

Reprendre votre activité, quoi qu'il arrive.

Nous concevons, formalisons et testons votre plan de reprise, du diagnostic à la mise en exercice.

Hello Pomelo en bref

50	200	+10	40
clients accompagnés	collaborateurs, 8 agences	ans d'expérience	experts DevOps et cloud

CE QUE NOUS OPÉRONS



Contexte

Le PRA recouvre des réalités différentes selon les organisations : procédures de reprise, moyens techniques, tests ou formalisation complète du dispositif. Quelle que soit sa forme, son objectif reste le même : permettre à l'organisation de reprendre ses activités critiques après un sinistre majeur.

LA DÉMARCHÉ - 9 ÉTAPES

Diagnostiquer

Quelques ateliers avec vos métiers et votre IT, préparés et animés par nos soins.

- [01] Cadrage**
Définit le périmètre, les objectifs et les responsabilités.
- [02] Analyse d'impact (BIA)**
Identifie les activités critiques, leurs besoins de reprise et les dépendances de l'existant.
- [03] Scénarios de risque**
Évalue l'impact des principaux sinistres sur l'activité et le SI.
- [04] Gap analysis**
Compare les besoins du BIA aux capacités réelles face aux scénarios.

Concevoir

Nous concevons l'essentiel. Quelques ateliers pour vous présenter les choix et les valider.

- [05] Stratégies de résilience**
Définit les solutions adaptées : sauvegarde, réplication, redondance, site de repli, mode dégradé...
- [06] Formalisation**
Formalise le PRA : déclenchement, rôles, ordre de reprise, procédures et communications.

Déployer et tester

Vos équipes réalisent le déploiement ; nous supervisons et restons à vos côtés.

- [07] Mise en œuvre**
Met en place les solutions retenues et prépare leur exploitation.
- [08] Tests et exercices**
Simule différents scénarios pour vérifier les procédures, les moyens de reprise et l'atteinte des RTO/RPO.
- [09] MCO et amélioration continue**
Met à jour le PRA, intègre les évolutions du SI et réalise régulièrement de nouveaux tests.

Cas d'usage

01

Un risque cyber qui évolue

Des attaques plus industrialisées, capables d'entraîner directement une interruption d'activité. 81 % des entreprises touchées constatent un impact réel sur leur activité (CESIN).

02

Des exigences réglementaires

ISO 27001 l'exige déjà pour la certification, et NIS2 l'imposera bientôt à environ 15 000 entités françaises supplémentaires.

03

Des exigences de l'écosystème

Les entreprises dépendent de plus en plus de leurs clients, fournisseurs et prestataires. Cette interdépendance pousse donneurs d'ordre et assureurs à exiger des garanties de continuité de la part de leurs partenaires.

04

Aléas et dépendances

Incendie, coupure électrique, panne fournisseur, et une dépendance croissante : environ 70 % du cloud européen tenu par trois acteurs américains.

Nos convictions

La résilience est une responsabilité de l'entreprise, pas uniquement de l'IT.

Une interruption informatique devient vite un problème métier. Elle doit être portée par **la direction et les métiers**, avec l'IT comme acteur clé de la reprise technique.

La résilience se pense dès la conception.

Ajouter la résilience une fois l'architecture figée coûte plus cher et complique la solution ; l'intégrer **dès la conception** permet de faire les bons choix au bon moment.

Le PRA est la base, pas la seule chose qui compte.

Le PRA formalise les moyens et les modalités de reprise, mais un document ne suffit pas en situation de crise : il faut aussi savoir **qui décide, qui alerte, qui communique**.

La gestion de crise cyber est une discipline à part entière : l'ANSSI y consacre sa propre collection de guides. (ANSSI)

Parlons de votre PRA.

30 minutes avec un expert résilience, sans engagement.



Pierre-Louis d'Aubert

Responsable Cloud

pierre-louis.daubert@hello-pomelo.com

+33 6 61 58 01 52

ILS NOUS FONT CONFIANCE

BNP PARIBAS

CHAUMET

leboncoin.fr

Tereos

enovos

homair