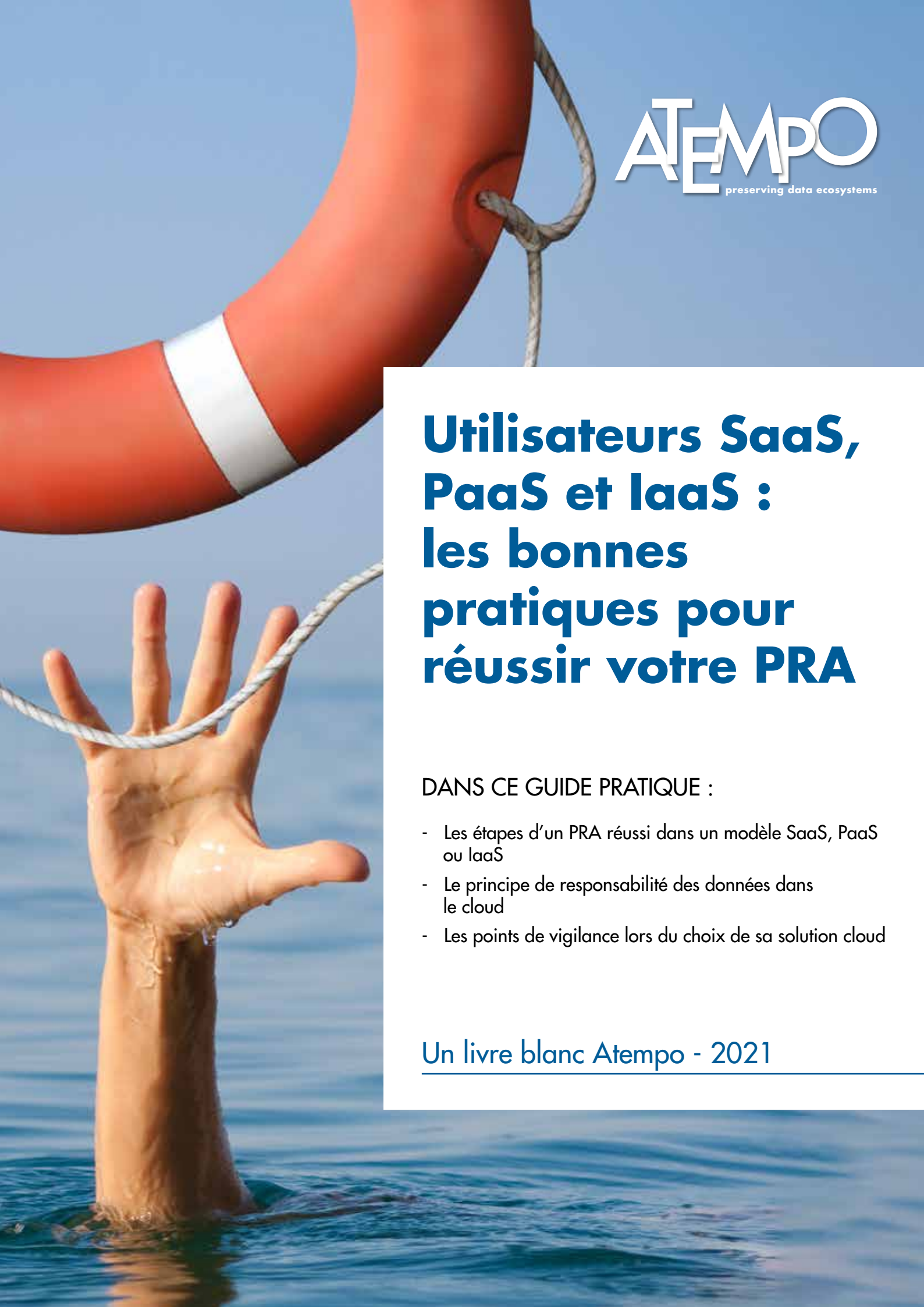


ATEMPO
preserving data ecosystems

Utilisateurs SaaS, PaaS et IaaS : les bonnes pratiques pour réussir votre PRA

DANS CE GUIDE PRATIQUE :

- Les étapes d'un PRA réussi dans un modèle SaaS, PaaS ou IaaS
- Le principe de responsabilité des données dans le cloud
- Les points de vigilance lors du choix de sa solution cloud

Un livre blanc Atempo - 2021

Table des matières

Introduction

Pour sa flexibilité, sa simplicité d'utilisation, ses capacités en matière de stockage et les réductions de coûts qu'il permet, le cloud a séduit une majorité d'entreprises qui ont vu dans cette technologie une évolution positive de leur organisation. Ainsi, au début des années 2010, les entreprises ont adopté massivement la technologie de cloud. Convaincues par les capacités exceptionnelles et les promesses du cloud, de nombreuses organisations ont par excès de confiance ou manque de vigilance, mal évalué l**e périmètre exact de la délégation confiée à leur fournisseur de services.** Par conséquent, elles ont parfois négligé la sécurité de leurs actifs les plus précieux : leurs données.

Les fournisseurs de services cloud offrent de nombreuses garanties pour protéger les données et applications des menaces en matière de cybersécurité ou des pannes matérielles. Mais comme ailleurs, des erreurs humaines ou des malveillances peuvent causer des fuites de données. Les entreprises sont d'ailleurs de plus en plus nombreuses à déclarer des incidents de sécurité dans le cloud. Un autre point qui mérite une attention particulière : les opérateurs de cloud ne sont pas à l'abri des catastrophes naturelles. Ce point est crucial : **les entreprises sont toujours propriétaires de leurs données** et ce, quel que soit leur choix d'infrastructure : local, cloud ou hybride.

Alors comment protéger ses données y compris lorsque l'on a recours à des fournisseurs de services cloud ? Comment mettre en place un plan de reprise d'activité (PRA) afin de relancer son activité lorsque le pire est arrivé ? Comment rester maître de ses données même dans le cloud ? Quels sont les points d'attention sur lesquels s'attarder avant de choisir son fournisseur de services ?

Ce document vous livre les meilleurs conseils sur **la stratégie à adopter et les façons de maintenir la continuité de vos activités en cas d'incident grave lorsque vous mettez en place une délégation de services dans le cloud.**

Chapitre 1 : Mise en situation

La digitalisation des entreprises et la multiplication des activités en ligne ont mené à une explosion du volume des données. Selon IDC, le cabinet de recherche international dans le domaine des technologies, **le volume mondial de données sera multiplié par 3,7 entre 2020 et 2025. Il sera ensuite multiplié par 3,5 tous les cinq ans jusqu'en 2035 pour atteindre la somme de 2142 zettaoctets.** La pandémie de covid-19 et la démocratisation du télétravail ont contribué à accélérer ce phénomène en bouleversant notre manière de travailler et de consommer. Et ce n'est pas tout : l'avènement de la 5G et le développement de l'IoT (Internet des Objets) devraient augmenter davantage la quantité de données produites.

Ces flux croissants de données mettent les infrastructures informatiques des entreprises à rude épreuve. Tout d'abord, ils aggravent le problème de cloisonnement des données. A mesure que la quantité de données produites augmente, les données sont réparties dans les différents départements de l'entreprise. Ces entités communiquent peu ou pas du tout entre elles, et chacune se considère propriétaire de ses données. Pourtant, à l'échelle de l'entreprise, les données sont désormais un atout indispensable pour tous les secteurs. Elles permettent de prendre de meilleures décisions et de gagner un avantage sur la concurrence. L'entreprise prend un risque à conserver un cloisonnement en silos de données : celui de perdre en compétitivité par manque de vision globale. Les organisations ont alors un défi important et complexe à relever : casser les silos de données pour y accéder et ainsi prendre des décisions capables d'améliorer leur performance.

L'autre défi majeur auquel font face les organisations est bien entendu **le stockage de ces volumes croissants de données.** L'arrivée du cloud leur a permis d'accroître leurs capacités de stockage tout en réduisant leurs coûts et leur espace de stockage matériel. Avec la démocratisation du travail à distance, le cloud offre aux collaborateurs une accessibilité aux données, quels que soient leur situation géographique et le matériel utilisé (ordinateur, tablette, etc.). Le cloud agit ainsi en facilitateur du travail collaboratif en permettant à plusieurs personnes d'accéder en même temps sur un même document. La perception trompeuse du cloud qu'ont nombre de dirigeants d'entreprise est que "tout est géré" par le fournisseur de services et seul le service est payant. La réalité est souvent bien plus nuancée.

Comme toute technologie, le **cloud n'est pas infaillible** et les données ne sont pas automatiquement à l'abri. Selon l'enquête Global Data Protection Index, menée par Dell en 2019, **une entreprise sur trois dans le monde a déjà connu une perte de données irréversible.**

À retenir

Une entreprise sur trois dans le monde a déjà connu une perte de données irréversible !

L'actualité nous rappelle régulièrement à quel point un sinistre entrainant une perte de données critiques peut mettre en péril l'existence d'une entreprise : lourdes conséquences financières, risque réputationnel, arrêt d'activité, etc.

Plusieurs catastrophes ayant défrayé la chronique ont mis en exergue les limites des services du cloud : incendie spectaculaire ayant détruit les datacenters d'un célèbre hébergeur français, ouragan ayant ravagé l'île sur laquelle les données d'une entreprise de biotechnologie étaient hébergées dans deux datacenters bien distincts, pannes sévères ayant altéré les services et affecté de nombreux clients d'un acteur majeur du stockage, etc.

Ces évènements impossibles à prédire et aux lourdes conséquences ont été baptisés « cygnes noirs » par le statisticien libano-américain Nassim Nicholas Taleb. Mais qu'il s'agisse de légers incidents ou d'importantes catastrophes, le risque de voir ses données disparaitre doit toujours être pris en compte.

En plus des risques précités, un autre fléau menace les organisations : la cybercriminalité. **Le nombre de cyberattaques, et notamment les attaques de type rançongiciel visant non seulement des entreprises privées mais aussi des villes ou des hôpitaux, a augmenté de 151% au cours des six premiers mois de l'année 2020** selon une étude menée par la firme américaine d'analyses Neustar. Ces attaques font perdre à l'entité visée une quantité de données très précieuses lorsque la rançon n'est pas payée.

Même les sauvegardes permettant de préserver la disponibilité des données quand les autres protections ont échoué, sont désormais la cible des « ransomware ». De fait, les cyberattaques ne figurent plus dans la catégorie « cygnes noirs », leur probabilité d'occurrence étant de plus en plus élevée.

Il devient critique de non seulement protéger l'outil de production et les données, mais surtout d'avoir un plan permettant de reprendre rapidement une activité après un incident.

Malheureusement, de nombreuses entreprises, et particulièrement des structures de petite taille, maîtrisent mal la chaîne de responsabilités. Elles considèrent, à tort, que leur fournisseur de services est responsable de leur écosystème de données. Pourtant, la responsabilité de chacune des parties est mentionnée dans les contrats établis entre les entreprises et leur fournisseur de solution cloud.

La notion de responsabilité partagée est un élément clé du modèle "as a Service". Ce modèle permet de déterminer le rôle du fournisseur de services dans la gestion des serveurs, des applications et bases de données. Il existe cependant une constante : **quelle que soit la forme de délégation choisie par une entreprise, la responsabilité de la protection et de la pérennité des données lui incombe puisqu'elle en est propriétaire.** [2]

À retenir

Quel que soit le mode de délégation choisi (SaaS, PaaS, IaaS), les entreprises sont les seules responsables de la protection de leurs données

Le schéma suivant illustre **le modèle de responsabilité partagée** et montre que quel **que soit le type de délégation (SaaS, PaaS ou IaaS), la sécurité des données revient aux entreprises clientes :**

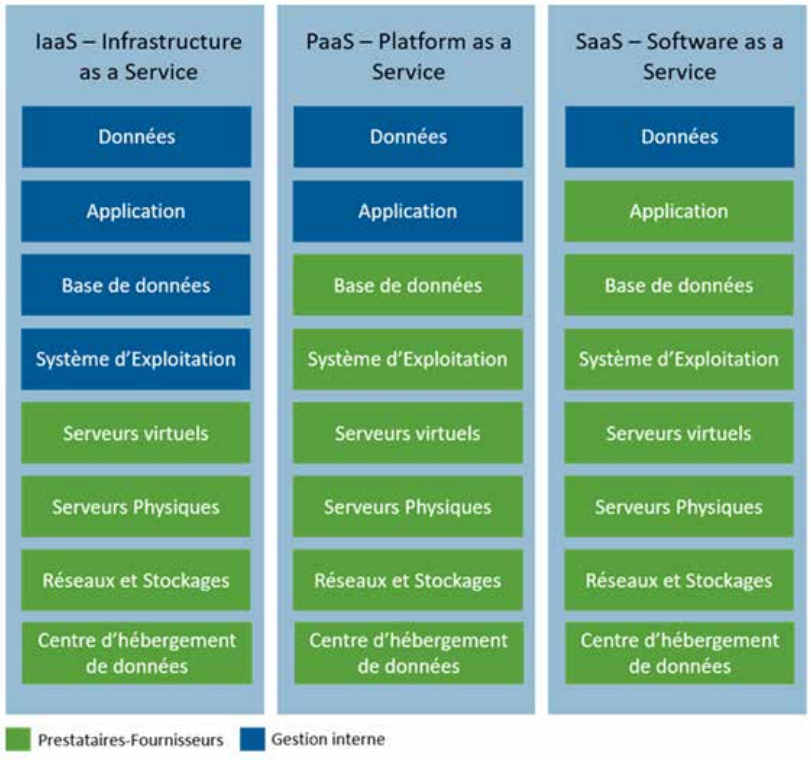


Schéma : Le principe de responsabilité partagée dans les modèles IaaS, PaaS et SaaS

En 2018, la société de conseil Gartner prédisait que **d'ici 2022, au moins 95% des failles de sécurité dans le cloud seront imputables aux clients.** Cette donnée prouve la part très faible de la responsabilité des fournisseurs de services dans la sécurité des données de leurs clients et l'importance pour les entreprises de comprendre que dans le cloud comme ailleurs, tout peut arriver.

La dépendance des entreprises à leur informatique met en exergue la nécessité de protéger leurs données via la mise en place de bonnes pratiques, avant même d'être confrontées à une situation de catastrophe. Celles-ci visent non seulement à protéger les données, mais à les récupérer après un incident et assurer une reprise de l'activité dans les meilleurs délais.

L'élaboration d'un PRA (Plan de Reprise d'Activité) fait partie intégrante de ces bonnes pratiques à respecter et ce, quelle que soit la taille de l'entreprise. Ce plan consiste à gérer les risques et à remettre en route rapidement l'ensemble des activités de l'entreprise en cas de sinistre majeur. C'est une réponse sur le long terme qui permet de revenir à une situation comme avant le sinistre. Le PRA ne doit pas être confondu avec le PCA (plan de continuité d'activité) qui fournit des procédures à mettre en place pour le maintien des activités essentielles de l'entreprise. Le PCA est une solution sur le court terme pour répondre très rapidement à une situation critique.

On estime qu'une entreprise victime d'un incident majeur ayant entraîné la destruction de son infrastructure informatique et la perte de ses données est amenée à disparaître dans 40% des cas, si l'arrêt de son activité a dépassé les 72h. Ce constat nous permet de réaliser l'importance de bien établir un PRA et de le tester en situation réelle, mais surtout de ne pas considérer que son fournisseur de solution assurera la sécurité de ses données en cas de sinistre. En prenant cette précaution, les entreprises sauront protéger ce qu'elles ont de plus précieux et de plus stratégique : leurs données.

À retenir

40% des entreprises dont l'activité a été interrompue plus de 72h après un incident majeur sont amenées à disparaitre

Chapitre 2 : Evaluer les risques et préparer les étapes de votre PRA

En janvier 2009, un Airbus 320 de la compagnie US Airways a subi une panne des deux moteurs après avoir percuté une compagnie d'oiseaux, peu de temps après avoir décollé de l'aéroport La Guardia de New York. L'équipage a pris la décision la plus stratégique et la moins risquée à ce moment-là : faire amerrir l'avion sur l'Hudson river, à l'est de Manhattan. Tout au long du vol, le pilote Chesley Sullenberger et son copilote, Jeffrey Skiles, ont fait preuve d'un calme et d'un courage remarquables. Ils ont même pris le temps de vérifier la procédure d'urgence pour s'assurer qu'ils pourraient se poser sur l'eau à la bonne vitesse et avec la bonne inclinaison de l'appareil. Les décisions prises par les pilotes et l'héroïsme dont ils ont fait preuve lors de l'amerrissage soulignent l'importance de se doter de **procédures spécifiques**, en plus d'une expérience technique (sans oublier une bonne intuition !).

Les catastrophes sont des événements rares mais très stressants, qui impliquent un ensemble de procédures à appliquer pour soit les éviter, soit atténuer leurs impacts. Mais, même sur la terre ferme, des incidents majeurs peuvent survenir. Prenons l'exemple de la perte de tout ou partie de l'infrastructure informatique d'une entreprise. Certes, dans un tel cas, aucune vie humaine n'est à déplorer mais un tel sinistre met en péril l'activité de l'entreprise. Lorsque les équipes IT accèdent à leur plan de reprise d'activité (PRA) après sinistre, elles doivent s'assurer que les actions prises pour remettre en route leurs systèmes informatiques auront le moins d'impact possible sur l'entreprise. Une chose est sûre : **toute tentative de redémarrage des systèmes informatiques sans un suivi des procédures de reprise après sinistre occasionnera une interruption d'activité longue, si ce n'est permanente.** Et dans une telle situation, chaque minute passée entraine de lourdes pertes financières pour l'entreprise...

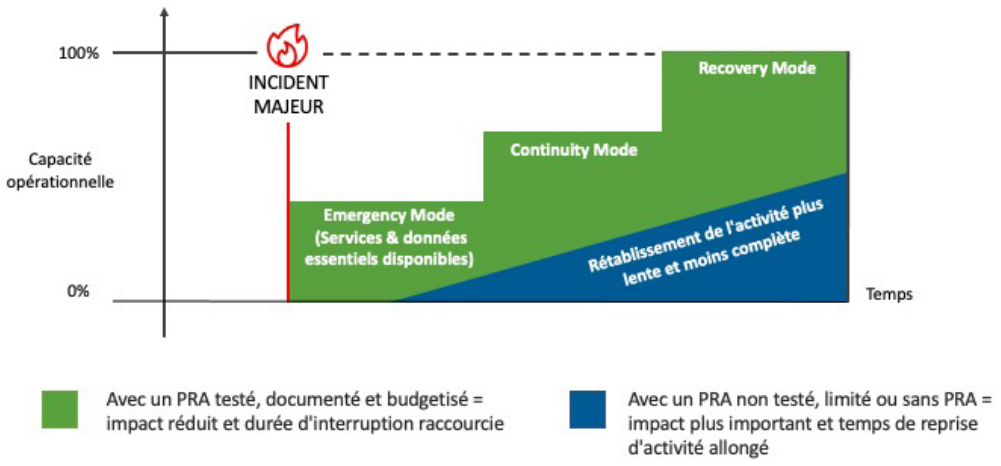


Schéma : Impact du test PRA sur le retour à la capacité opérationnelle et le temps de rétablissement

Alors, qu'est-ce qu'un PRA ? C'est une question vaste et complexe qui ne pourrait être traitée intégralement dans ce guide. Un PRA d'un système informatique est un **ensemble de procédures qui détaillent quelles machines, applications et données doivent être rétablies après un sinistre, et dans quel ordre.** Le document compte entre une dizaine et une centaine de pages et inclut plusieurs procédures de récupération matérielles et logicielles.

La salle dans laquelle se trouve les serveurs est-elle en état de marche ? Y a-t-il de l'électricité ? Peut-on y accéder ? Le réseau est-il disponible ?

En cas de sinistre, qui a la charge de vérifier et exécuter chaque procédure de reprise et dans quel ordre ? Pour déceler des anomalies ou des faiblesses, **chacune de ces procédures devra être entièrement et régulièrement testée, en situation réelle** ou dans des conditions proches d'un incident réel.

À retenir

Chacune des procédures du PRA doit être testée régulièrement en situation réelle

Nous vivons dans un monde hybride dans lequel nos systèmes et nos données se trouvent rarement au même endroit. Par conséquent, le plan de reprise après sinistre fera appel à différentes ressources qui seront plus ou moins impactées. Si un incendie se déclare dans un datacenter et entraine une indisponibilité de l'accès à un serveur web, vous aurez besoin de savoir où se trouve la dernière sauvegarde hors site, comment la restaurer sur un autre serveur web et comment reconfigurer le DNS (système de nom de domaine) pour permettre à vos clients et parties prenantes d'accéder à votre site.

Aucune entreprise ni aucun fournisseur SaaS n'est à l'abri d'un sinistre majeur. Vous vous demandez peut-être ce qu'il se passerait si vous perdiez les données de votre CRM hébergé dans le cloud lors d'une cyberattaque par exemple. A quelle vitesse pourriez-vous restaurer des données à partir d'une sauvegarde hors site et récupérer les données sensibles de vos clients ? Si l'un des datacenters de votre fournisseur IaaS disparaissait, seriez-vous en mesure d'accéder à un serveur de secours ou de revenir à une infrastructure sur site dans un délai acceptable ?

Chaque ensemble de données ou processus métier doit se voir attribuer un facteur de risque. Par exemple, sur une échelle de 0 à 10, quel serait le degré de gravité de l'impact de la perte de vos données ? Quels sont les RPO (objectif de perte minimale de données) et RTO (objectif du délai maximal de reprise) acceptables pour chaque service ?

- Le RPO désigne la quantité de données qu'il est considéré acceptable de perdre lorsqu'une entreprise subit un sinistre.

- Le RTO concerne la durée maximale d'interruption d'un service, d'une application ou d'un ensemble de données acceptable.

L'interruption d'activité dépend de l'entreprise. Elle pourra être de quelques secondes pour une application bancaire, de quelques heures pour une messagerie ou d'une semaine et plus pour des documents RH. Puisqu'il est très coûteux de disposer de plusieurs copies de ses données, il est rarement possible d'avoir un ratio RPO/RTO proche de zéro (c'est à dire avec aucune perte de données et un redémarrage de l'activité immédiat).

Plus les temps de RPO et RTO seront faibles, plus les coûts seront élevés.

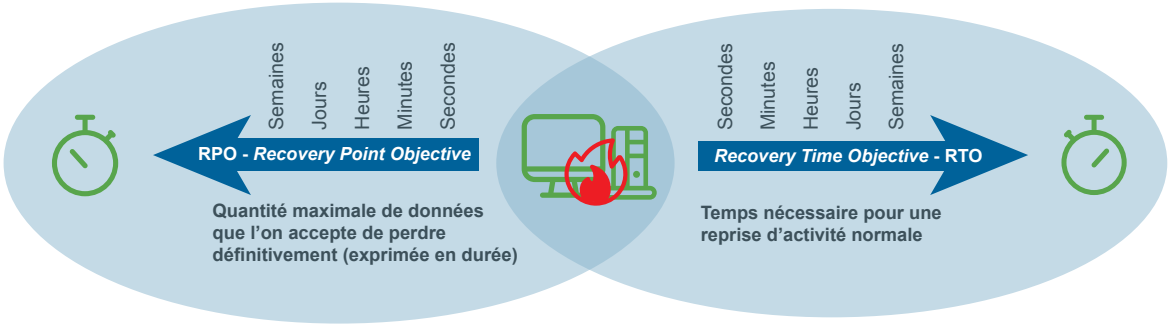


Schéma : RPO ou RTO, la différence

Des décisions doivent donc être prises et les coûts de chaque PRA évalués. En cas d'incident majeur, combien coûtera l'interruption d'activité d'un service à l'entreprise ? Comme évoqué dans la première partie de ce document, la responsabilité des données incombe aux entreprises qui en sont propriétaires. N'importe quel avocat vous le dira : plus c'est écrit petit, plus c'est important !

Nous vous recommandons de bien lire vos contrats et de passer en revue les SLA (le contrat ou la partie du contrat par laquelle un prestataire s'engage à fournir un ensemble de services à un ou plusieurs clients). Si cela est nécessaire, renégociez-les et adaptez-les à vos besoins. L'évaluation des risques et les procédures de PRA font partie intégrante de plusieurs normes internationales de sécurité, notamment ISO 27001 et font l'objet d'obligations imposées par les assurances dans certains métiers et secteurs d'activité.

Mais même en respectant des normes et en empilant les polices d'assurances, que vous soyez dirigeant d'entreprise ou DSI, vous **continuez à être le garant ultime des données de vos clients, patients ou employés.** Donc mieux vaut un PRA le plus sûr et le plus testé possible...

Pour résumer les différentes étapes d'accès et de reconstruction des applications internes et externes, mais aussi des systèmes (sur site, cloud, IaaS, SaaS, etc.), voici ce que vous devez retenir :

- **Comprendre et identifier les impacts potentiels** au cas par cas ;
- **Evaluer les risques** liés à la perte de données ;
- **Identifier les RPO/RTO acceptables** pour chaque département et application dans l'entreprise ;
- **Evaluer le coût en fonction de la criticité des données et applications** (référentiel de sauvegarde sur les technologies de type Worm...) ;
- **Tester entièrement et régulièrement le PRA**, y compris avec ses fournisseurs de service ;
- S'assurer que ses fournisseurs de service restent en activité et respectent les règles du jeu ;
- Etc.

À retenir

Les 3 clés d'un PRA réussi :

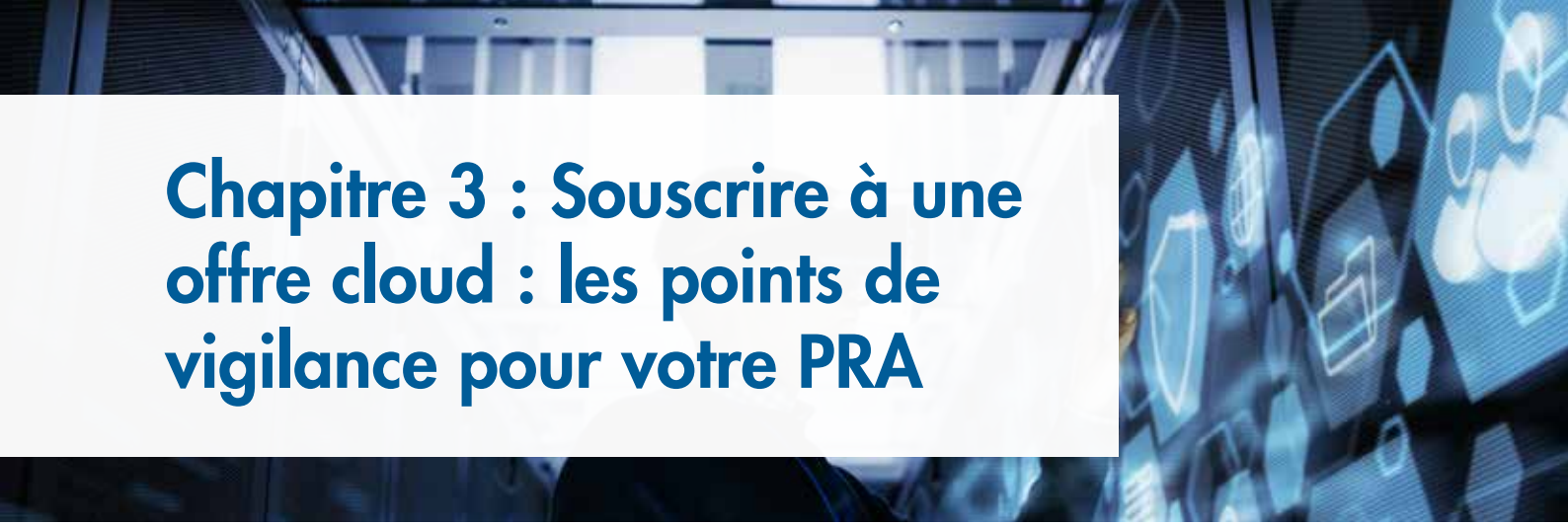
L'évaluation des risques, les procédures spécifiques et les tests de PRA sont coûteux en temps et en argent. La procédure dans son intégralité dépasse souvent le périmètre d'un responsable IT et même d'une équipe IT au complet. La direction et les délégués à la protection des données (DPOs) sont les personnes clés si un tel scénario est amené à se produire. Vous pouvez obtenir de l'aide en faisant appel à :

Des cabinets de conseil qui peuvent se rapprocher des parties prenantes et les aider à élaborer un PRA partiel ou complet ;

Des partenaires technologiques et **des intégrateurs** qui peuvent garantir la disponibilité de nouvelles ressources logicielles et matérielles;

Des solutions de protection et de reprise après sinistre. Elles sont la pierre angulaire de tout PRA. Choisissez judicieusement votre solution et testez votre PRA régulièrement et en conditions réelles.

Chacun des points évoqués ci-dessus constitue la politique de protection des données d'une entreprise en cas de sinistre majeur, une situation que vous espérez ne jamais connaître !



Chapitre 3 : Souscrire à une offre cloud : les points de vigilance pour votre PRA

Quelle que soit la forme de services cloud à laquelle elle souscrit, qu'il s'agisse de l'utilisation d'une plateforme SaaS, PaaS ou de services IaaS, l'entreprise est le maître d'œuvre de la réflexion à la mise en place de son PRA. Il existe **8 points cruciaux sur lesquels nous vous recommandons d'être vigilant** lors des différentes étapes de la réflexion à la mise en place d'une **délégation auprès d'un fournisseur de services cloud :**

LA LECTURE DES CONTRATS

Le premier réflexe à avoir est de faire relire l'ensemble des contrats de délégation opérationnelle à votre service juridique. Gardez en tête que saisir une cour située aux Etats-Unis peut vous coûter très cher. Cependant, la lecture des contrats n'est pas seulement à réserver à vos équipes juridiques.

Certains points doivent être soigneusement étudiés par la direction informatique, en particulier le niveau et le périmètre du service. Contrairement aux idées reçues, un service cloud n'implique pas automatiquement une haute disponibilité de vos applications ou une réplication automatique de vos données, ni même l'externalisation de vos sauvegardes ou la sauvegarde automatique de vos données. Par conséquent, il convient d'être vigilant et de bien lire les contrats établis avec chaque fournisseur de services. Vérifiez particulièrement :

1. **Le périmètre du service :** Est-il question de garantir un accès à une machine physique ? À une machine virtuelle ? A une application ? Quel est le nombre précis d'utilisateurs ? Etc. ;

2. **Le niveau de service (SLA)** fourni concernant les applications. Si la clause est absente, nous vous conseillons de la faire ajouter afin de définir les niveaux de qualité du service à fournir et en particulier, le taux de disponibilité ou d'indisponibilité à garantir par le fournisseur de services. Gardez en tête que 99% de disponibilité représente en réalité un arrêt de service possible de 7,2 heures par mois !

À retenir

Faites relire attentivement vos contrats à votre service juridique

Le tableau ci-dessous-vous donne une grille de lecture de ces métriques en les traduisant en temps d'arrêt annuel ou mensuel. Précisez les plages horaires de ces disponibilités (365 jours et 24 heures par exemple) et les plages de maintenance autorisées. Pensez également aux pénalités concernant les clauses de taux de service à respecter. Si le taux de disponibilité du service est important pour votre activité, n'hésitez pas à inciter fortement votre fournisseur de services à le respecter.

TAUX	TEMPS D'ARRÊT PAR AN	TEMPS D'ARRÊT PAR MOIS
99%	87 heures, 36 minutes, soit plus de 3 jours et demi	7,2 h
99,9%	8 heures, 45 minutes, 36 secondes	43,2 min
99,99%	52 minutes, 33,6 secondes	4,32 min
99,999%	5 minutes, 15,36 secondes	25,9 s
99,9999%	31,68 secondes	2,5 s

3. Les engagements pris concernant la protection de vos données.

Voici quelques exemples intéressants de tournures de phrase qu'il est préférable d'avoir déjà lu pour éviter toute surprise : "en cas de force majeure, le contrat se résilie automatiquement après un mois", "le client doit faire ses propres sauvegardes" ou encore "le client est responsable de l'externalisation de ses sauvegardes".

Pour la dernière étape de cette partie contractuelle, pensez à faire valider vos contrats de délégation opérationnelle par un juriste. Ce dernier aura une lecture complémentaire à l'approche "informatique" et pensera automatiquement à contrôler la juridiction.

Saisir une cour de justice aux Etats-Unis peut vous coûter très cher. Vous pouvez procéder de même avec votre assureur, il est toujours préférable de recueillir son avis avant un sinistre.

LA PROTECTION DES DONNÉES

Il est très important de comprendre qu'une réplication n'est pas une sauvegarde de vos données et ne vous protège pas de la perte de celles-ci ou de leur compromission par un "malware".

4. La réplication de données consiste soit à assurer l'accès à des applications ou des données, soit à mettre à disposition plusieurs copies des données de l'entreprise sur différents stockages pour en partager l'accès à la donnée depuis plusieurs sites, sans interférer avec les travaux des autres. Certaines réplications sont réalisées en temps réel (réplication synchrone), d'autres à intervalles réguliers (réplications asynchrones).

Certes, les réplications impliquent une copie des données mais il faut garder à l'esprit qu'elles ne capturent qu'une version à date et ne permettent pas de reconstruire un historique. La sauvegarde, à l'inverse, capture les données à intervalles de temps réguliers et dans la durée.

Elle permet de remonter le temps sur une période prédéfinie et de restaurer les données telles qu'elles étaient à un instant T, individuellement ou dans un ensemble cohérent. La sauvegarde est l'outil de base de tout plan de reprise d'activité.

5. L'offre du fournisseur cloud que vous envisagez décrit très probablement un système dédié à la sécurité de vos données ou mentionne même le mot "sauvegarde". Nous vous recommandons d'être curieux.

Gardez en mémoire les bonnes pratiques de référence listées ci-dessous car tout compromis aura des conséquences sur la pérennité de vos données et de votre entreprise.

La sauvegarde 3-2-1-1

- La règle est la suivante : créez trois copies de vos données, stockez vos copies sur au moins 2 types de support de stockage, stockez l'une de ces copies hors site et une autre hors ligne.

La mise hors ligne est à réaliser en appliquant le principe d'isolation "Air Gap", soit en déplaçant une copie pour qu'elle soit physiquement isolée et externalisée (disque amovible ou bande mise au coffre), ou soit par une isolation « fonctionnelle » (serveur arrêté pour que l'accès réseau ne soit pas actif). La sauvegarde « Air Gap » garantit ainsi que la copie de sauvegarde ne puisse être altérée ou effacée.

Schéma : Bonnes pratiques : Sauvegarde 3-2-1-1

- Les durées de rétention (périodes de garde) de vos sauvegardes doivent être longues. Ne raccourcissez jamais la rétention, même si celle-ci a un coût. Si le coût de stockage de ces sauvegardes est une préoccupation, choisissez une solution de sauvegarde disposant à minima d'une déduplication des sauvegardes "at rest", c'est à dire sur le stockage propre à la solution de sauvegarde.

Le principe est de « dédoublonner » le stockage tout en permettant de reconstruire l'information à la demande. Gardez en tête qu'une déduplication sera plus performante qu'un système de compression utilisé seul.

Dans l'idéal, combinez déduplication et compression. Faites le test des bénéfices en termes de volume de stockage et n'oubliez pas de prendre en compte l'impact « temps » induit par l'empilement de ces deux couches de traitement qui peut significativement ralentir les traitements.

Pensez également à la conformité aux lois et régulations auxquelles votre entreprise est soumise, en particulier :

6. Les obligations faites aux dirigeants d'entreprise liées à la mise en place de procédures de sécurisation des systèmes d'information. Notez que la responsabilité pénale peut être engagée en cas de problème avec les données de l'entreprise (Article 226-17 du Code Pénal).

7. Le RGPD. Avec ce règlement, l'Europe régule sérieusement les conditions de stockage des données personnelles de ses ressortissants. Une « infraction » peut vite arriver en souscrivant à une offre SaaS qui semble opérée en Europe mais qui est en réalité fournie par une société soumise à des lois hors de l'UE.

Rappelons qu'en cas de non-respect des règles du RGPD, les entreprises s'exposent à une amende de 2 à 4% de leur chiffre d'affaires annuel. Pensez à solliciter un DPO (délégué à la protection des données) pour valider vos délégations et leur conformité avec le RGPD.

Pour éviter toute déconvenue, nous préconisons de choisir en amont un prestataire qui localise les données dans un pays de l'UE et qui est soumis à la réglementation européenne.

8. Le cas échéant, il peut être bon de prendre du recul et de reconsidérer les choix faits d'un point de vue géopolitique et économique (souveraineté technologique) selon votre engagement ou votre activité.

Conclusion

Vous l'aurez compris, les catastrophes sont inhérentes à la vie de votre entreprise et le cloud n'est ni plus ni moins qu'une technologie faillible composée de plusieurs machines garantissant un service. La protection de vos données, votre actif le plus précieux, passe par une bonne compréhension du périmètre de la délégation confiée à votre fournisseur de solutions. Ainsi, que vous utilisiez une offre de services SaaS, PaaS ou IaaS, les données sont toujours sous votre responsabilité.

Un autre grand défi pour votre entreprise concerne la prévention des risques et votre capacité à continuer à opérer après un incident majeur. La préparation d'un PRA aussi complet que possible décrivant les procédures à appliquer pour relancer rapidement votre activité et atténuer les conséquences dévastatrices du sinistre, est cruciale. Bien entendu et puisque la théorie n'a de sens sans la pratique, ce plan devra être testé aussi souvent que possible en conditions réelles et réajusté au besoin. Mais d'autres bonnes pratiques telles qu'une lecture scrupuleuse de vos contrats de délégation, des sauvegardes régulières de vos données ou le choix d'un fournisseur de solution soumis à la réglementation européenne vous éviteront les déconvenues.

Dans ce contexte et afin d'adresser ces défis, il devient à la fois capital et urgent de vous faire accompagner par un partenaire européen, expert de la protection des données et de la reprise d'activité après sinistre.

À propos d'Atempo

Atempo, éditeur de logiciels français et leader européen avec une présence internationale, propose des solutions pour sauvegarder, archiver, déplacer et restaurer les données critiques de milliers d'entreprises dans le monde. Avec plus de vingt-cinq années d'expérience dans la protection des données, Atempo propose une gamme complète de solutions éprouvées pour la sauvegarde des serveurs physiques et virtuels, des postes de travail et la migration entre différents stockages de très gros volumes de données. Les trois solutions phares d'Atempo, **Lina**, **Miria** et **Tina**, sont labellisées '**Utilisé par les armées Françaises**' et '**France Cybersecurity**'. Sélectionné dans le cadre du programme Alumni French Tech 120 destiné à faire émerger 25 licornes d'ici 2025, l'entreprise, dont le siège social se trouve à Paris, dispose d'un puissant réseau de grossistes

Pour plus d'information : www.atempo.com