

# PLAN DE CONTINUITÉ D'ACTIVITÉ ET PLAN DE REPRISE INFORMATIQUE

## En bref

Le **Plan de Continuité d'Activité (PCA)** regroupe l'ensemble des mesures anticipées permettant à une organisation de maintenir ou restaurer ses activités critiques à un niveau acceptable en cas de crise majeure (cyberattaque, sinistre, défaillance IT...). Il inclut une composante spécifique aux systèmes d'information : le **Plan de Reprise Informatique (PRI)**, qui définit les modalités techniques de redémarrage du SI.

Pour le commissaire aux comptes, l'enjeu est double : évaluer l'impact potentiel sur la continuité d'exploitation et la fiabilité des états financiers.

Les principaux risques clés à surveiller portent sur :

- L'absence d'identification des processus critiques et d'objectifs de reprise (RTO/RPO),
- L'obsolescence du PCA/PRI face aux évolutions de l'environnement et du SI,
- Le défaut de tests réguliers rendant le PCA potentiellement inefficace en situation réelle,
- La méconnaissance du plan par les acteurs censés le mettre en œuvre,
- La non-intégration des prestataires essentiels dans la stratégie de continuité.

Le commissaire aux comptes devra ainsi s'assurer de :

- Évaluer l'existence et la pertinence des PCA et PRI,
- Vérifier l'implication de la gouvernance dans le pilotage du PCA
- Évaluer l'adéquation entre les objectifs métier et les capacités de reprise informatique
- S'assurer de la réalisation et de la documentation des tests réguliers
- Apprécier l'impact potentiel des lacunes du PCA sur la continuité d'exploitation

## Séquence 1

# Comprendre la thématique

## Contexte et enjeux

Le plan de continuité d'activité (PCA) vise à établir un ensemble de mesures pour assurer la continuité des activités essentielles de l'entreprise en cas de sinistre ou d'événement perturbateur majeur. Il intègre notamment :

- Une analyse d'impact métier (BIA) identifiant les processus critiques,
- Des objectifs de reprise (RTO : temps maximal d'interruption, RPO : perte de données admissible),
- Un volet informatique appelé Plan de Reprise Informatique (PRI) qui constitue sa déclinaison technique pour le redémarrage du système d'information et la restauration des données essentielles.

L'enjeu principal est de permettre à l'entité de maintenir ou de reprendre rapidement ses activités critiques à la suite d'un incident informatique. Il contribue à la résilience organisationnelle en assurant que l'entité puisse continuer à remplir ses obligations légales, contractuelles et opérationnelles, même dans des conditions dégradées.

La dépendance croissante des organisations envers leurs systèmes d'information et l'augmentation des menaces (cyberattaques, catastrophes naturelles, pandémies) rendent le PRI plus crucial que jamais.

Un PCA/PRI pertinent doit permettre à l'organisation de répondre aux questions suivantes :

- Quelles sont les activités essentielles à maintenir ?
- Quels sont les délais de reprise acceptables (RTO) et les pertes de données tolérables (RPO) ?
- Quelles ressources (humaines, techniques, informationnelles) sont nécessaires à la reprise ?
- Comment s'organiser la gestion de crise et qui en a la responsabilité ?

# PLAN DE CONTINUITÉ D'ACTIVITÉ ET PLAN DE REPRISE INFORMATIQUE

- Quelles sont les procédures dégradées permettant de fonctionner pendant la crise ?
- Les prestataires critiques sont-ils intégrés dans le dispositif ?

Les caractéristiques d'un PCA robuste incluent sa formalisation, son appropriation par les acteurs concernés, sa mise à jour régulière, son test périodique et son alignement avec la stratégie de résilience de l'entreprise.

## Conséquences pour le commissaire aux comptes

Pour le commissaire aux comptes (CAC), l'absence ou la faiblesse d'un Plan de Continuité d'Activité (PCA) ou d'un Plan de Reprise Informatique (PRI) constitue un facteur de risque, à intégrer dès la phase d'évaluation du contrôle interne et de la cartographie des risques.

### Continuité d'exploitation

D'un point de vue normatif, ce risque renvoie à la NEP 570 relative à la continuité d'exploitation. Lorsqu'un incident grave (cyberattaque, sinistre, défaillance technique majeure) est susceptible de compromettre la survie de l'entité, l'absence de PCA/PRI peut faire naître une incertitude significative sur la continuité d'exploitation.

Dans un tel cas, le CAC doit en évaluer l'impact comptable (dépréciations d'actifs, pertes d'exploitation, provisions éventuelles) et se poser la question d'un signalement dans son rapport, voire d'une observation ou d'une réserve si l'incertitude n'est pas suffisamment documentée ou traitée par la direction.

### Fiabilité des systèmes d'information et des données comptables

Une défaillance du SI sans solution de secours claire peut également remettre en cause la fiabilité des comptes, notamment si les sauvegardes sont absentes, incomplètes ou mal testées.

Le CAC doit intégrer ces éléments dans son analyse des risques (NEP 315), en particulier lorsque des processus critiques (paie, facturation, stock, clôture) sont concernés. Par exemple, l'indisponibilité prolongée d'un outil de paie ou de facturation peut générer des erreurs ou des omissions dans les enregistrements comptables.

### Adaptation de la stratégie d'audit

Lorsque l'organisation ne peut fonctionner qu'avec ses outils numériques (ce qui est souvent le cas aujourd'hui), l'absence de solution de repli pour des applications critiques impose au CAC de revoir sa stratégie d'audit. Cela peut se traduire par :

- un renforcement des tests de sauvegarde/restauration,
- des entretiens plus poussés avec les responsables IT,
- ou encore la mise en œuvre de procédures spécifiques pour s'assurer que les données exploitées sont complètes et fiables en cas de reprise informatique.

### Contrôle interne et procédures dégradées

En l'absence de plan formalisé ou de solution de repli informatique, l'entité recourt souvent à des procédures manuelles ou improvisées. Ces modes dégradés sont rarement encadrés et peuvent être sources d'anomalies ou de fraudes.

Le commissaire aux comptes doit alors évaluer dans quelle mesure ces modes dégradés et/ou la reprise des données peuvent altérer la production d'une information financière fiable, et s'ils doivent faire l'objet de recommandations ou d'une communication aux organes de gouvernance.

### Conformité réglementaire

Dans certains secteurs, la mise en place d'un PCA/PRA n'est pas seulement une bonne pratique, mais une exigence réglementaire. Le commissaire aux comptes, sans se substituer à l'organe de contrôle sectoriel, doit rester attentif à la conformité de l'entreprise avec ses obligations réglementaires en matière de continuité d'activité.

Le défaut de conformité peut non seulement constituer un risque juridique ou opérationnel pour l'entité, mais également un signal d'alerte pour le CAC quant au degré de maîtrise globale du dispositif de contrôle interne.

Dans les cas les plus sensibles, cela peut justifier une communication spécifique aux organes de gouvernance, voire à l'ACPR ou l'AMF selon les cas.

## Séquence 2

# Mission du CAC : objectifs, bonnes pratiques et outils

### Thématique 1

## Identification des activités critiques (BIA, RTO/RPO), des sauvegardes, des ressources employés

### Objectifs

Dans le cadre de l'évaluation du dispositif de continuité d'activité, le CAC doit s'assurer que l'entité a identifié ses activités critiques, ses ressources essentielles (humaines, techniques, logicielles) et qu'elle a défini des objectifs de reprise réalistes et cohérents en cas de sinistre.

Les principaux éléments à rechercher sont :

- L'existence d'une Business Impact Analysis (BIA) ou d'une analyse équivalente permettant d'identifier les processus vitaux et leur criticité.
- La définition claire, par le métier et partagée avec la DSI, des RTO (Recovery Time Objective) et RPO (Recovery Point Objective) pour les applications clés.
- L'évaluation des ressources nécessaires à la reprise (personnes, outils, sites de repli...).
- Le lien entre ces éléments et les choix technico-opérationnels (sauvegardes, redondance, plans de secours).
- Le RTO correspond au délai maximal admissible d'interruption d'un service, au-delà duquel les conséquences sur l'activité de l'entité deviennent significatives. Il détermine le temps de redémarrage requis pour chaque application critique.

Le RPO, quant à lui, représente la durée maximale de perte de données tolérée. Il traduit le niveau de sauvegarde nécessaire : un RPO de 4 heures implique que les

sauvegardes doivent être programmées pour garantir qu'en cas de restauration, seules les 4 dernières heures de données puissent être perdues, et non davantage.

L'objectif du CAC n'est pas de valider techniquement la stratégie de continuité, mais de vérifier qu'elle est alignée avec les enjeux financiers de l'entité, et qu'un sinistre sur les ressources critiques n'entraînerait pas de perte significative non anticipée dans les comptes.

### Bonnes pratiques

#### Assurer l'alignement stratégique avec la direction générale

Avant tout, le CAC doit vérifier que les enjeux de continuité d'activité sont connus, compris et portés au niveau de la gouvernance de la société. Un PCA/PRI ne peut être efficace s'il reste cantonné à la DSI.

**Astuce :** lors des entretiens, poser des questions simples mais révélatrices à la direction comme :

« En cas d'indisponibilité totale du SI, quelles sont les fonctions que vous considérez comme vitales ? »

« Avez-vous validé formellement les délais de reprise (RTO) proposés par vos équipes ? »

« Existe-t-il une instance ou un plan de crise identifiée pour prendre les décisions si un sinistre survient ? Quelle sont ces membres ? »

#### Encourager la formalisation d'une BIA (Business Impact Analysis)

Même sous forme simple, une BIA permet de structurer la réflexion de l'entreprise sur :

- les activités critiques,
- les impacts financiers d'une interruption,
- et les objectifs de reprise (RTO/RPO) associés.

**Astuce :** s'appuyer sur des guides existants (CRCC, ISO 22301) ou proposer un canevas simplifié pour initier la démarche dans les PME.

#### Maintenir un dialogue structuré avec la DSI

La DSI est souvent dépositaire de la mise en œuvre technique du PRI, mais elle ne porte pas, à elle seule, la responsabilité du PCA dans son ensemble, qui relève d'une démarche transversale pilotée par la direction générale. Le CAC doit s'assurer que la DSI :

- Connaît les ressources critiques à protéger,
- Dispose d'une vision claire des priorités de reprise,
- Et peut démontrer que les sauvegardes et les tests sont en phase avec les objectifs métiers.

**Astuce :** utiliser une trame d'entretien commune DSI/ Directions métiers, pour évaluer le niveau de coordination et éviter les silos.

**Vérifier la robustesse des stratégies de sauvegarde et de reprise**

Le CAC doit s'assurer que les sauvegardes :

- sont fréquentes et externalisées,
- sont testées régulièrement pour garantir leur efficacité,
- couvrent bien l'ensemble des données critiques (comp-ta, paie, facturation, GED, etc.).

**Astuce** : demander à voir un journal de sauvegarde ou un rapport de test de restauration récent, et croiser les résultats avec les RTO/RPO affichés.

(Cf. Fiche 06 « Exploitation Informatique »)

**Analyser la couverture des ressources humaines critiques**

Le CAC peut également alerter sur la dépendance à des personnes clés dans la gestion de crise (ex. : une seule personne connaît les procédures de redémarrage).

**Astuce** : interroger la DSI ou la direction sur les mesures prises en cas d'indisponibilité des référents : « Les procédures sont-elles formalisées ? Qui prend le relais ? Avez-vous formalisé les rôles de crise ? »

**Outils & documentations mises à disposition**

Le CAC peut s'appuyer sur :

- Les documents internes : BIA, schéma directeur IT, tableau des RTO/RPO par application, fiches de processus critiques, fiches de poste de crise.
- Des grilles d'entretien types avec la DSI ou les métiers pour identifier les ressources essentielles et les dépendances SI.
- Les rapports de test de PCA et/ou PRI (si existants), logs de sauvegarde/restauration, tableaux de criticité par système.
- Les référentiels externes : ISO 22301 (management de la continuité), guides CRCC/CNIL sur le PCA, trames proposées dans le cadre de cette fiche.

**Impact dans la stratégie du commissaire aux comptes**

Une absence d'identification claire des activités critiques ou d'objectifs de reprise peut révéler une méconnaissance du risque de continuité par l'entité. Cela accroît le risque d'interruption non maîtrisée ayant un impact sur les comptes.

Le CAC adaptera alors sa stratégie d'audit en :

- Réalisant des tests spécifiques sur la qualité des sauvegardes,
- Demandant des justificatifs sur les délais de restauration déclarés,
- Ajustant ses procédures sur les cycles sensibles (paie, ventes, stocks) en fonction des scénarios à risque,
- Et, si nécessaire, intégrant ce point dans sa communication à la gouvernance, voire dans son rapport.

**Thématique 2****Formalisation/exactitude/complétude du PCA/PRI et sa mise en œuvre****Objectifs**

Le commissaire aux comptes doit apprécier dans quelle mesure le PCA/PRI de l'entité est formalisé, complet, mis à jour et réellement opérationnel.

Il s'agit d'évaluer la gouvernance du dispositif, la cohérence des documents, et le niveau de mise en œuvre réelle (tests, maintenance, communication...).

Les objectifs sont :

- Vérifier que le PCA/PRI est documenté et validé par la direction,
- S'assurer qu'il couvre l'ensemble des processus et ressources critiques,
- Évaluer s'il est testé régulièrement, mis à jour, et intégré aux pratiques courantes de l'entreprise,
- Identifier les écarts entre théorie et réalité, notamment dans la préparation des équipes.

## Bonnes pratiques

### S'assurer de la formalisation d'un PCA/PRI structuré et validé

Un PCA non formalisé ou limité à un fichier technique ne permet pas une réponse efficace en cas de crise.

**Astuce** : demander le dernier plan validé, vérifier la date de mise à jour et la signature de la direction.

### Contrôler l'exhaustivité du périmètre couvert

Le PCA doit couvrir les processus critiques métiers, les applications associées, les sites, les personnels clés et les prestataires essentiels.

**Astuce** : croiser la liste des processus avec la cartographie des risques et les exigences clients/tiers.

### Vérifier que des tests sont réalisés et donnent lieu à des actions correctives

Un plan non testé est un plan théorique. L'efficacité opérationnelle repose sur l'expérience des équipes et les retours d'expériences.

**Astuce** : exiger la dernière synthèse de test et vérifier si les recommandations ont été suivies.

### S'assurer que le plan est maintenu à jour

Un PCA figé est vite obsolète (nouveaux logiciels, départs de personnel, prestataires modifiés...).

**Astuce** : interroger la direction sur la fréquence de revue et les déclencheurs de mise à jour.

### Évaluer le niveau de préparation des acteurs en cas de crise

Même avec un bon plan, l'absence de formation ou de communication limite l'efficacité.

**Astuce** : demander si les différents acteurs ont été formés ou briefés récemment.

## Outils & documentations mises à disposition

Le CAC peut s'appuyer sur :

- Le document PCA/PRI officiel (version validée, avec date et diffusion),
- Les rapports de tests, comptes rendus et plans d'action associés,
- La liste des processus, ressources, applications et prestataires critiques,
- Les procédures de restauration, de communication de crise, d'escalade,

- Les preuves de formation ou sensibilisation du personnel impliqué,
- Les référentiels externes : ISO 22301, guide ANSSI, proposées dans le cadre de cette fiche.

## Impact dans la stratégie du commissaire aux comptes

Un PCA non formalisé ou non testé crée une incertitude majeure sur la capacité de l'entreprise à assurer la continuité de ses processus comptables et financiers. Cela peut affecter directement :

- L'hypothèse de continuité d'exploitation (NEP 570),
- La fiabilité des données financières (perte d'historique, rupture d'exploitation, erreurs de clôture),
- Et la capacité à répondre à des obligations contractuelles ou réglementaires.

Le CAC adaptera sa stratégie d'audit en :

- Renforçant les tests sur les cycles critiques (notamment si dépendance à l'outil) en cas de crise,
- Et documentant ses constats pour communication à la gouvernance ou justification de son opinion.

## Séquence 3

# Cas d'usage

## Contexte de l'entité

La société MÉTALPLUS est une PME industrielle spécialisée dans la fabrication de pièces métalliques pour l'aéronautique. Elle emploie 80 collaborateurs et génère un chiffre d'affaires de 15 M€. Son activité repose sur une GPAO et un ERP intégré, déployé récemment pour la gestion des commandes, des stocks et de la production.

Le commissaire aux comptes intervient dans le cadre de la certification des comptes au 31/12/2024. Dès la phase de prise de connaissance, il identifie une dépendance forte à l'outil de production, et prend connaissance d'un incident informatique significatif l'année précédente (48 h d'interruption, pénalités clients).

## Problématiques rencontrées

- L'entreprise ne dispose pas de PCA/PRI formalisé,
- Les sauvegardes sont internes et non testées,
- Aucune exigence contractuelle en matière de continuité vis-à-vis des prestataires critiques n'est formulée,
- La compétence technique est concentrée sur une seule personne, sans documentation claire des procédures de redémarrage.

## Travaux à réaliser

### Organisation et analyse métier

Le CAC doit évaluer la cohérence entre les besoins métiers et les capacités de reprise prévues :

- L'entité a-t-elle mené une analyse d'impact métier (BIA) ?
- Les activités critiques sont-elles clairement identifiées et hiérarchisées ?
- Les objectifs de reprise (RTO = temps ; RPO = données) sont-ils définis et réalistes ?
- Existe-t-il des procédures dégradées documentées pour les fonctions vitales (facturation, paie, stock) ?
- Une dépendance excessive à une personne clé a-t-elle été identifiée ? Des mesures de relais sont-elles prévues ?

### Dispositif technique et infrastructure

Le CAC s'assure de la robustesse du socle technique censé garantir la résilience :

- Les sauvegardes sont-elles régulières, externalisées, testées ? Existe-t-il un journal ou rapport associé ?
- Le PRI (Plan de Reprise Informatique) a-t-il été testé ?
- Les procédures de restauration sont-elles formalisées, accessibles et maintenues à jour ?
- Des ressources de secours (site de repli, matériel, cloud) sont-elles identifiées ? Sont-elles suffisantes ?
- Des tests de montée en charge ou de cyber-résilience ont-ils été réalisés récemment ?

### Prestataires et environnement externe

(Cf. Fiche 09 : « Sous-traitance & Cloud »)

Le CAC évalue l'intégration des tiers dans la stratégie de continuité :

- Les prestataires critiques (ERP, hébergeur, infogérant) sont-ils formellement inclus dans le PCA ?
- Des engagements de service (SLA) sont-ils définis contractuellement (disponibilité, délais de reprise) ?
- Existe-t-il une clause de réversibilité ou de portabilité des données en cas de rupture ?
- Le prestataire a-t-il fourni des rapports (ISAE 3402, SOC, tests PRI) exploitables pour l'audit ?
- En cas de défaillance du tiers, quelles solutions alternatives ou délais de redémarrage sont prévus ?

### Gouvernance, pilotage et communication de crise

Le CAC doit vérifier l'ancrage du PCA dans la gouvernance :

- Le PCA est-il validé et porté par la direction générale ?
- Le plan a-t-il été mis à jour au cours de l'exercice en fonction des évolutions (SI, structure, sites) ?
- Une instance de pilotage est-elle identifiée ? Les rôles sont-ils définis ?
- Existe-t-il un plan de communication (interne, clients, partenaires) ?
- Le personnel clé a-t-il été formé ou sensibilisé ?

## Impact pour l'approche d'audit

- Le CAC évalue l'incidence de l'absence de PCA et évalue l'impact potentiel des risques de continuité sur les états financiers au regard de la NEP 570,
- Il renforce ses travaux sur les en-cours de production et les transactions issues de l'ERP,
- Il documente et communique de manière formelle aux organes de gouvernance avec une recommandation de formalisation du PCA, test inclus.

## Séquence 4

# Allez plus loin

## Évolutions réglementaires récentes

### Directive NIS 2 (Network and Information Security)

Adoptée en 2022 et applicable à partir de 2024, cette directive européenne renforce les exigences en matière de cybersécurité et de résilience opérationnelle pour les entités essentielles et importantes. Elle impose notamment la mise en place de mesures de gestion des risques incluant des plans de continuité d'activité.

### Règlement DORA (Digital Operational Resilience Act)

Applicable au secteur financier européen à partir de 2025, ce règlement impose des exigences strictes en matière de résilience opérationnelle numérique, incluant des plans de continuité d'activité robustes et des tests réguliers.

### ISO 22301 :2019

Cette norme internationale sur les systèmes de management de la continuité d'activité a été mise à jour en 2019, avec un accent sur l'approche par les risques et l'intégration avec les autres systèmes de management.



## Ressources pratiques

### Outils CRCC

- Guide d'audit informatique complet (disponible sur le site de la CRCC)
- Questionnaire d'évaluation du PCA (format Excel, disponible en téléchargement)

### Documentation technique

- Guide ANSSI : « Élaborer un plan de continuité d'activité système d'information » (version 2023)
- Guide CLUSIF : « Plan de Continuité d'Activité - Stratégie et solutions de secours du SI »
- AFNOR : Guide de mise en œuvre de l'ISO 22301

### NEP et référentiels

- NEP 315 (Connaissance de l'entité et évaluation des risques)
- NEP 330 (Procédures d'audit mises en œuvre à l'issue de l'évaluation des risques)
- NEP 570 (Continuité d'exploitation)
- ISAE3402 (Rapports d'assurance sur les contrôles au sein d'une société de services)

## Formations recommandées

### Formation CNCC/CRCC

#### Organismes spécialisés

- BCI (Business Continuity Institute) : "Introduction to Business Continuity Management"
- ISACA : "IT Disaster Recovery Planning and Management"

#### E-learning

- MOOC ANSSI : « Sécurité numérique »