Avant-propos

La résilience humaine a toujours été fascinante, cette capacité de survie permettant de transcender les plus grandes tragédies humaines.

Les entreprises et organisations publiques (que nous appellerons organismes, tout au long de cet ouvrage) évoluent dans un environnement de plus en plus instable, les crises se succédant, toutes en diversité et en complexité. Dans ce contexte, les organismes se sont, progressivement mais résolument, engagés dans une démarche de résilience, en se dotant notamment d'un plan de continuité des activités (PCA).

Cet ouvrage n'a pas la prétention d'être exhaustif. Son ambition est double.

Il s'agit, tout d'abord, de livrer une méthode complète, éprouvée et pragmatique, pour guider utilement des organismes qui souhaiteraient s'inscrire dans cette démarche de résilience et s'équiper d'un plan de continuité des activités, pour affronter le pire, avec efficacité. Ce dispositif, véritable outil stratégique, permet d'organiser de façon opérationnelle la reprise des activités les plus vitales d'un organisme, quand celui-ci se trouve confronté à une crise majeure impactant gravement son fonctionnement.

Nous avons également souhaité évoquer l'émergence du nouveau paradigme de la résilience des organismes. Face à de nouveaux enjeux sociétaux, à des risques systémiques, à l'émergence de crises « hors cadre », à un contexte en rupture avec un environnement stable, les organismes glissent progressivement de l'incertitude vers l'inconnu.

Dans une nouvelle société technologique de l'instant et du mouvement, ils doivent, désormais, pouvoir faire face à des crises complexes, d'ampleur sans précédent, du fait de menaces interconnectées, créant complexité et effets dominos, potentiellement dévastateurs. En effet, il est désormais incontournable d'appréhender des menaces de natures très différentes : cyber, rupture technologique, climatique, accès aux ressources, sanitaire, géopolitique ou encore de sûreté, amplifiées par une déferlante des médias. L'ensemble de ces

ingrédients impose donc une approche largement renouvelée. À l'heure où nous écrivons cet ouvrage, la crise sanitaire du coronavirus (Covid-19) illustre parfaitement ces enjeux chaotistiques mondiaux.

Aujourd'hui, la résilience des organismes, capacité intrinsèque à transcender l'adversité, implique d'adapter les dispositifs de réponse existants aux évolutions de l'environnement, aux nouvelles menaces. Elle exige, surtout, de s'appuyer désormais sur l'Humain, au travers notamment du développement de capacités et de coopérations nouvelles, le tout dans une approche objectivement optimiste, doublée d'une détermination sans faille.

Comme le disait André Malraux : « Le courage est une chose qui s'organise. »

Partie I
Le plan de continuité des activités, une nécessité… pour faire face à un sinistre majeur

La continuité d'activité est une discipline apparue relativement récemment dans les organismes.

Après les événements de mai 1968, la notion de secours informatique a commencé à voir le jour de façon timide. En France, quelques centres de secours informatiques, tout d'abord mutualisés, apparaissent dans les années 1970-1980, avec pour objectif principal de pallier l'indisponibilité physique du système d'information face aux sinistres, les plus redoutés à l'époque, à savoir l'incendie et l'inondation.

Le grand *black-out* électrique de 1977 aux États-Unis, conjugué à l'avènement de l'informatique dans les organismes, a permis d'impulser la notion de plan de secours informatique mutualisé, notamment chez les premiers grands constructeurs informatiques américains. Les outils de secours informatiques et la mise en place de systèmes de sauvegardes se concrétisent aux États-Unis dans les années 1980.

C'est au cours des années 1990 que l'on assiste progressivement à l'apparition d'un besoin de continuité, côté utilisateurs, pour compléter les outils de secours informatique.

L'incendie du Crédit lyonnais en 1996, qui a eu des impacts directs sur l'activité des salles de marché, a généré en France une vraie prise de conscience du besoin de secours utilisateurs, d'une culture de crise et, donc, de continuité des activités, peu d'organismes du tertiaire disposant d'un PCA à l'époque. Ce courant sera bientôt renforcé par les craintes de dysfonctionnements majeurs du fait du passage à l'an 2000, nombre d'organismes ayant mis en place des dispositifs d'envergure pour pouvoir réagir et permettre la continuité des activités en cas de « *bug* informatique ».

La vraie prise de conscience mondiale de la nécessité de mettre en place un dispositif de continuité des activités dans les organismes a émergé à la suite des attentats du World Trade Center du 11 septembre 2001 à New York. Le décès de 2 750 personnes, la présence de quelque 350 entreprises et la destruction complète de quelque 800 000 m^2 de bureaux ont mis en évidence le caractère indispensable de prévoir le pire, pour la survie des hommes et des organismes, face à des événements absolument inconcevables jusqu'alors.

Le 11 septembre 2001 a provoqué un changement de paradigme pour la continuité des activités dans le monde. La notion d'impérieuse nécessité de se préparer au pire a donc vu le jour de façon brutale, mais incontestable dans les organismes.

Certains événements majeurs sont venus ensuite confirmer et amplifier cette nécessité de s'organiser et de se préparer : tsunami en Indonésie le 26 décembre 2004, attentats de Londres en 2005, risque de pandémie H1N1 en 2009 et, surtout, le séisme suivi d'un tsunami et d'une catastrophe nucléaire à Fukushima au Japon le 11 mars 2011. Cette dernière catastrophe a illustré, de façon magistrale et dramatique, les effets dominos, qui, en l'espèce, n'ont pas été pris en considération dans les travaux de prévention, car jugés bien trop irréalistes.

Ces événements dramatiques ont permis d'intégrer, dans les consciences des organismes, que l'imprévisible pouvait se produire avec des impacts catastrophiques, tant sur le plan humain qu'économique.

Le Printemps arabe (2011), le virus Ebola (2014), les vagues d'attentats, notamment en France en 2015 et 2016, et, ces dernières semaines, la crise du coronavirus, n'ont fait que confirmer la multitude des risques et l'ampleur des conséquences exposant potentiellement les hommes, les sociétés et les organismes.

Les enjeux de continuité sont ainsi apparus clairement et ont mis en lumière deux prises de conscience essentielles pour les organismes : tout d'abord, la nécessité de se préparer au pire, de renoncer à l'improvisation pour développer une véritable capacité de résilience, gagner un temps précieux et, enfin, la nécessité d'intégrer un devoir d'humilité face à ces événements parfois inconcevables, la préparation ne faisant qu'augmenter les chances de succès, malheureusement sans promesse de résultat.

La continuité des activités apparaît de nos jours comme un nouvel outil de pérennité pour les organismes. Avec cet outil, ils disposent d'une organisation spécifique, limitant les impacts d'une crise, tout en augmentant la confiance de leurs parties prenantes et en améliorant leur résilience. Face à des risques majeurs, mais de probabilité très faible, la responsabilité et le pari de Pascal[1] doivent, malgré tout, inciter nos organismes à prendre au sérieux ces risques et donc s'engager pour pouvoir y faire face.

Le célèbre psychiatre Boris Cyrulnik[2], au sujet de la résilience humaine, indique que : « C'est dans la souffrance que l'on est contraint de faire un choix crucial : ou bien l'on reste mort, ou bien l'on se remet à vivre. » À la différence des individus, pour les organismes, ce choix ne peut être fait qu'en amont de la crise, car le jour J, il est déjà trop tard et souvent seuls les enjeux de mort demeurent.

1 Le pari de Pascal est un argument philosophique mis au point par Blaise Pascal, philosophe, mathématicien et physicien français du XVII[e] siècle. L'argument tente de prouver qu'une personne rationnelle a tout intérêt à croire en Dieu, que Dieu existe ou non. En effet, si Dieu n'existe pas, le croyant et le non-croyant ne perdent rien ou presque. En revanche, si Dieu existe, le croyant gagne le paradis tandis que le non-croyant est enfermé en enfer pour l'éternité. (Source : Wikipédia)

2 *Interview* sur France Inter du 12 avril 2019.

1
La définition et les éléments de contexte

1.1 La définition du PCA

La première définition du PCA, retenue par le *Journal officiel* (26/04/2004) identifie « un ensemble de mesures visant à assurer, selon divers scénarios de crises, y compris face à des chocs extrêmes et le cas échéant de façon temporaire, en mode dégradé, des prestations de services essentiels de l'entreprise puis la reprise planifiée des activités. »

Cette définition, déjà bien aboutie, a été complétée en 2012 par une définition de la norme NF EN ISO 22301[3] qui retient le PCA comme : « La capacité de l'organisme à poursuivre la production de produits ou la prestation de services à des niveaux prédéfinis acceptables après un incident perturbateur. »

Nous retiendrons que le plan de continuité des activités (PCA) est un ensemble de mesures et de moyens, garantissant la continuité des activités vitales, afin d'assurer la résilience, voire la survie d'un organisme, à la suite d'un sinistre majeur de toute nature.

1.2 Les éléments de contexte

1.2.1 La notion de sinistre majeur

Le PCA doit permettre de faire face à des événements significatifs par leur ampleur et/ou leur gravité, c'est-à-dire des événements majeurs, voire des crises. Il convient donc de distinguer l'événement (qui est juste un changement) d'un incident, qui conduit potentiellement à un état différent (crise, urgence, déstabilisation forte).

3 *Sécurité et résilience – Systèmes de management de la continuité d'activité – Exigences*, article 3.3, AFNOR, novembre 2019.

Dans le cadre de la construction d'un PCA, on considère que le sinistre est inéluctable, qu'il se réalisera et donc perturbera de façon significative l'organisme. Il est essentiel de partir du postulat que le scénario de sinistre majeur redouté se réalisera, car cela signifie l'abandon d'une approche classique de prévention, de diminution du risque et donc d'évitement du sinistre, pour adopter une véritable posture de riposte face au risque.

Habitués, jusqu'à présent, à adopter des logiques de « rempart » pour éviter la réalisation des scénarios redoutés, les organismes doivent désormais se préparer à la survenance du pire. Cela ne veut pas dire pour autant que l'organisme renonce à toutes les actions de prévention. Néanmoins, avec cette approche d'humilité, on considère que la prévention ne sera pas suffisante pour épargner l'organisme.

Face à la réalisation du sinistre, le PCA nous permettra de nous organiser, de nous adapter à cet environnement complexe et évolutif, pour pouvoir en atténuer les conséquences les plus funestes.

1.2.2 Une approche sous un angle "*worst case*"

Quel niveau de gravité doit-on retenir dans le cadre des travaux de construction du PCA ? Doit-on volontairement se mettre dans la situation opérationnelle la plus critique ou retenir une période plus calme, car plus fréquente sur l'année ?

Ne sachant pas quel événement l'organisme est susceptible de rencontrer, il est communément retenu par les experts de la continuité de se positionner dans la position du "*worst case*", c'est-à-dire de la situation la plus défavorable pour l'organisme, même si celle-ci ne se retrouve que sur une période très limitée dans l'année (taux d'absentéisme majeur, période de recouvrement unique auprès de clients, etc.). On peut envisager de construire des plans sur différents niveaux d'indisponibilité, partielle ou totale. Si cette approche a du sens, il n'en demeure pas moins qu'il est indispensable de commencer par une couverture du scénario le plus majorant pour l'organisme.

Le besoin de couvrir plusieurs niveaux de dégradation peut, à la suite de l'analyse des risques, mettre, par exemple, en évidence des impacts considérables en cas de dégradation partielle du système d'information, l'organisme ne pouvant se satisfaire de certains services en mode dégradé. L'objectif n'étant pas de s'organiser pour faire face à un incident mineur, il est important de se fixer comme objectif principal de gagner en robustesse face à un événement tout à fait majeur et dans des circonstances les plus défavorables.

Le domaine de la continuité ne doit laisser aucune place à la chance. On évoque souvent la loi de Murphy[4], qui illustre parfaitement les objectifs de contexte qu'il convient de retenir dans la réalisation de ces travaux de modélisation.

1.2.3 Une reprise des activités réduite à l'essentiel, dans un mode dégradé

Le PCA projette l'organisme dans une situation extraordinaire, au sens premier du terme, la dose létale redoutée étant souvent en lien avec l'autorisation réglementaire d'exploitation. Il s'agit, pour chaque organisme, par temps calme, de faire des choix stratégiques, décisifs pour sa survie et de planifier sa réaction en cas de survenance d'un sinistre majeur. Cet arbitrage ne pouvant être raisonnablement effectué le jour J, du fait de facteurs évidents (surprise, manque de temps, effet du stress, etc.), c'est la mission du responsable PCA que de préparer les actions qui seront indispensables en temps de « guerre ».

En général, le sinistre majeur provoque un arrêt brutal de l'ensemble des activités de l'organisme. L'activation du PCA peut minimiser les impacts de cette interruption, en permettant une reprise *a minima* et graduelle des activités les plus vitales, c'est-à-dire les activités prioritaires identifiées. Le PCA n'a pas vocation à organiser la reprise de l'intégralité des activités de l'organisme, ce qui serait illusoire, mais il doit avoir identifié les activités les plus vitales et avoir organisé leur reprise opérationnelle, pour réduire les impacts du sinistre sur l'organisme.

En cas d'activation du dispositif, la reprise des activités vitales de l'organisme ne peut vraisemblablement plus se faire sous le mode nominal identique, elle est donc organisée sous un mode que l'on appelle dégradé. En effet, l'organisme doit pouvoir s'affranchir des exigences extrêmes de qualité pour ne retenir que les modes opératoires les plus simples et efficaces pour atteindre ses objectifs primaires. Il ne s'agit pas d'une approche facile, car l'ensemble des organismes retiennent aujourd'hui des critères de qualité assez élevés et s'en défaire n'est pas simple. Pour chaque activité de l'entreprise, il faut déterminer et faire valider le niveau de dégradation de service acceptable, que cela soit pour les activités « Métiers » ou encore celles du système d'information.

4 La loi de Murphy, développée par Edward A. Murphy Jr, un ingénieur aérospatial américain qui en énonça le premier le principe, est un adage qui s'énonce de la manière suivante : « Tout ce qui est susceptible d'aller mal, ira mal. » (Source : Wikipédia)

1.2.4 L'implication des parties prenantes

On entend par partie prenante : « La personne ou organisme qui peut avoir une incidence, être affectée ou se sentir affectée par une décision ou une activité.[5] » Par parties prenantes au PCA, il faut entendre tout d'abord l'ensemble des directions et des acteurs internes à l'organisme qui peuvent avoir un rôle déterminant dans l'organisation de la riposte, en tant que vrai contributeur. Il ne faut pas oublier non plus l'importance capitale des parties prenantes extérieures à l'organisme : prestataires, fournisseurs, sous-traitants, partenaires, clients, mais également pouvoirs publics et même concurrents. Toutes les parties prenantes internes ou externes ont des intérêts communs avec l'organisme et interagissent avec elle. À ce titre, elles doivent être prises en considération pendant tout le cycle de vie du PCA.

1.2.5 Une indispensable humilité

Si la préparation à un fonctionnement en mode dégradé est incontournable, il n'en demeure pas moins que le PCA ne répondra probablement pas à toutes les situations. Le responsable PCA doit faire preuve d'humilité et rappeler ces limites à la gouvernance, afin qu'elle ait bien conscience que les crises ne se déroulent jamais comme on a pu les modéliser.

Comme nous l'évoquerons en dernière partie de cet ouvrage, les profonds bouleversements actuels, dans notre société tout entière, nous invitent à conserver modestie et humilité sur l'efficacité de nos outils de riposte. Il est évidemment essentiel que le dispositif construit soit parfaitement opérationnel et le cycle de vie du PCA doit pouvoir le confirmer de façon régulière. Néanmoins, l'organisme doit avoir conscience que les circonstances du sinistre seront probablement différentes des modélisations, et que le dispositif préparé ne permettra de disposer, peut-être, que d'un premier niveau de riposte.

Il est difficile de prévoir l'ampleur et les caractéristiques d'une crise et le responsable PCA doit imaginer des scénarios d'ampleur et de complexité nouvelles, même si le scénario qui touchera l'organisme sera probablement inédit, voire inconnu jusqu'alors. Certains scénarios sont effectivement loin de notre imagination et il faut accepter de se préparer à l'hypothèse du sinistre inconnu. Qui avait pu imaginer les contours et conséquences des catastrophes telles que les attentats du 11 septembre 2001, la catastrophe de Fukushima ou la crise sanitaire du coronavirus, qui, après avoir menacé l'Asie, déferle sur l'Europe. Cette crise touche désormais tous les continents, avec des effets dévastateurs absolument inédits et d'une rare complexité et intensité. Le caractère sociétal

5 Norme NF EN ISO 22301, article 3.21.