
Québec

Avis au lecteur

Le présent guide se veut un outil de référence mis à la disposition des organismes publics. Son contenu est présenté à titre indicatif.

Ce guide est disponible sur le site de la Communauté des dirigeants de l'information et leur entourage à l'adresse : https://di.collaboration.gouv.qc/informationnel/obligations/gestion-de-projets/references/.

Le guide de mise en œuvre de la reprise informatique a été rédigé par le :

Sous-secrétariat du dirigeant principal de l'information
Secrétariat du Conseil du trésor
4e étage, secteur 400
875, Grande Allée Est
Québec (Québec) G1R 5R8

Si vous avez des commentaires concernant le présent guide, vous pouvez les communiquer à l'adresse courriel obligationsri@sct.gouv.qc.ca.

Table des matières

1 Objectifs du Guide

En application de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises gouvernementales* (ci-après la Loi) et de la *Directive sur la sécurité de l'information gouvernementale* qui en découle, le dirigeant principal de l'information (DPI) doit soutenir les organismes publics en matière de ressources informationnelles. De plus, la Directive oblige les organismes publics à s'assurer de la mise en œuvre des processus formels de sécurité de l'information permettant notamment d'assurer la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents. Parmi ces processus, la reprise informatique constitue un processus formel permettant d'assurer la disponibilité de l'information et, par le fait même, d'appuyer la continuité des services.

Le présent guide a pour objectif d'outiller les organismes publics dans la préparation d'un plan de reprise informatique. Que ce soit par leur taille, leur mission ou leurs ressources, les besoins et les moyens des organismes publics varient énormément. Considérant cette grande diversité, ce guide ne préconise pas les méthodes à privilégier, mais présente plutôt les éléments à considérer en matière d'élaboration, de mise en œuvre, de maintenance, d'évolution et d'activation d'un plan de reprise informatique.

Ainsi, il appartient aux organismes publics eux-mêmes de cibler les solutions qui correspondent le mieux à leur réalité.

2 Sommaire exécutif

Un grand nombre des services gouvernementaux requièrent l'utilisation de systèmes informatiques. L'importance prise par ceux-ci dans la réalisation des services de mission des organismes publics contribue directement à la dépendance des organisations vis-à-vis des technologies de l'information (TI). De ce fait, la reprise informatique constitue un des outils fondamentaux de la continuité des services. Dans ces circonstances, la préparation d'un plan de reprise informatique efficace permet de garantir la disponibilité des ressources informationnelles aux services de mission qui en ont besoin.

Néanmoins, il importe de bien comprendre le rôle joué par la reprise informatique et ses limites. Un plan de reprise informatique doit répondre aux besoins en continuité des affaires de l'organisation, d'où l'importance d'un plan les définissant précisément.

3 Contexte

3.1 Objectifs du plan de reprise

En cas de sinistre pouvant avoir une incidence sur les ressources technologiques supportant les systèmes de mission, un plan de reprise informatique permet aux organismes publics de se relever rapidement en suivant des procédures établies à l'avance. De plus, par la mise en place d'un plan de reprise informatique efficace, les organismes publics atteignent les objectifs de sécurité touchant la disponibilité de l'information en même temps qu'ils se conforment à la Directive sur la sécurité de l'information gouvernementale.

3.2 Contextes organisationnel et gouvernemental

L'élaboration et la mise en place d'un plan de reprise informatique nécessitent un engagement formel de la haute direction et de l'ensemble des paliers hiérarchiques de l'organisme. Une multitude de compétences sont requises pour en assurer la réalisation. Ainsi, la coopération des lignes d'affaires, des détenteurs d'actifs, des gestionnaires et même des utilisateurs est à prévoir.

De plus, les rôles et responsabilités au niveau stratégique, tactique et opérationnel doivent être clairement définis. En effet, l'efficacité de la reprise informatique repose en grande partie sur une compréhension claire des tâches de chaque intervenant, et ce pour tous les niveaux décisionnels.

Les pratiques de sécurité et le cadre de gouvernance de la sécurité de l'information s'appuient sur les documents structurants suivants :

- La Directive sur la sécurité de l'information gouvernementale
- Le Cadre gouvernemental de gestion de la sécurité de l'information
- Le Cadre de gestion des risques et des incidents à portée gouvernementale

3.3 Clientèle cible

Le Guide de reprise informatique s'adresse tant aux responsables de la gestion des TI qu'à tous les responsables organisationnels touchés par le plan de reprise. Le guide offre une vision globale de la reprise TI permettant aux responsables, conseillers et coordonnateurs organisationnels de prendre les décisions adéquates, le moment venu. De plus, une compréhension claire de la reprise informatique permettra de baliser les choix quant aux solutions retenues, tant d'un point de vue financier que stratégique.

4 Élaboration et mise en œuvre d'un plan de reprise informatique

4.1 Prérequis

L'élaboration et la mise en place d'un plan de reprise informatique ne peuvent être du seul ressort de l'entité responsable de la gestion des TI. La réalisation d'un tel projet exige la contribution et la mobilisation de l'ensemble de l'organisation.

Avant de débuter l'élaboration d'un plan de reprise informatique, plusieurs informations (les services de mission de l'organisme, par exemple) doivent d'abord avoir été recueillies. Elles permettront de déterminer les actifs informationnels qui devront être inclus à la reprise. De plus, cette cueillette permettra de déterminer quelles sont les durées d'interruption et les pertes de données acceptables pour les lignes d'affaires.

La tâche d'identifier les actifs informatiques critiques peut être réalisée par une équipe autre que celle responsable de la reprise. Toutefois, il est primordial que les responsables en gouvernance des TI de l'organisation soient impliqués dans ces travaux, car c'est à eux qu'incombera ultimement la responsabilité d'approuver les priorités du plan de reprise. Le choix de la stratégie de reprise devra impérativement se faire en collaboration avec les lignes d'affaires concernées, afin qu'elles puissent bien en comprendre la portée.

4.2 Identification des actifs critiques

L'article 60 de la Loi sur la sécurité civile (chapitre S-2.3) exige que les organismes publics recensent les services essentiels qu'ils fournissent et qu'ils établissent des mesures pour maintenir ou rétablir la fourniture de ces biens et services en cas de sinistre. Plusieurs de ces mesures se retrouvent à l'intérieur des « Plans de continuité des services

essentiels » (PCSE). Les processus et fonctions mis en relief par le PCSE permettent de déterminer plusieurs des actifs informationnels critiques à la mission des lignes d'affaires.

Cependant, certains services technologiques peuvent ne pas être définis comme des services essentiels, mais être tout de même critiques à l'organisation. Il peut s'agir, par exemple, d'obligations légales ou d'enjeux financiers importants. Dans ces cas, les services essentiels à la population ne seraient pas compromis, mais les impacts pourraient être majeurs pour l'organisation. Dans d'autres circonstances, certains services pourraient s'avérer très importants, mais ne pas nécessiter obligatoirement le support technologique qui s'y rattache.

Ainsi, un inventaire exhaustif des tâches et des services de l'organisation, ainsi que de ses actifs TI, est un préalable essentiel à la mise en place d'un plan de reprise. Pour cette étape, la collaboration de plusieurs membres de l'organisation est nécessaire, dont les ressources TI, les lignes d'affaires, les pilotes et même les utilisateurs. En effet, il est pratiquement impossible pour les responsables de la reprise eux-mêmes de déterminer, seul, ce qui est crucial ou non à l'organisation.

Une fois les actifs informatiques critiques bien identifiés, il est nécessaire d'évaluer les degrés de tolérance de l'organisation face à une interruption des services des TI. Ces degrés de tolérance se traduisent par les paramètres suivants :

- Perte maximale de données[1];
- Durée maximale d'interruption[2];
- Objectif du délai de reprise[3].

La « **perte maximale de données[4]** » représente le point à partir duquel les informations utilisées par une activité doivent être restaurées afin de permettre son fonctionnement à la reprise. La « **durée maximale d'interruption acceptable[5]** » définit le temps nécessaire pour que les impacts défavorables pouvant découler de l'interruption d'un service deviennent inacceptables. L' « **objectif du délai de reprise[6]** » concerne quant à lui la durée après un incident durant laquelle un service doit être repris. Il est à noter que l' « **objectif du délai de reprise** » doit logiquement être plus petit que la « **durée maximale d'interruption acceptable** ».

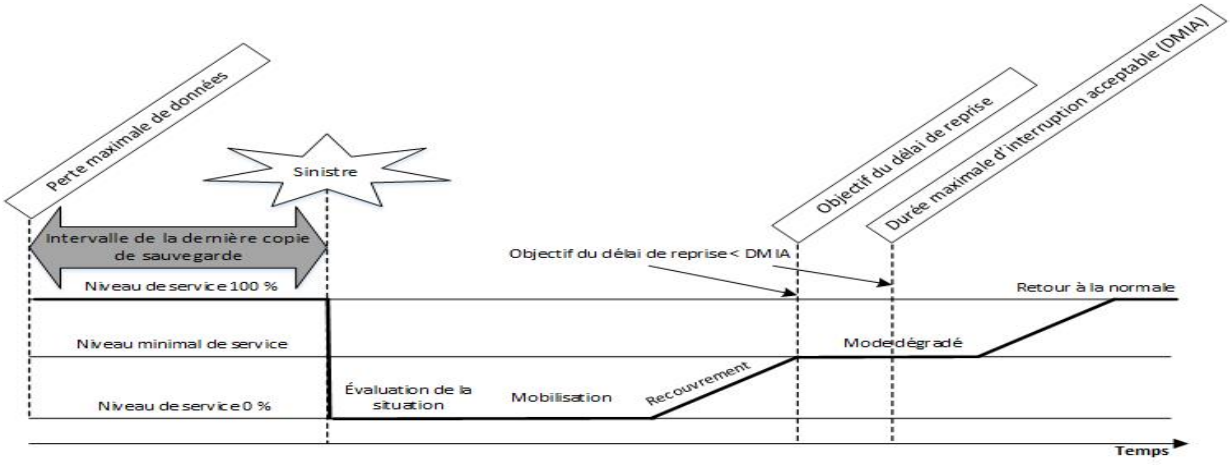

Figure 1 Déroulement et degrés de tolérance d'interruption

[1] Équivalent du *Recovery Point Objective (RPO)*
[2] Équivalent du *Maximum Acceptable Outage (MAO)*
[3] Équivalent du *Recovery Time Objective (RTO)*
[4] ISO 22301, paragraphe 3.44
[5] ISO 22301, paragraphe 3.25
[6] ISO 22301, paragraphe 3.45

L'estimation des degrés de tolérance à l'interruption se doit d'être calculée avec beaucoup de minutie, mais surtout avec l'accord de l'ensemble des lignes d'affaires et de l'organisation. En effet, un niveau de tolérance très bas risque de faire grimper rapidement les coûts de la solution de reprise. À l'inverse, une mauvaise estimation des pertes de données et de l'interruption acceptables pourrait prolonger le délai de reprise au-delà d'un seuil tolérable pour l'organisation. Il s'agit d'une tâche complexe consistant à évaluer de manière juste les besoins de l'organisation afin d'en arriver avec une solution de reprise adéquate, tant financièrement qu'opérationnellement.

4.3 Définition des stratégies de reprise informatique

Lorsque vient le moment de choisir une stratégie de reprise informatique, plusieurs options peuvent être considérées. Le choix de l'une plutôt qu'une autre sera principalement pris en fonction des besoins de l'organisation et des coûts d'une solution satisfaisante.

La nécessité du plan de reprise informatique vient du fait que le risque d'une interruption de service est jugé inacceptable. Dans ces conditions, les options consistent soit à éliminer ce risque, l'atténuer pour le rendre tolérable ou le transférer à un tiers.

Dans la situation où le risque est tolérable, ou supprimable, il n'y a pas de besoin en reprise informatique. Il pourrait s'agir, dans ces cas, d'opérations dont l'interruption n'est pas critique ou dont les processus peuvent être modifiés pour éliminer les risques (ex : virement bancaire plutôt qu'émission de chèques par la poste). C'est lorsque le besoin demeure essentiel, mais que le risque d'une interruption reste inacceptable, qu'un plan de reprise s'impose. Il permettra d'atténuer le risque pour le rendre tolérable.

L'option de transférer, en tout ou en partie, le risque d'une interruption de service, peut parfois être un choix intéressant pour certaines organisations. Par exemple, l'implantation d'infrastructures et de services en infonuagique, ou à l'externe, peut s'avérer simple et avantageux dans certaines situations. Néanmoins, cette solution n'élimine pas complètement le besoin d'un plan de reprise informatique. En effet, l'assurance d'un niveau de service adéquat, qui concorde avec les besoins de l'organisation, doit être garantie pour le fournisseur externe. De plus, les processus de remontage, de copie de sauvegarde, de coordination ou de mobilisation, par exemple, devront aussi être considérés, même en l'absence d'infrastructures TI locales.

4.3.1 Les mesures de sécurité préventives

L'implantation d'un plan de reprise constitue en soi une mesure d'atténuation du risque. Il permet de limiter le délai d'interruption pour le rendre acceptable. Conjointement au plan de reprise, plusieurs autres mesures peuvent être prises pour atténuer encore plus les risques d'interruption.

L'analyse d'impact offre la possibilité de s'assurer que des mesures préventives sont mises en place pour pallier les menaces et vulnérabilités susceptibles d'affecter la disponibilité des services. Il s'agit de contrôles préventifs qui accompagnent les stratégies de reprise informatique et qui facilitent l'atteinte des objectifs de reprise fixés. À titre d'exemple, on peut citer : l'installation d'onduleurs ou de génératrices pour pallier les problèmes de coupures de courant; la mise en place d'un système de lutte contre les incendies ou la bonne disposition des salles de serveurs pour éviter les interruptions dues aux dégâts d'eau.

4.3.2 Copies de sauvegarde et de restauration

La sauvegarde et la restauration des données font partie intégrante de l'offre de service TI de l'organisation. Elles sont aussi des composantes primordiales d'un plan de reprise informatique, et leur absence constituerait un manquement majeur à la sécurité informationnelle. Ainsi, sans en être directement les détenteurs, il incombe aux personnes responsables de la reprise TI de s'assurer que des copies de sauvegarde valables seront disponibles en cas d'activation du plan. Différentes méthodes de sauvegarde peuvent être adoptées selon les besoins spécifiques à chacun des organismes.

4.3.3 Mise en œuvre

Lors de la mise en œuvre du plan de reprise, trois types d'installations[7] s'offrent aux organisations en matière de sites alternatifs de reprise :

- **La salle blanche** (Cold site) : Une salle blanche (ou vide) est une installation de remplacement qui n'est ni aménagée ni équipée de façon opérationnelle. L'équipement doit être configuré et remonté avant de démarrer les activités. Beaucoup de temps et d'efforts sont nécessaires pour rendre une salle blanche complètement opérationnelle, mais c'est l'option la moins coûteuse.
- **Le centre de relève** (Warm site) : Un centre de relève est une installation déjà préparée sur le plan des infrastructures. Cependant, plusieurs heures seront nécessaires pour le rendre complètement opérationnel.
- **Le centre de relève immédiate** (Hot site) : Un centre de relève immédiate est entièrement configuré et aménagé. Il peut être activé en quelques minutes, voire en quelques secondes. Le centre de relève immédiate est l'option la plus coûteuse.

Le choix de l'une ou l'autre de ces stratégies se détermine surtout par la **durée maximale d'interruption acceptable**. Plus le délai de reprise désiré est court, plus la solution devra être rapide et donc coûteuse.

Choix et localisation du centre de traitement alternatif

Selon les besoins et les moyens des organisations, les centres de traitement alternatifs peuvent se situer dans un autre local, sur un autre étage, dans un autre bâtiment, chez une autre organisation ou chez un fournisseur externe (en infonuagique ou dans un CTI partagé). Évidemment, ces options présentent des niveaux d'assurance très variables. Cependant, le choix du site de reprise dépend directement de la tolérance de l'organisation aux risques d'interruption des services TI. Il appartient donc à l'organisme concerné de définir ses risques potentiels et ce qui lui est acceptable ou non pour faire le choix adéquat.

Bien que l'éloignement entre le site principal et le site alternatif soit souvent un gage de sécurité, il peut aussi devenir un handicap. Par exemple, si les intervenants ont à se déplacer à des centaines de kilomètres pendant plusieurs jours pour réaliser la reprise TI, il y aurait une perte d'efficacité pour des gains plutôt minimes. À l'opposé, si le serveur de reprise se trouve dans la même pièce que le serveur principal, le plan fonctionnerait en cas de piratage informatique, mais nullement en cas d'inondation du local. Les options retenues pour le plan de reprise TI doivent donc considérer la garantie contre les risques, mais aussi l'efficacité d'exécution et les coûts qui y sont associés.

Si l'organisation en a les moyens, elle pourrait choisir de louer son centre de traitement alternatif ou d'en être la propriétaire. Cependant, il importe de ne pas éliminer d'emblée certaines stratégies sous prétexte qu'elles pourraient s'avérer trop onéreuses. Une entente de service entre deux organismes, l'infonuagique ou un centre de traitement partagé peuvent être des solutions de reprise efficaces et abordables. L'importance de choisir une solution convenable et adaptée aux besoins de l'organisation demeure toujours la priorité en matière de reprise TI.

Une fois la stratégie de reprise choisie, l'étape du développement proprement dit peut être amorcée. Cette étape comprend généralement l'élaboration des procédures de recouvrement, la documentation de ces procédures et la validation du plan (tenue d'un exercice initial). Cette phase initiale vise principalement à valider si la solution est viable, ainsi qu'à en documenter les processus.

Validation du plan

Malgré une planification et des estimations minutieuses, la réalisation pratique du remontage et du recouvrement TI représente l'unique moyen de garantir que la stratégie de reprise fonctionne réellement. De plus, cette phase

[7] Installation de remplacement - Sécurité publique Canada

« terrain » de l'élaboration du plan permet de déceler les obstacles qui n'auraient pas été anticipés. La tenue d'un exercice initial, suite au remontage et au recouvrement, permet quant à lui de valider que le plan fonctionne du point de vue des techniciens, mais aussi de celui des utilisateurs.

Même s'ils ne concernent pas directement le domaine informatique, plusieurs processus doivent être envisagés en appui au plan de reprise TI[8]. Par exemple, les procédures liées aux communications, à la mobilisation, à la logistique ou au volet décisionnel. De plus, les procédures de reddition de compte, entre les intervenants du plan et la gouvernance, doivent être organisées afin ne pas nuire au déroulement de la reprise.

Sans être entièrement élaborés lors du développement du plan, ces processus peuvent être intégrés aux exercices de reprise TI et ainsi assurer la solidité du plan de reprise TI.

5 Maintenance et évolution du plan de reprise

5.1 Organisation des exercices

De par sa nature, le plan de reprise doit pouvoir être démarré et mis en service en tout temps. Toutefois, l'implantation du plan de reprise ne peut être considérée comme une fin en soi. En effet, après sa mise en œuvre, il est primordial de veiller à son entretien et à son amélioration.

Les infrastructures TI des organisations évoluent constamment, et il doit en être de même pour le plan de reprise informatique. Un excellent moyen permettant d'encadrer cette évolution consiste à le tester régulièrement. Dans cette optique, **un calendrier d'exercices et de tests du plan de reprise informatique** permet de :

- Valider les procédures et processus en place;
- Mettre à jour et corriger le plan;
- Former et sensibiliser le personnel impliqué.

L'élaboration d'un calendrier d'exercices doit être constituée en fonction d'objectifs préalablement définis. Cependant, il est utopique d'espérer une exécution parfaite du plan à la première tentative. En ce sens, le choix d'un objectif général permet de subdiviser l'atteinte de ce dernier en un calendrier d'exercices et de tests périodiques, ayant chacun des objectifs spécifiques différents. Cette planification à long terme permet alors une évolution régulière et réaliste du plan de reprise, tout en l'améliorant constamment.

Planification

Lors de la préparation d'un exercice de reprise, il est important de définir en premier lieu les objectifs spécifiques qui poussent à réaliser ce test. Ces objectifs peuvent être proposés ou définis par l'équipe de reprise, mais aussi par la gouvernance, la gestion et même les lignes d'affaires. Ce qui importe avant tout, c'est que ces objectifs fassent consensus dans l'organisation et que leur atteinte soit réalisable.

En effet, le choix d'objectifs atteignable permet au personnel d'apprivoiser les processus et de consolider le plan de reprise. Toutefois, une séquence logique des objectifs à atteindre, lors des exercices subséquents, permettra de rehausser la solidité du plan de reprise, d'où l'importance d'un calendrier d'exercices et de tests planifié à long terme.

[8] Voir annexe 3.

Types d'exercices[9]

La tenue régulière d'exercices de reprise informatique, surtout si ils impliquent de nombreuses ressources, peut éventuellement recevoir un accueil tiède de certains secteurs de l'organisation. De ce fait, une variation des scénarios et des objectifs, mais surtout des types d'exercices, permet de conserver la mobilisation et la motivation de l'organisation envers le plan de reprise.

Le tableau suivant présente les caractéristiques et avantages des quatre types différents d'exercices.

Types d'exercices		
Types d'exercice	Description	Avantages
Vérification papier	Révision documentaire des processus.	Peu contraignant. Peut être réalisé régulièrement ou lors d'une évolution TI.
Table de travail (*Walk-through*)	Révision du plan de reprise en table de discussion selon un scénario prédéterminé.	Permettent de faire interagir différents processus. Ne perturbe pas les opérations courantes.
Exercice ou test partiel	Exercice de reprise des certains aspects du plan de reprise TI, incluant une reprise « réelle » de certaines composantes. (ex : remontage des serveurs dans un site externe)	Permettent de corriger les procédures de manière fiable. Valide concrètement les processus du plan de reprise.
Test complet	Reprise complète des ressources TI, impliquant les lignes d'affaires et les utilisateurs.	Permettent de garantir le fonctionnement du plan de reprise TI.

Selon le déroulement d'un exercice, rien n'empêche d'en rehausser le niveau de difficulté en intégrant des paramètres tels qu'une étape de mobilisation des ressources ou l'ajout d'incidents imprévus. Évidemment, ces intrants doivent concorder avec des objectifs précis, et non pas être ajoutés sans raison valable.

Afin de tenir à jour et de garantir le fonctionnement du plan de reprise, il est suggéré d'effectuer une révision du plan **une fois par an**[10]. Par la même occasion, la tenue d'un exercice de reprise complet est une excellente opportunité d'optimiser cette révision. Toutefois, la tenue d'autres types d'exercices, ciblant des lignes d'affaires ou des services TI spécifiques, permet de valider en continu le plan de reprise TI. Plusieurs de ces exercices, comme les tables de travail ou la vérification papier, ont l'avantage de pouvoir se dérouler sans perturber les opérations courantes, ce qui permet de les tenir plus fréquemment.

Déroulement des exercices

Lors d'un incident réel, il est fort probable que les ressources et le personnel nécessaire soient entièrement alloués à l'exécution de la reprise. Cependant, lors de la tenue d'un exercice, il est important de prendre en compte que certains services devront continuer leurs opérations. Ainsi, il serait préférable de valider au préalable si l'absence des ressources et de personnel nécessaires n'entrera pas trop en conflit avec le déroulement des opérations.

[9] Voir les définitions à l'annexe 1.
[10] ISO 27301, section 5.5

Même s'il cela peut paraître anodin, l'élaboration d'un scénario est de mise pour encourager la motivation et la participation du personnel. Il leur permet de situer le déroulement de l'exercice et de prendre conscience de l'importance du plan de reprise. Néanmoins, il importe que le scénario soit plausible et cohérent avec les objectifs de l'exercice.

Il n'est pas nécessaire d'élaborer des scénarios extrêmement complexes pour atteindre les objectifs prévus. Par exemple, l'absence d'un ou de deux techniciens clefs, qui ne pourraient travailler que par accès distants pour cause de tempête, complexifierait énormément le déroulement de l'exercice. À titre d'exemple, voici quelques paramètres qui peuvent être considérés pour varier le déroulement des exercices :

- Varier les lieux (inaccessibilité aux locaux habituels);
- Personnels distants (tempête de neige);
- Reprise en infonuagique (infrastructure locale piratée);
- Etc.

Afin de renforcer l'expertise du personnel face à la reprise TI, il est important de s'assurer que les participants varient d'un exercice à l'autre. Cette rotation permet d'assurer la pérennité du plan, mais aussi de favoriser les échanges et le transfert d'expertise.

Suivi

Pendant le déroulement de l'exercice, il est impératif de noter les moments et les durées d'exécution des processus, ainsi que les entraves rencontrées. Une personne attitrée spécifiquement à cette tâche est suggérée. De plus, la communication entre les intervenants et la collaboration de tous les participants sont primordiales à ce stade. Ce sont principalement ces notes prises lors du déroulement de l'exercice qui permettront d'en évaluer la réussite et de faire évoluer le plan de reprise.

5.2 Évolution du plan de reprise

Les actifs TI évoluent en fonction des besoins d'affaires. Ces modifications nécessitent l'adaptation constante du plan de reprise informatique. Pour permettre une évolution adéquate du plan, ce dernier doit être intégré dans les pratiques des unités administratives et dans le processus de gestion du changement de l'organisation. Il importe donc aux lignes d'affaires, mais aussi aux responsables de la reprise, de s'assurer que les processus liés à la reprise soient mis à jour lors de changements significatifs. Cependant, il peut arriver que des impacts sur le plan de reprise soient omis ou négligés. La tenue régulière d'exercices permet de détecter et de pallier ces lacunes.

Cycle de maintenance

Une fois la mise en œuvre du plan de reprise accomplie, la phase de maintenance du plan de reprise peut être démarrée. Une méthode efficace de planification consiste à définir les objectifs d'un exercice en fonction des risques anticipés ou critiques, mais aussi en considérant les résultats des exercices précédents. Cette façon de faire permet de faire avancer le plan selon des objectifs plus ambitieux à chacun des exercices.

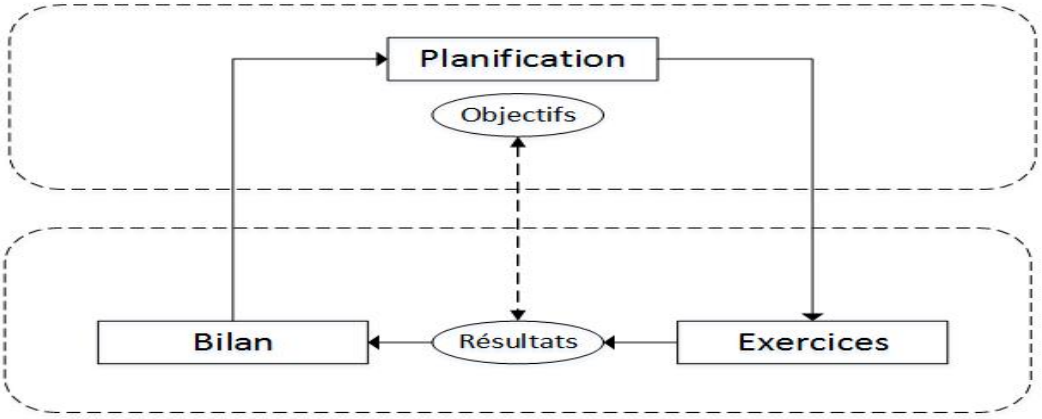

Figure 2 Cycle de maintenance du plan de reprise informatique

La tenue d'un bilan après un exercice et la rédaction d'un rapport est un atout considérable pour l'évolution du plan de reprise. Le bilan avec les participants permet de relever les détails moins apparents lors de l'exercice et de recevoir leurs suggestions pour ceux à venir. Le rapport permet aux gestionnaires et à la gouvernance d'être informés des résultats de l'exercice, en fonction des objectifs établis, et de pouvoir évaluer la maturité du plan de reprise.

Si l'évolution durable du plan de reprise informatique nécessite une vision à long terme, la planification se doit, elle aussi, d'évoluer. La tenue d'exercices ciblés et fréquents permet d'apprivoiser plus facilement les processus du plan de reprise informatique tout en sensibilisant périodiquement l'ensemble de l'organisation.

6 Activation du plan de reprise informatique

6.1 Critères et conditions d'activation du plan

Suite à une perte de service TI, la décision d'activer ou non un plan de reprise dépend principalement de l'évaluation des impacts engendrés par l'incident. Cette évaluation doit permettre aux dirigeants de prendre les mesures nécessaires pour déclarer le sinistre et demander l'activation du plan de reprise.

En plus d'un processus d'évaluation basé sur des critères préétablis, cette étape nécessite l'élaboration préalable d'une procédure d'escalade et d'un processus de mobilisation. Ces processus permettront de déterminer la gravité de l'événement, d'aviser la haute direction et de mobiliser l'équipe informatique s'il y a lieu.

6.2 Exécution du plan

L'exécution du plan consiste à entamer la reprise proprement dite. Cette phase permet la réalisation de la restauration des données et des systèmes suivant les méthodes appropriées, en utilisant les stratégies de reprise préalablement définies par l'équipe de reprise informatique. Les activités de cette phase permettent aussi de communiquer les progrès de la reprise aux personnes concernées et de répondre, si nécessaire, aux besoins de l'équipe.

Certaines situations peuvent exiger beaucoup des équipes impliquées et occasionner un niveau de stress et de fatigue supérieur à la normale, ce qui pourrait engendrer des problèmes supplémentaires. Il importe donc de prévoir les mesures logistiques nécessaires afin de s'assurer que le personnel en place soit pris en charge en cas de besoin.

6.3 Retour à la normale

Le retour à la normale est le processus pendant lequel les activités quittent le mode dégradé de reprise (voir figure 1) pour revenir à l'état antérieur à l'incident. Bien qu'il ne s'agisse pas d'une étape propre à la reprise, il est primordial d'anticiper les actions s'y rattachant le plus tôt possible. En effet, l'octroi des services en mode dégradé peut subvenir aux besoins de la clientèle pour un certain temps, mais il pourrait engendrer de sérieux délai de livraison par la suite.

Ainsi, suite à l'activation d'un plan de reprise, les efforts pour un retour à la situation normale doivent être déployés le plus rapidement possible afin de ne pas faire perdurer les conséquences de l'incident.

6.4 Post-mortem

Cette étape permet de tirer profit des expériences vécues pendant l'incident. Il est profitable que l'ensemble des parties prenantes y participent, car il s'agit d'une bonne occasion de partager les connaissances acquises.

Idéalement, les activités réalisées ont été documentées, principalement les mesures prises et les problèmes rencontrés. Les types de documents pouvant être réalisés pendant le déroulement du plan de reprise informatique sont présentés à l'annexe 3.

Une fois toutes les activités terminées, la rédaction d'un rapport permettra d'informer les dirigeants de manière officielle et assurera la pérennité des connaissances acquises lors de l'incident.

7 Annexes

7.1 ANNEXE I – DÉFINITIONS

Actif informationnel : Tout document défini au sens de l'article 3 de la Loi concernant le cadre juridique des technologies de l'information (L.R.Q., chapitre C-1.1). Cette même loi assimile au document « toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite ».

Aléa : Phénomène, manifestation physique ou activité humaine susceptible d'occasionner des pertes en vies humaines ou des blessures, des dommages aux biens, des perturbations sociales ou économiques, ou une dégradation de l'environnement.

Centre de traitement alternatif : Centre informatique prenant temporairement le relais d'un centre principal rendu indisponible en raison d'un sinistre afin que soit maintenue la continuité des services.

Continuité des services : Capacité d'une organisation d'assurer, en cas de sinistre, la poursuite de ses processus d'affaires selon un niveau de service prédéfini.

Déclaration de sinistre : Acte officiel par lequel un événement est qualifié de sinistre par le comité de crise, ce qui provoque le déclenchement du plan de continuité des services.

Disponibilité : Propriété qu'ont les données, l'information et les systèmes d'information et de communication, d'être accessibles et utilisables en temps voulu et de la manière adéquate par une personne autorisée.

Confidentialité : Propriété d'une information de n'être accessible et divulguée qu'aux personnes ou entités désignées et autorisées.

Intégrité : Propriété d'une information ou d'une technologie de l'information de n'être ni modifiée, ni altérée, ni détruite sans autorisation.

Politique de sécurité : Énoncé général émanant du conseil d'administration et indiquant la ligne de conduite adoptée relativement à la sécurité, à sa mise en œuvre et à sa gestion.

Risque : De manière générale, sans être nécessairement appliqué au domaine de la sécurité de l'information, un risque est une probabilité d'apparition d'une menace qui, dans le cas de l'exploitation d'une situation de vulnérabilité, peut potentiellement avoir un impact sur un actif informationnel (actif ou information) *(Source : Norme ISO/CEI 27005).*

Processus critique : Processus d'affaires ou de soutien nécessaire au bon fonctionnement des services de l'organisme public.

Sinistre : Événement résultant d'un ou de plusieurs aléas, qui cause de graves préjudices aux personnes ou d'importants dommages aux biens et exige de la collectivité touchée des mesures inhabituelles.

Exercice : processus visant à se former, à évaluer, à mettre en pratique et à améliorer les performances au sein d'une organisation.

Test : Un test est un type unique et particulier d'exercice qui intègre l'attente de la réussite ou de l'échec d'un élément parmi les buts ou les objectifs de l'exercice planifié.

Système d'information : Ensemble organisé de moyens mis en place pour recueillir, emmagasiner, traiter, communiquer, protéger ou éliminer l'information en vue de répondre à un besoin déterminé, dont notamment les TI et les procédés utilisés pour exercer ces fonctions.

Plan de continuité des services : Planification stratégique, tactique et opérationnelle comportant un ensemble d'informations et de procédures documentées prêtes à l'utilisation pour assurer la continuité des services d'une organisation.

Plan de reprise informatique : Composante du plan de continuité des services, qui prévoit toutes les circonstances d'arrêt de l'exploitation des ressources informatiques ,de même que les mesures curatives applicables à chacun des cas d'indisponibilité, afin que soit assurée, sur site ou hors site, la continuité des services.

Durée maximale d'interruption acceptable: Temps nécessaire pour que les impacts défavorables pouvant résulter de la non fourniture d'un produit/service ou de la non réalisation d'une activité deviennent inacceptables.

Objectif du délai de reprise : Durée après un incident durant laquelle un produit ou un service doit être repris, une activité doit être reprise ou des ressources doivent être rétablies.

Perte maximale de données : Point à partir duquel les informations utilisées par une activité doivent être restaurées afin de permettre son fonctionnement à la reprise.

7.2 ANNEXE II - NORMES EN APPUI À LA MISE EN PLACE D'UN PLAN DE REPRISE INFORMATIQUE

Le plan de reprise informatique contribue à assurer la continuité des services de mission d'un organisme public advenant une interruption ou une dégradation du fonctionnement des systèmes informatiques qui supportent ces services. Le plan de reprise informatique permet ainsi la poursuite du fonctionnement des processus critiques ciblés par les organismes publics, selon des délais préalablement établis. Pour réaliser le plan de reprise informatique, l'organisme public doit s'appuyer sur une démarche structurée. À cet égard, plusieurs méthodologies et normes reconnues sont recommandées. On peut notamment citer les suivants :

ISO 27001
ISO 27001 : Technologies de l'information- Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences

La norme ISO 27001 fournit des indications sur les mesures à mettre en place en termes de reprise informatique en support à la continuité des services. À cet effet, les sections A.17.1 et A.17.2 tiennent compte des objectifs et mesures de sécurité à mettre en place dans ce contexte. Cette section fournit aussi des contrôles relatifs aux procédures de continuité des opérations, aux plans de reprise d'activité et aux redondances. Cependant, la norme ISO 27001 décrit uniquement ce qui doit être accompli, sans indiquer la façon de le faire. Cet objectif est réalisé par la norme ISO 27031.

ISO 27031
ISO 27031 : Technologies de l'information – Techniques de sécurité – Lignes directrices pour la préparation des technologies de la communication et de l'information pour la continuité d'activité.

Cette norme couvre la reprise informatique et la place dans un contexte de support à la continuité des services. Elle guide les organisations sur les aspects technologiques à considérer lors du développement de la continuité des opérations. Elle décrit aussi les concepts et les principes de préparation des technologies de l'information et de la communication pour la continuité des opérations, et fournit un cadre permettant d'identifier et de spécifier tous les aspects pouvant aider à améliorer la préparation des technologies pour assurer la continuité des activités. Elle s'applique à toute organisation (privée, gouvernementale et non gouvernementale, quelle que soit sa taille) développant son programme de planification de la reprise informatique.

ISO 22301
ISO 22301 : Sécurité sociétale — Systèmes de management de la continuité d'activité — Exigences

Cette norme spécifie les exigences relatives à la planification, l'établissement, la mise en œuvre, l'exploitation, la surveillance, l'examen et la maintenance d'un système de gestion de la continuité des services. Elle aide les organisations à se protéger contre les incidents perturbateurs, à s'y préparer, à y faire face et à se rétablir. Les exigences spécifiées dans ISO 22301 sont génériques et sont destinées à toutes les organisations, ou à des parties de celles-ci, indépendamment du type, de la taille et de la nature de l'organisation. Le champ d'application de ces exigences dépend de l'environnement d'exploitation et de la complexité de l'entreprise.

ISO 27002
ISO 27002 : Technologies de l'information- Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information

La norme ISO 27002 fait partie des normes de la famille ISO 2700X, qui promeuvent les meilleures pratiques de gestion de la sécurité de l'information[11]. La norme ISO 27002 propose une série de contrôles qui suggèrent de tenir compte des risques de sécurité de l'information au niveau de l'organisation.

[11] www.iso.org

COBIT 2019

COBIT 2019 est un cadre dédié à la gouvernance et la gestion de l'information et de la technologie d'entreprise. Ce cadre considère que les objectifs technologiques doivent contribuer à la réalisation des objectifs d'affaires. Il tient compte de 40 stratégies de gouvernance et de gestion. Les stratégies suivantes peuvent être retenues en ce qui a trait à la reprise informatique :

BAI04

Disponibilité et capacité gérées *(Managed availability and capacity)* : Maintenir la disponibilité du service, la gestion efficace des ressources et l'optimisation des performances du système par la prédiction des performances nécessaires et des exigences de capacités.

DSS03

Problèmes gérés *(Managed problems)* : Augmenter la disponibilité, améliorer les niveaux de service, réduire les coûts, améliorer la satisfaction client en réduisant le nombre de problèmes opérationnels, et identifier les causes profondes dans le cadre de la résolution des problèmes.

DSS04

Continuité gérée *(Managed continuity)* : S'adapter rapidement aux situations, poursuivre les opérations commerciales et maintenir la disponibilité des ressources et des informations à un niveau acceptable pour l'entreprise en cas de perturbation importante.

7.3 ANNEXE III – LISTE NON-EXHAUSTIVE DE LA DOCUMENTATION D'APPUI AU PLAN DE REPRISE INFORMATIQUE

Voici, pour information, une liste non exhaustive de document pouvant supporter un plan de reprise informatique :

- Schémas de réseau et configuration;
- Configuration de stockage;
- Configuration de l'application;
- Les détails de sauvegarde / restauration;
- Informations sur les comptes à hauts privilèges;
- Les coordonnées des fournisseurs de services et d'équipements;
- Emplacement du support d'installation et des licences;
- Dépendances avec d'autres services;
- Documentation de l'environnement de récupération, y compris l'emplacement de l'installation de récupération et les composants requis tels que :
    - Alimentation électrique
    - Climatisation
    - Les présentoirs et la connectivité réseau
    - Procédure de récupération de l'infrastructure des données et des applications utilisées par le service, ainsi que toute dépendance à d'autres services
    - Documentation de récupération détaillée pour les processus ou systèmes visés
- Etc.