Livre Blanc 2021

# PLAN DE CONTINUITÉ D'ACTIVITÉ OU PLAN D'URGENCE DE POURSUITE D'ACTIVITÉ : DE LA RÉGLEMENTATION AUX OPPORTUNITÉS POUR VOTRE ENTREPRISE

TNP

ACCÉLÉRATEUR DE PERFORMANCE

# Sommaire

# Anticiper les risques et organiser la continuité de l'activité : un enjeu actuel et une préoccupation majeure pour les entreprises

**L'épisode de la pandémie de la Covid-19 illustre parfaitement les situations exceptionnelles auxquelles les organisations peuvent être confrontées. Ces circonstances défavorables peuvent être de diverses natures et la mise en place d'une réponse adaptée avant leur survenance permet d'assurer la continuité des activités essentielles et in fine la survie de l'entreprise.**

**Il convient de parler de sinistre lorsque ces circonstances impactent significativement l'activité de l'entreprise,** qu'il s'agisse d'une problématique de santé publique, d'un acte de malveillance, d'une défaillance technique, d'une catastrophe climatique ou encore d'une simple erreur humaine.

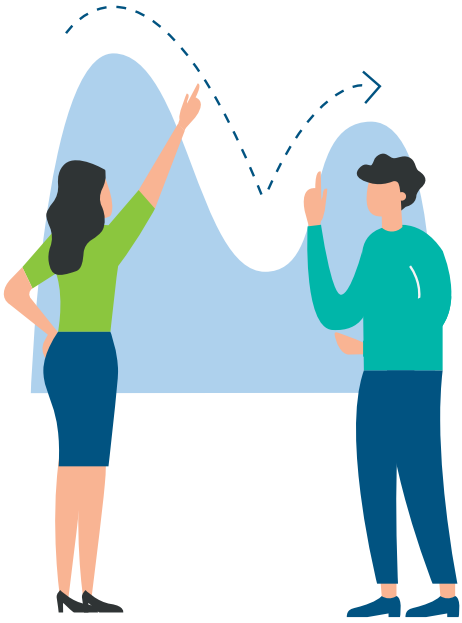
D'après une étude du *Disaster Recovery Institute International*, **43% des entreprises qui n'ont pas mis en place de dispositif de continuité de l'activité font faillite suite à un sinistre.** 29% de celles qui y survivent dans un premier temps finissent par péricliter au cours des deux années qui suivent. **Les chiffres montrent à quel point les organisations sont vulnérables face aux perturbations impactant leurs activités essentielles.**

Les conséquences peuvent être importantes sur la pérennité de votre entreprise, allant de l'**incapacité à délivrer vos produits** ou services attendus par vos clients, à l'**incapacité totale à relancer vos activités.** Ainsi au-delà des pertes financières, de la perte de la confiance des clients et des partenaires et des sanctions juridiques, **c'est bien le risque de faillite qui menace les entreprises non suffisamment préparées.**

Alors que les cyberattaques se multiplient et se complexifient, il convient d'envisager celles-ci avec la même gravité que les menaces « physiques ». Citons à cet égard la pratique émergente du *Cryptojacking* (minage malveillant de cryptomonnaie) qui a augmenté de 8000%[1], ou celle du *phishing* ou hameçonnage qui a connu une recrudescence pendant la crise du coronavirus et qui figurent toujours en tête des menaces cyber[2] **Ces menaces ont des répercussions directes, particulièrement en cas d'incident IT, car 40% des entreprises sont en faillite l'année même.**

Il parait alors évident que les organisations qui ne prévoient pas de **dispositif de continuité de l'activité** hypothèquent leurs chances de survie en cas de fort ralentissement ou d'arrêt total de leurs activités.

À l'inverse, les entreprises qui préparent en amont leur réponse à un sinistre sont plus à même d'y faire face. **96% des entreprises**



***« Les organisations qui ne prévoient pas de dispositif de continuité de l'activité hypothèquent leurs chances de survie en cas d'incident entrainant un fort ralentissement ou un arrêt total de leurs activités opérationnelles »***

***« 27 % des organisations ayant subi une interruption de leurs activités ont déclaré avoir eu une perte de revenus. »***

**dotées d'un plan de continuité ou de reprise d'activité sont capables de survivre à des attaques par *ransomware*** (prise en otage de données ou d'application en contrepartie d'une somme d'argent[3]).

**Le maintien de l'activité passe également par la comparaison entre le coût d'un PCA et les risques qu'il prévient.** La reprise d'activité après sinistre demeure coûteuse, et plus encore pour les entreprises qui n'auraient pas su anticiper ces sinistres. En effet, 27 % des organisations ayant subi une interruption de leurs activités ont déclaré avoir subi une perte de revenus[4].

**Ces enjeux concrets démontrent le besoin de sensibilisation du personnel des entreprises aux bonnes pratiques et soulignent l'urgence pour les organisations de renforcer leur Plan de Continuité d'Activité** afin d'organiser, en amont, la poursuite ou la reprise des activités essentielles. L'impact et les coûts des éventuels évènements défavorables se voient ipso facto réduits et la résilience de l'entreprise optimisée.

**La mise en place d'un PCA a donc pour but de permettre à une entreprise de survivre à une situation exceptionnelle, préserver ses actifs et son activité à un niveau viable.**

*1. https://phoenixnap.com/blog/disaster-recovery-statistics*

*2. https://www.tnpconsultants.com/fr/actualites/coronavirus-le-phishing-conforte-sa-place-de-menace-numero-1-en-cas-de-faille-de-securite*

*3. https://phoenixnap.com/blog/disaster-recovery-statistics*

*4. https://commwestcorp.com/10-data-recovery-statistics/*

# Une normalisation progressive des exigences applicables en matière de gestion des risques et de continuité d'activité

**Si la mise en place d'un Plan de Continuité d'Activité répond avant tout à des besoins métiers** (poursuite de l'activité, réduction de coûts, etc.), il permet également dans certaines industries d'assurer **la conformité de l'entreprise aux exigences légales et réglementaires.** Ayant pris la mesure des risques et de la proportion d'entreprises en difficulté du fait d'un sinistre, les législateurs ont graduellement exigé des différents acteurs l'élaboration d'un PCA. Citons notamment les secteurs banque et assurance, ou encore les OIV et OSE.

**En 2004, Bâle II introduit la notion de risque opérationnel et l'accompagne d'obligations visant à assurer la continuité des activités.** Citons à titre d'exemple la mise en place d'un PCA réglementaire par type de métier. Ces exigences ont été renforcées par Bâle III en 2010. Ces principes ont été repris et déclinés dans la directive européenne CRD II[5] et le règlement européen CRR[6], tous deux entrés en vigueur en 2014.

Le secteur assurantiel n'est pas en reste avec le **Règlement européen Solvency II** qui, suite à sa prise d'effet en 2016, a rendu indispensable la mise en place d'un plan de continuité permettant de limiter les pertes financières dues aux sinistres. **L'objectif de la réglementation est de sécuriser le dispositif de sous-traitance, notamment pour les prestataires importants ou critiques (PIC), et ce dès l'entrée en relation avec le prestataire.**

En 2016, la directive européenne NIS *(Network and Information Security)* relative à la sécurité des réseaux et des systèmes d'information fixe des obligations en matière de gestion des risques pour assurer la continuité, la sécurité et l'intégrité du fonctionnement des OIV (Opérateurs d'Importance Vitale) et OSE (Opérateur de Services Essentiels) ou encore des SIIV (Systèmes d'Information d'Importance Vitale). **Ses objectifs sont d'accroître la coopération stratégique européenne et de renforcer la cybersécurité des OSE.**

Dans le cadre de l'Union bancaire européenne, un « paquet bancaire » a été publié le 7 juin 2019, avec notamment pour objectif d'**accroître la résilience des acteurs du secteur financier et assurantiel.** Composé du règlement CRR II et de la directive CRD V[7] (tous deux transposant les exigences de Bâle III), la directive BRRD II[8] et le règlement SRMR[9] il y est fait références aux exigences de maîtrise des risques opérationnels et de continuité d'activité.

# PCA

**2004**

**Bâle 2 :** dispositif prudentiel
Directive MIF *(Market in Financial Instruments Directive)*

**2012**

**ISO 22301:2012 :** complète le cadre réglementaire relatif aux exigences en termes de continuité des SMCA

**2016**

**Prise d'effet de Solvency II :** assurer la solvabilité et la continuité de l'activité chez les acteurs du secteur assurantiel et leurs partenaires (assurances, filiales et succursales)

**2016**

**Adoption de la directive NIS** par le parlement Européen prévoyant la création d'un cadre réglementaire pour renforcer la cybersécurité des Opérateurs de services qui sont essentiels au fonctionnement de l'économie et de la société (OSE).

**2018**

**Transposition de la Directive NIS** dans les lois nationales des États Membre de l'UE

**2018**

**ISO 22301:2019**
(continuité des SMCA)

**2019**

**Paquet bancaire du 7 juin 2019**
Reprenant un ensemble d'exigences à appliquer pour la gestion des risques et la continuité d'activité

*5. Directive 2013/36/ue du parlement europeen et du conseil du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/ce et 2006/49/CE.*

*6. Règlement (UE) No 575/2013 du parlement européen et du conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement et modifiant le règlement (UE) No 648/2012.*

*7. Directive (UE) 2019/878 du parlement européen et du conseil du 20 mai 2019 modifiant la directive 2013/36/UE en ce qui concerne les entités exemptées, les compagnies financières holding, les compagnies financières holding mixtes, la rémunération, les mesures et pouvoirs de surveillance et les mesures de conservation des fonds propres.*

*8. Directive (UE) 2019/879 du parlement européen et du conseil du 20 mai 2019 modifiant la directive 2014/59/UE en ce qui concerne la capacité d'absorption des pertes et de recapitalisation des établissements de crédit et des entreprises d'investissement et la directive 98/26/CE.*

*9. Règlement (UE) 2019/877 du parlement européen et du conseil du 20 mai 2019 modifiant le règlement (UE) No 806/2014 en ce qui concerne la capacité d'absorption des pertes et de recapitalisation des établissements de crédit et des entreprises d'investissement.*

# Chaque État a complété le cadre international en matière de continuité d'activité par des prescriptions locales

**En France, la notion de Plan d'Urgence et de Poursuite de l'Activité (PUPA)** s'est substituée à la notion de PCA par l'arrêté du 3 novembre 2014, remplaçant le règlement 97-02 **obligeant dès 1997 les établissements de crédit à se doter d'un PCA.** Ce changement est principalement sémantique et les définitions de PUPA et PCA sont similaires. Cette nouvelle appellation permet d'avoir plus de visibilité sur l'objectif final de la démarche lors d'un projet de diagnostic ou de mise en œuvre.

La continuité de l'activité est également devenue **une obligation au Luxembourg pour les Opérateurs d'Infrastructure Critique (OIC) et les OSE.** Dès 1996, la circulaire CSSF 96-126 a prévu la mise en place d'un plan de continuité d'activité pour la fonction informatique du personnel financier. Par la suite, un Règlement Grand-Ducal en date du 21 février 2018 précise la structure des plans de sécurité et de continuité de l'activité des infrastructures critiques. Une loi nationale a transposé la directive NIS et son exigence de continuité de l'activité pour les OSE luxembourgeois et leurs fournisseurs.

**La Protection des Infrastructures Critiques (PIC) a fait l'objet d'une stratégie nationale en Suisse dès 2012.** Elle est complétée par un Plan de mise en œuvre de la Stratégie Nationale de Protection de la Suisse contre les cyber risques (SNPC) 2018-2022 comportant 29 mesures concrètes de gestion des incidents et de résilience. Et notamment l'obligation pour chaque organisation responsable d'une infrastructure critique de disposer d'un PCA faisant l'objet d'un contrôle externe.

**L'obligation d'assurer la continuité des OSE figure également dans la loi Belge du 7 avril 2019** transposant la directive NIS. Chaque OSE a été désigné fin 2019 par son autorité sectorielle respective, piloté par le Centre pour la Cybersécurité en Belgique (CCB) qui incite les entreprises à se doter d'un PCA.

À l'instar de la France, du Luxembourg, de la Suisse et de la Belgique, la Principauté de **Monaco impose également des exigences en termes de continuité d'activité** aux OIV qui utiliseraient des SIIV. De plus, l'arrêt ministériel n°2017-56 du 1er février 2017 sur la politique de sécurité des systèmes d'information de l'État qui exige un PCA dans le secteur public.

Hors Europe, le Maroc a choisi de s'inspirer de la **norme ISO 22301:2019 qui réglemente le management de la continuité d'activité.** Les entreprises sont donc encouragées à recourir au PCA pour prévoir et gérer les risques auxquelles elles pourraient être confrontées.

# Un argument de confiance et de fiabilité pour les parties prenantes

**La capacité de votre entreprise à maintenir ses activités malgré un sinistre est un argument de valeur et un vecteur de confiance. En plus de répondre à une nécessité opérationnelle et à une obligation réglementaire, le PCA permet de rassurer les acteurs clés dont les intérêts sont affectés par les activités de votre entreprise.**

L'élaboration et la mise en œuvre d'un PCA permettent de démontrer la capacité de votre entreprise à anticiper, gérer les crises, maitriser les pertes et in fine maintenir son activité vis-à-vis de ses clients et partenaires.

Pour les équipes internes, la mise en place d'un PCA est une opportunité de documenter et de challenger les processus déjà en place afin de les préciser et de les améliorer.

La transparence affichée contribue à renforcer l'image de marque et **la confiance des clients** qui considèrent votre résilience comme un critère de sélection et donc un avantage compétitif pour votre entreprise.

Vis-à-vis des assureurs, le PCA démontre la capacité à lisser et placer sous contrôle les risques et devient un atout majeur à faire valoir dans les négociations de primes en fonction de la sinistralité.

***«Le PCA est également l'occasion de construire un modèle de collaboration responsable intégrant tous les partenaires stratégiques et fournisseurs essentiels.»***

TNP

ACCÉLÉRATEUR DE PERFORMANCE

# TNP, PARTENAIRE DE VOTRE TRANSFORMATION

**Afin de pérenniser son développement, une entreprise doit investir dans sa capacité de transformation en relevant les nouveaux défis d'un contexte en perpétuelle évolution et un avenir économique incertain avec la crise sanitaire actuelle.**

**TNP a développé un nouveau paradigme holistique** pour répondre aux enjeux de transformation et d'accélération de la performance.

1. **Processus et opérationnel**
2. **Solutions et technologie**
3. **Organisationnel et humain**

Notre démarche se décline en **cinq étapes modulables** et conçues pour que chacune apporte à son échéance un maximum de valeur pour le client :

1. **Compréhension**
   du contexte, des ambitions et des enjeux
2. **Évaluations**
   → **TOP-DOWN,** analyse quantitative macro et collecte des feedbacks
   → **BOTTOM-UP,** sur les activités à fort potentiel d'optimisation
3. **Plan d'actions**
   avec qualification et priorisation des initiatives de transformation et optimisation
4. **Mise en œuvre**
   réalisée conjointement avec toutes les parties prenantes
5. **Pérennisation**
   du changement ancré dans la culture d'entreprise

**SATISFACTION CLIENTS | TIME TO MARKET | QUALITÉ DE SERVICE**
**BIEN ÊTRE COLLABORATEURS | PERFORMANCE OPÉRATIONNELLE**
**AGILITÉ | RÉSILIENCE | MAÎTRISE DES COÛTS | MAÎTRISE DES RISQUES**
**ENGAGEMENT DES ÉQUIPES**

www.tnpconsultants.com

# Un ensemble de dispositifs pour pallier la diversité des impacts

**Le PCA doit permettre à votre entreprise de renforcer sa résilience face à différents facteurs de risque (naturels, environnementaux, humains et techniques). Le PCA est donc constitué d'un ensemble de mesures et de dispositifs complémentaires destinés à couvrir cette diversité de risques.**

**Opérationnellement, un PCA consiste en l'activation coordonnée de dispositifs permettant :**

- → De restaurer rapidement l'activité à des niveaux acceptables (en passant parfois par un mode dégradé) ;
- → De restreindre les durées d'indisponibilité totale, limitant ainsi les impacts sur les opérations et les pertes potentielles.

**On distingue ainsi six composants majeurs du PCA :**


1 **Le Plan de Continuité Métiers,** qui définit les mesures et actions à conduire par les métiers pour la poursuite des activités vitales ainsi que le mode de fonctionnement dégradé des activités.

2 **Le Plan de Repli Logistique,** qui précise les solutions de repli des services sinistrés dans des locaux de secours, internes ou externes ou par du télétravail ou travail distant.

3 **Le Plan de Continuité Informatique** (ou Plan de Sécurité Informatique), qui recense les solutions de secours de l'informatique, des réseaux et de la téléphonie.

4 **Le pilotage opérationnel du PCA,** qui est prévu par le Plan de Gestion de Crise et qui s'applique en situation de crise, afin d'orchestrer une réponse plus rapide et plus efficace via la détection et la qualification des incidents.

5 **Le Plan de Reprise d'Activité,** qui détaille pour chaque activité les modalités de reprise de l'activité « nominale » suite à un sinistre ou une période de fonctionnement en mode dégradé.

6 **Le Plan de Continuité Opérationnel du PCA,** qui régit l'adéquation et le maintien des mesures avec les risques encourus et les impacts associés.

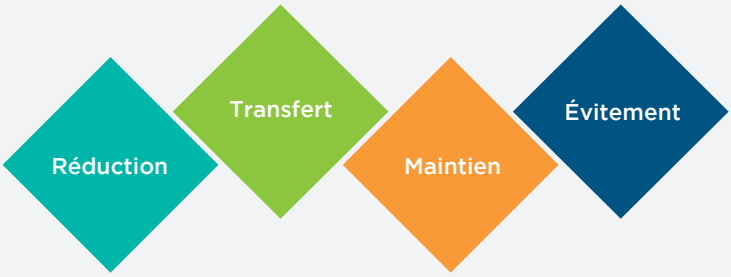
# Le PCA doit aboutir à la création de mesures concrètes pour faire face à la réalité des risques

**Dans cette optique, la démarche que nous proposons nécessite l'inventaire des activités, des processus et des ressources critiques (humaines, matériels, financières, etc.). Puis, sur base de cet inventaire, nous proposons l'identification des menaces et des vulnérabilités potentielles. L'objectif étant de distinguer ce qui est critique de ce qui parait l'être et de concentrer les efforts sur les risques les plus impactants pour votre entreprise.**


La première étape est d'établir **la carte d'identité de l'entreprise,** c'est-à-dire définir le **contexte de votre entreprise** (secteur d'activité, stratégie, objectifs, valeurs, environnements internes et externes), identifier les dépendances de l'organisation, les enjeux, les besoins et attentes, ainsi que les contraintes (légales, réglementaires et contractuelles) afin que le **PCA soit cohérent** avec la **stratégie de l'entreprise,** correctement **priorisé** en **mobilisant les parties concernées.**
Puis, sur base d'une **cartographie globale** reprenant **l'inventaire** des **produits, services et processus clés** de l'organisation, nous proposons d'effectuer un ***«Business Impact Assessment»,*** c'est-à-dire d'évaluer les **impacts** (financiers, institutionnels, juridiques, clients, internes, image) qui résulteraient d'un arrêt ou d'un ralentissement des activités. C'est grâce à ces travaux que nous serons en mesure de distinguer les activités critiques parmi toutes celles de votre entreprise.

L'étape suivante consiste à identifier **les menaces et les vulnérabilités** pesant sur les activités et les actifs critiques de votre organisation. Cette analyse consiste à estimer la probabilité ou la **vraisemblance** qu'une menace exploite une vulnérabilité ainsi que les **impacts** ou les dommages engendrés par la survenance de cette menace. Notre analyse détermine **la sévérité du risque** et retient en **priorité les risques ayant un impact majeur sur le niveau de disponibilité** ou **d'activité.**

## Pour gérer un risque, il existe quatre types de traitements possibles




- La **réduction** du risque, en appliquant des mesures pour le rendre acceptable ;
- Le **transfert** du risque, en le partageant avec des parties externes (assurance, externalisation de l'activité…) ;
- Le **maintien** ou la rétention du risque lorsque le coût de réduction du risque dépasse le montant de pertes potentielles suite à une interruption de l'activité et que l'organisation peut supporter les conséquences de la survenance du risque ;
- L'**évitement** du risque, qui intervient lorsque les coûts de réduction du risque ou les conséquences suite à sa survenance dépassent ce que l'organisation peut assumer. Elle renonce alors à l'activité concernée ou en modifie les conditions d'exploitation.

Nous vous aidons ensuite à définir des **objectifs de continuité.** La continuité peut être évaluée à l'aune de trois paramètres : un niveau minimum de disponibilité, un niveau minimum d'indisponibilité et un niveau de fonctionnement dégradé. Ces niveaux sont caractérisés par des métriques comme la Durée Maximale d'Interruption Admissible (DMIA) ou encore la Perte de Données Maximale Admissible (PDMA).
Nous privilégions la mise en place d'une **stratégie PCA déclinée pour chaque actif ou activité,** au travers de la définition de **niveau de service minimum souhaitée,** de **durée d'interruption maximale tolérée** et de **durée de rétablissement souhaité.**

Pour finir, nous construisons ensemble le plan de rétablissement précisant les ressources nécessaires et la dépendance entre les différentes mesures de rétablissement de l'activité.

Le succès de la démarche est conditionné par une **volonté forte des directions générales** des organisations puisqu'elle concerne potentiellement **l'ensemble des activités de l'entreprise** et nécessite la mobilisation d'une équipe dédiée à sa mise en place et son maintien dans la durée.

Vous l'aurez compris : à la fin de cette phase, le PCA est constitué mais sa validité n'est pas garantie dans le temps tant que sa gouvernance n'est pas définie pour porter son amélioration continue.

# La constitution du PCA s'inscrit dans la durée

**La définition, le maintien et l'évolution du PCA s'inscrivent dans un processus continu plus global de gestion des risques défini par la norme ISO 22301 sous le nom de Système de Management de la Continuité d'Activité, appelé SMCA (ou BCMS en anglais).**

Comme évoqué précédemment, le PCA est structuré autour de **six dispositifs** complémentaires auxquels sont associés un **périmètre** et une **gouvernance particulière** dont il faut préciser **les acteurs** (rôles et responsabilités), **les exigences** (moyens humains matériels et organisationnels) **et les conditions de mise en œuvre** (procédures) et ces critères évoluent dans le temps impliquant l'actualisation régulière de votre PCA.


Afin d'assurer l'**adaptation constante** du PCA aux évolutions de votre entreprise (croissance, nouvelles activités stratégiques, changements de fournisseurs, digitalisation, etc.), la mise en place d'une démarche PDCA *(Plan, Do, Check, Act)* pilotée par une équipe dédiée est recommandée.

La phase de conception du PCA est donc suivie d'une **phase d'évaluation** des différentes mesures, qui permet de s'assurer de leur efficacité par des **tests et expérimentations des dispositifs.** Ces tests vont notamment permettre de valider l'efficience du PCA, confirmer la réponse aux exigences de continuité et identifier les axes d'amélioration.

Les révisions du PCA peuvent naturellement concerner les dispositifs et procédures à appliquer, mais également les aspects organisationnels comme le RACI, les critères de déclenchement du PCA, le *Business impact analysis* ou encore les KPI à surveiller.

Un tel projet implique donc un investissement significatif pour votre entreprise. Il nécessite la mobilisation de moyens humains et matériels dans la durée (de la conception à l'amélioration continue) qu'il convient de mettre en balance avec **l'estimation des dommages éventuels.**

Afin d'optimiser la charge qu'implique un PCA, nous recommandons d'adopter une politique de ***« Continuity by Design and by Default »*,** en développant une culture de la résilience et de la continuité tout en appliquant les mesures au plus près des actifs et dans les processus dès leur mise en place.

# Notre approche *« Continuity by Design and by Default »*

**Lorsqu'on évoque PCA, on entend souvent protocoles de reprise, site de secours, redondance des dispositifs, solutions de replis... autant de termes qui signifient que des moyens additionnels et coûteux sont à mettre en œuvre en plus de ce qui est prévu pour garantir un fonctionnement nominal aux opérations de l'entreprise. L'approche de TNP ne consiste pas seulement à adjoindre des dispositifs à l'existant mais surtout à intégrer les mesures de continuité au sein du fonctionnement quotidien de votre entreprise.**

Au travers de notre démarche, nous cherchons à **diminuer l'impact et la charge** du PCA tout en optimisant les capacités de restauration à des niveaux acceptables de fonctionnement.

Le principe n'est plus de maintenir à grands frais des moyens de secours dédiés exclusivement au PCA mais d'inclure certains dispositifs dès l'origine pour assurer une meilleure réactivité en cas de sinistre et un gain en termes de fiabilité grâce à **un mode de fonctionnement nominal « auto-résilient ».**

Par ailleurs, pour s'assurer d'appliquer les bonnes pratiques, il peut être tentant d'imposer unilatéralement un cadre de PCA tel que le proposent ISO 22301 ou le NIST, en appliquant strictement à l'ensemble du périmètre les exigences telles que décrites par ces normes. **Cependant, appliquer systématiquement un cadre peut se transformer en *« machine à reporting »* et devenir une contrainte plutôt qu'un atout.** C'est pourquoi nous préconisons une approche plus **pragmatique et différenciée** en fonction des enjeux et des risques et qui va tenir compte des ressources disponibles, des savoir-faire et des moyens de l'entreprise.

C'est également pour cette raison que nous avons élaboré notre approche ***« Continuity by design and by default »***. Celle-ci permet de renforcer l'implémentation du PCA, d'optimiser les coûts (moins d'exercices de tests, moins de ressources dédiées) et de bénéficier d'une plus grande réactivité en cas de crise (meilleure proactivité de la part des collaborateurs et des opérations).

**Notre méthodologie s'appuie sur quatre piliers :**

1. La **co-construction** du PCA, en premier lieu, permet d'impliquer les différentes compétences au sein des lignes métiers et opérationnelles. Les retours de la part des opérationnels permettent une conception et une mise en œuvre répondant aux exigences métier et réglementaire.

2. Pour être exploitables, les mesures qui constituent le PCA doivent être intelligibles par tous. Cet objectif est atteint grâce à un effort de la **normalisation** des taxonomies, cadres et principes. En effet, un cadre intégré par les collaborateurs et par conséquent dans la culture de l'entreprise est plus naturellement appliqué (opérations quotidiennes, projets,...).

**3** Autant que possible, les mesures qui composent le PCA sont à élaborer à partir de l'existant, soit en le perfectionnant, soit en les actualisant, ce qui simplifie leur adoption et encourage leur application, les rendant ainsi plus **pragmatiques.**

**4** Pour finir, l'approche *« Continuity by design and by default »* cherche à tirer parti des expériences des collaborateurs et de leur connaissance opérationnelle de l'entreprise. En **capitalisant** sur ces savoirs, il sera plus simple d'évaluer les risques et les faiblesses et de dresser des scenarii de crise plus réalistes.

**Pour s'assurer que le PCA soit toujours en phase avec le contexte et les objectifs de votre entreprise, il doit s'inscrire dans une démarche d'amélioration continue. Il participera ainsi au déploiement d'une culture d'excellence opérationnelle et de gestion des risques au sein de votre organisation devenant de facto un facteur d'accélération de la performance et de résilience.**

# TNP : Transformation ‘N’ Performance

TNP est un **cabinet de conseil français, européen, hybride et indépendant, leader de la performance.** Il accompagne les dirigeants dans leurs **transformations digitales, opérationnelles et réglementaires.** Il ambitionne de devenir **n°1 du conseil indépendant en Europe et Afrique subsaharienne d’ici 2030.**

## Hybride

Bilingue **métier-technologies**

## Indépendant

Pour exercer librement notre métier
et proposer **des solutions adaptées**

## Engagé

**sur les résultats** en mode co-construction pour
une croissance et une **performance économique durables**

## Notre ADN

1 **Forte séniorité** des équipes

2 **Multisectoriel**

3 Orienté **résultats**

4 **Multispécialiste**

5 **Associés présents** sur les missions

## En chiffres 2019

**510**
**collaborateurs**
(dont 450 en France)

**70 m€**
**de chiffre d'affaires**
(dont 64 M€ en France)

**10 bureaux**
Paris, Lyon, Marseille, Monaco, Milan, Luxembourg, Genève, Casablanca, Cochin, Mumbai

**Des missions en cours dans + de 25 pays**

## Notre organisation

Noter organisation **couvre l'ensemble des secteurs** de l'économie et qui répond à vos enjeux.

Nous intervenons sur **l'ensemble des secteurs d'activités** et mettons à votre disposition nos experts qui **combinent expertises sectorielles et métiers.**

TNP possède **cinq grands domaines d'expertises** qui **répondent à vos enjeux actuels et à venir.**

### → MULTISECTORIEL

| BANQUE | ASSURANCE & PROTECTION SOCIALE | MOBILITÉ | INDUSTRIE & SERVICES | SECTEUR PUBLIC & SANTÉ |
|---|---|---|---|---|
| → Banque de détail | → Assurance de biens | → Ferroviaire | → Automobile | → Gouvernements |
| → Banque de financement et d'investissement | → Assurance de personnes | → Aérien | → Energie & Utilités | → Collectivités territoriales |
| → Banque privée, gestion d'actifs et titres | | → Maritime | → Retail & Luxe | → Hôpitaux |
| | | → Routier | → Pharmaceutique | → Défense |

### → MULTISPÉCIALISTE

- TRANSFORMATION NUMÉRIQUE & TECHNOLOGIQUE
- TRANSFORMATION DIGITALE & SOLUTIONS MÉTIERS
- EXCELLENCE OPÉRATIONNELLE & CROISSANCE DES REVENUS
- DATA MANAGEMENT, DATA PROTECTION, CYBERSÉCURITÉ
- TRANSFORMATION RÉGLEMENTAIRE, FINANCE & RISQUE

# Vos interlocuteurs TNP

**Gilles BAILLOU**
***Partner***
***Expert CIO Advisory***
*gilles.baillou*
*@tnpconsultants.com*

**Florence BONNET**
***Partner***
***Experte en protection des données personnelles et cybersécurité***
*florence.bonnet*
*@tnpconsultants.com*

**Xavier FORTUNA**
***Manager***
***Expert Architecture d'entreprise et sécurité***
*xavier.fortuna*
*@tnpconsultants.com*

**Nathalie MEGE**
***Managing Partner TNP Luxembourg***
***Experte Excellence opérationnelle et transformation des entreprises***
*Nathalie.mege*
*@tnpconsultants.com*

**Henry-Julien VAYSETTE**
***Manager***
***Expert Finance & risque***
*henry-julien.vayssette*
*@tnpconsultants.com*

# Glossaire

**Cellule de crise :** dispositif mis en place à la survenance d'un sinistre et dont l'objectif est le retour au niveau d'activité nominale de la façon la plus efficiente possible.

**DMIA / RTO (Durée Maximale d'Interruption Admissible / *Recovery Time Objective*) :** durée maximale entre la survenance du sinistre et un retour au niveau d'activité minimal défini.

**Impact :** niveau d'incidence d'un évènement, ses conséquences.

**LPM :** Loi de Programmation Militaire.

**MTD (*Maximal Tolerable Downtime*) :** durée maximale d'arrêt du ou des services après la survenance du sinistre.

**NIS (directive) :** *Network and Information Security*.

**Niveau d'activité dégradé :** l'entreprise n'est pas en mesure de fournir l'ensemble de ses services habituels. Il est critique de repasser au plus vite à un niveau d'activité nominal (le magasin est ouvert avec seulement une partie des effectifs).

**Niveau d'activité minimal :** niveau minimal acceptable en dessous duquel le service sera considéré comme non rendu (le magasin est ouvert uniquement pour le passage et le retrait de commandes).

**Niveau d'activité nominal :** niveau d'activité normal, hors période de crise.

**OIV :** Organisation d'Importance Vitale.

**OSE :** Opérateur de Services Essentiels.

**PCA :** Plan de Continuité d'Activité.

**PCI :** Plan de Continuité informatique.

**PCO :** Plan de Continuité Opérationnelle.

**PDMA / RPO (Perte de Données Maximale Admissible / *Recovery Point Objective*) :** durée maximale de perte de données acceptable au moment de la survenance du sinistre.

**PGC :** Plan de Gestion de Crise.

**PRA :** Plan de Reprise d'Activité.

**Probabilité :** probabilité de survenance d'un évènement.

**PRL :** Plan de Repli et Logistique.

**PCM :** Plan de Continuité Métier.

**Risque :** association de l'impact et de la probabilité de survenance d'un évènement.

**SIIV :** Système d'Information d'Importance Vitale.

**WRT (*Work Recovery Time*) :** durée Maximale entre le passage au niveau d'activité minimale et le retour au niveau d'activité nominale.

**SMCA / BCMS :** Système de Management de la Continuité d'Activité / *Business Continuity Management System.*

**TCI :** *Total Cost of Interruption.*

**TCB :** *Total Cost of BCP.*

# Contact


**TNP France (siège social)**
31 rue du Pont, 92 200 Neuilly-Sur-Seine
**01 47 22 43 34**

**TNP Luxembourg**
26B Boulevard Royal, L-2449 Luxembourg
**(+352) 2 899 99 44**

commarket@tnpconsultants.com
**www.tnpconsultants.com**


TNP

ACCÉLÉRATEUR DE PERFORMANCE


**Février 2021** - Conception graphique : StudioChadho - Estelle Dho / Crédits visuels : shutterstock