

A photograph of several modern skyscrapers, including the Burj Khalifa, taken from a low angle looking up. The buildings have a distinct purple tint.

WAVESTONE

# Plans de Continuité d'Activité (PCA)

Enjeux et solutions

20 Novembre 2019



# Présentation



## **Axel PETERSEN**

---

- Diplômé de l'ESIEA
- Manager dans la practice Cybersecurity Digital Trust
- Une expertise sur la continuité d'activité et le management de la sécurité



Dans un monde où la capacité à se transformer est la clé du succès,  
nous éclairons et guidons nos clients dans leurs décisions les plus stratégiques



Des clients leaders  
dans leur secteur



2,500 collaborateurs  
sur 4 continents



Parmi les leaders du conseil  
indépendant en Europe,  
n°1 en France

Paris | Londres | New York | Hong Kong | Singapour\* | Dubaï\* | São Paulo\*  
Luxembourg | Madrid\* | Milan\* | Bruxelles | Genève | Casablanca | Istanbul\*  
Lyon | Marseille | Nantes

# Une capacité unique à combiner expertise sectorielle, connaissance des fonctions de l'entreprise et maîtrise des technologies

## FONCTIONS

---

- Stratégie
- Management et financement de l'innovation
- Marketing, ventes & expérience client
- People & change
- Finance & performance
- Operations & logistique

## SECTEURS

---

- Banque & assurance
- Télécoms & média
- Biens de consommation & distribution
- Industrie
- Énergie & utilities
- Transport & voyages
- Immobilier
- Secteur public & institutions internationales

## TECHNOLOGIES

---

- Stratégie digitale & SI
- Technologies digitales & émergentes
- Architecture SI & data
- Cybersécurité & confiance numérique

# Objectifs du cours



**Partager la notion de  
Plan de Continuité  
d'Activité (PCA)...**



**... pour sensibiliser à la  
nécessité de mitiger  
des risques ...**



**... et vous donnez la  
base des solutions  
envisageables**

# Agenda

## ► 1. Introduction à la continuité d'activité

1. 1 Concepts clés

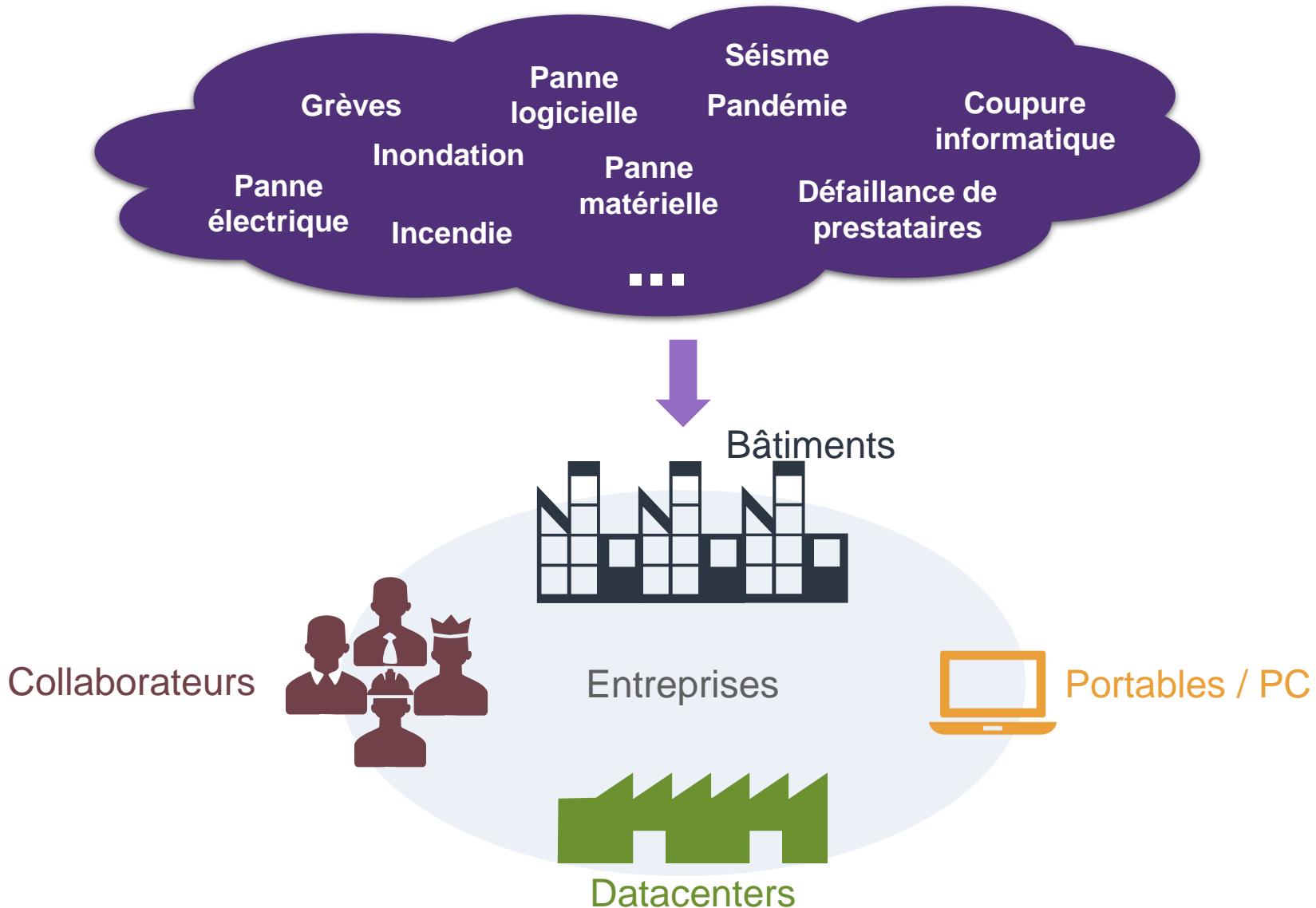
1. 2 Démarche de mise en place d'un PCA

## 2. Plans de Continuité Informatique

## 3. Plans de Continuité des Opérations

## 4. Gestion des incidents et des crises

# Des menaces pèsent sur les entreprises



# Des menaces bien réelles !

**11 septembre 2001**

Attentats du World Trade Center



Terrorisme

2750 morts, 800 000 m<sup>2</sup> de bureaux rasés. 350 entreprises et 40 000 personnes étaient présentes sur le site.

**11 mars 2011**

Séisme au large du Japon



Catastrophes naturelles

Séisme puis tsunami et catastrophe nucléaire. 20 000 morts, conséquences majeures sur les infrastructures, forte perturbation de l'activité économique du pays.

**13 Aout 2015**

L'explosion de Tianjin



Accident

Une série d'explosion tua plus de 100 personnes et en blessa des centaines. D'importants dégâts ont été signalés jusqu'à 2km autour du site.

**Février 2017**

Une partie d'AWS inaccessible



Erreur humaine

Une mauvaise commande tapée par un technicien lors d'une maintenance a causé une interruption de nombreux services AWS pendant plusieurs heures.

**Avril 2017**

Panne de climatisation Rennes 2



Gestion de la température

2 jours d'interruption du SI de l'université de Rennes suite à une surchauffe du datacenter dû à une panne de la climatisation entraînant l'annulation d'exams.

**Mai 2017**

Wannacry



Cyber-attaque

Plus de 300.000 ordinateurs dans 150 pays ont été touché par ce rançongiciel. Des entreprises comme Renault ont été contraintes de suspendre leurs activités.

**Mai 2017**

British Airways



Panne électrique

Indisponibilité du SI pendant plusieurs jours suite à une surtension dans le datacenter principal provoquant l'annulation de centaines de vols. Un coût de plusieurs centaines de M€.

**Juillet et Novembre 2017**

OVH



Pannes électrique

Juillet : incident électrique avec perte des baies de stk qui ne redémarreront pas (30h d'indisponibilité, +100 serveurs virtuels impactés).

Novembre : 2 lignes EDF 20KVA HS + 2 chaînes électrogène en défaut

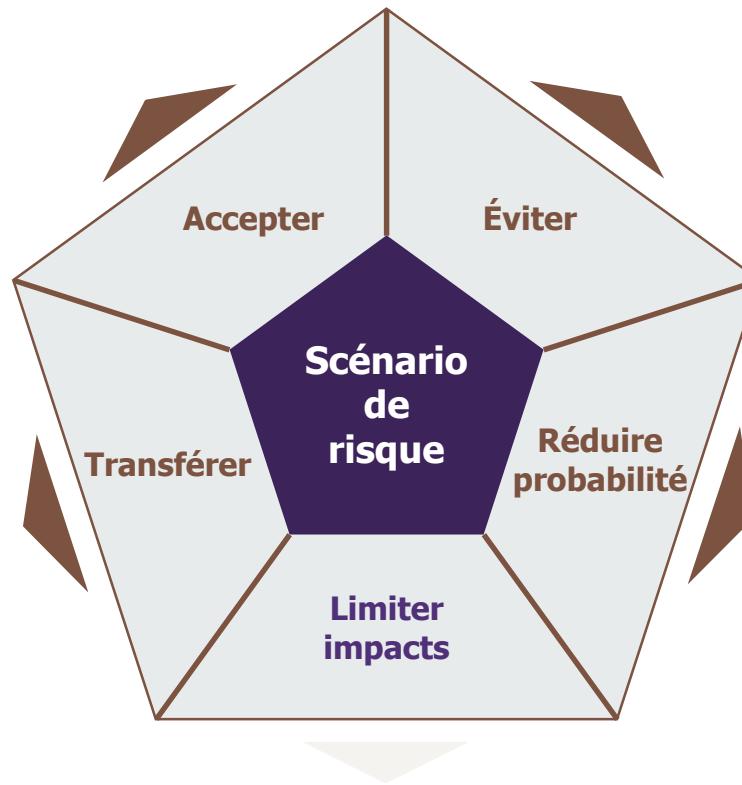
# Plusieurs options pour traiter les risques

## Accepter

Accepter la menace et ses impacts potentiels pour l'entreprise

## Éviter

Ne pas lancer ou à arrêter une activité à cause des risques encourus



## Transférer

Déporter le risque sur un tiers (prise d'une assurance, transfert d'une activité à un prestataire, ...)

## Réduire la probabilité

Traiter le risque en amont, en réduisant sa probabilité d'occurrence

## Limiter les impacts

**Plan de Continuité d'Activité (PCA) :** ensemble de dispositifs permettant de limiter les impacts lorsqu'un ou plusieurs scénarios de risques sont avérés

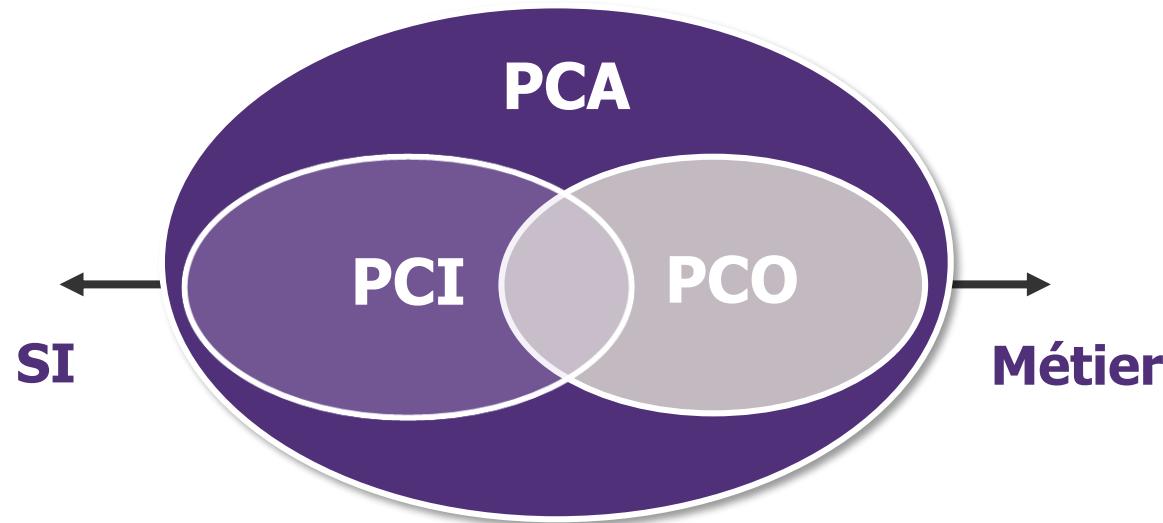
→ Un dispositif relevant d'un **équilibre coût / couverture de risques**

Couverture de risques

Coût

## Quelques éléments de terminologie PCA

Le Plan de Continuité d'Activité englobe l'ensemble des **actions, processus et organisations** permettant la continuité des activités critiques de l'Entreprise



**Le Plan de Continuité Informatique (PCI)** se focalise sur la disponibilité de tout ou partie du Système d'Information

- En cas d'incident
- Face à un sinistre majeur

**Le Plan de Continuité des Opérations (PCO)** se focalise sur la poursuite des missions essentielles des métiers jugés vitaux face notamment à un sinistre majeur

Attention : l'emploi des terminologies PCA, PCI, PRI, PSI, PRA ... n'est pas uniforme et la signification qui leur est donnée varie selon les entreprises et parfois en leur sein même

# PCI vs Cyber-résilience

## PCI

Ensemble des moyens techniques et organisationnels permettant la continuité des activités informatiques critiques de l'Entreprise

**Couverture du risque d'incident ou de panne**

*Ex : panne électrique, incident télécom, panne serveur...*



**Garantir la continuité de service au quotidien et la reprise sur incident complexe**

**Couverture du risque de sinistre majeur sur périmètre critique**

*Ex : incendie, inondation, accident industriel...*



**Garantir la reprise d'activité sur sinistre majeur, ayant possiblement entraîné une perte de données et dans un contexte fortement dégradé**

Terminologies employées le plus souvent :  
PRI : Plan de Reprise Informatique  
PRA : Plan de Reprise d'Activité  
PSI : Plan de Secours Informatique  
DRP : Disaster Recovery Plan

## Cyber-résilience

**Faire face à une menace non déterministe pouvant aussi affecter les dispositifs de secours**

*Ex : APT, ransomware, DDOS ...*



**Possiblement dans un contexte de perte de confiance dans le SI (postes, serveurs ...) et de ses dispositifs de secours**

# Focus sur le PCI

## Garantir la continuité\* de service au quotidien

-  Perte d'un serveur
-  Perte d'un équipement réseau
-  Perte d'un composant stockage
-  Perte d'un équipement électrique
-  Perte d'un équipement de clim.
-  Perte de lien électrique
-  Perte de lien télécom

## Garantir la reprise sur incident complexe

Cas complexes ou pas francs, au-delà des cas traités par la continuité de service au quotidien.  
Ils nécessitent une analyse et une intervention plus spécifique.

## Garantir la reprise de l'informatique du périmètre critique sur sinistre majeur (PSI)

Ex :  Inondation  Incendie

**La reprise de l'informatique sur sinistre majeur est activée suite à la décision d'une cellule de crise après avoir suivi un processus d'escalade.**

**Peut nécessiter de mobiliser des moyens humains exceptionnels** (acteurs spécifiques, horaires non ouvrés, ...)

**\* La bonne pratique des datacenters est de s'appuyer sur des technologies fortement redondantes qui permettent de couvrir sans aucun impact client les pannes les plus courantes**

# Deux grandes notions à définir avec les métiers : DIMA / PDMA

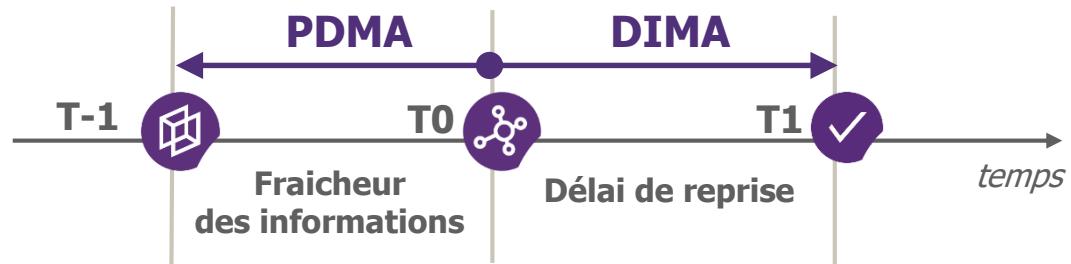
## 2 critères attendus dans l'expression de besoin de continuité

### DIMA ou Recovery Time Objective (RTO)

Durée d'interruption maximale admissible  
ex : durée pendant laquelle j'accepte l'indispo du mail

### PDMA ou Recovery Point Objective (RPO)

Perte de donnée maximale admissible  
ex : historique de mails perdus que j'accepte



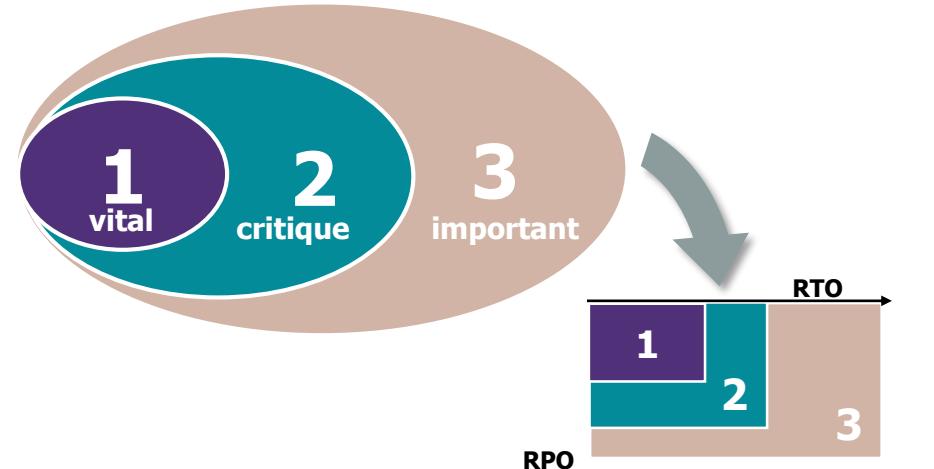
## Une expression de besoins de continuité métier « à objectiver »

### Une réflexion autour de cercles de criticité ...

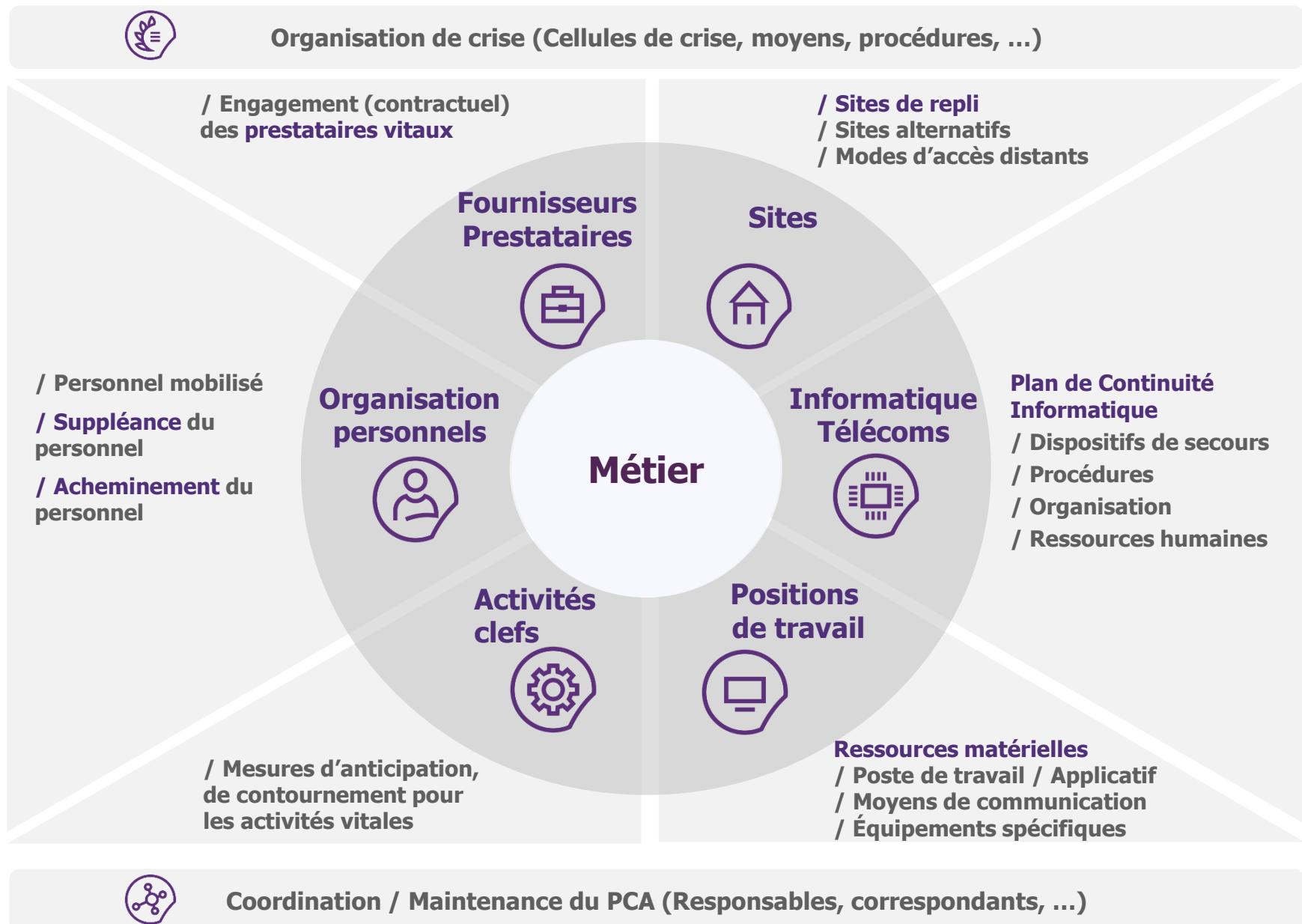
- / Pour répartir les **processus métiers** les plus importants et en déduire les applications concernées
- / Intégrer les **infrastructures** supportant ces applications

### Qui se déclineront en ...

- / **Priorités** de traitement dans le cadre du PCA
- / Potentiellement en **niveaux de sécurité** (DIMA, PDMA)
  - > En tenant compte des moyens et des ressources de la DSIT
  - > Pour industrialiser les solutions de secours



# Les différentes composantes d'un PCA



## Une norme pour le PCA : ISO 22301

Officiellement publiée en mai 2012, l'**ISO 22301** s'inspire fortement de celle faisant précédemment référence pour la continuité d'activité (BS 25999, publiée par le British Standard Institute), qu'elle remplace.

Les entreprises certifiées sont surtout présentes dans le monde anglo-saxon.

Plusieurs stratégies sont possibles pour les entreprises vis-à-vis de cette nouvelle norme :

### Alignement

Adoption des processus les plus utiles pour augmenter l'efficacité de la démarche continuité

### OBJECTIF

Piloter la continuité par les risques et entrer dans une démarche de progrès continu

- / Donner de la cohérence et de la légitimité à la démarche continuité
- / Prioriser les investissements
- / Impliquer les acteurs métiers et le management
- / Faire la publicité en interne d'un processus continuité efficace

*... mais des efforts plus difficiles à valoriser en externe si l'on ne va pas jusqu'à la certification*

### Certification

Respect intégral de la norme et garantie **externe** de sa mise en œuvre

Et en plus...

- / Constituer un élément **differentiant** sur le marché
- / Répondre à des **attentes** de la part des parties prenantes (AO, audits...)
- / Faciliter d'autres **démarches réglementaires** (Bâle II, Solvency, CRBF, Obligation OIV, ...)
- / Garantir de mener à bien les **plans d'actions** continuité définis

*... mais*

- / *attention à poursuivre les efforts après l'obtention de la certification*
- / *la certification ne garantit pas le caractère opérationnel du PCA !*

*NB : La norme ISO 22301 est conçue afin de permettre une mise en œuvre « en parallèle » d'autres normes (ISO 27001 par exemple) en consolidant l'organisation et en mutualisant certaines actions (on parle alors de « **Systèmes de Management Intégrés** »)*

# Agenda

## ► 1. Introduction à la continuité d'activité

1. 1 Concepts clés

1. 2 Démarche de mise en place d'un PCA

## 2. Plans de Continuité Informatique

## 3. Plans de Continuité des Opérations

## 4. Gestion des incidents et des crises

# Démarche d'élaboration d'un PCA



# ETAPE 1 : cadrage

1

## Cadrage

Analyser les **scenarios de risque**

Définir les **besoin métiers**

### 1 Recensement des menaces

#### Facteurs naturels

Tremblement de terre, inondation, éboulement, glissement de terrain, ...

#### Facteurs environnementaux

Proximité avec des sites industriels...

#### Facteurs techniques

Dégâts physique, indisponibilité d'un équipement, faille logicielle, cyber-attaque...

#### Facteurs humains

Phénomènes sociaux, mouvements sociaux  
vandalisme, erreur humaine...

2

### PSI



#### Indisponibilité totale ou partielle du SI

- / Black-out électrique du Datacenter
- / Propagation d'un virus ou malware
- / ...

### PCO



#### Indisponibilité de fournisseurs critiques

- / Sinistre dans le périmètre du fournisseur,
- / Indisponibilité des fournisseurs SI...



#### Indisponibilité totale ou partielle d'un site

- / Incendie
- / Inondation
- / ...



#### Indisponibilité du personnel

- / Pandémie,
- / Mouvement social,
- / ....

3

### Identification des processus critiques

- / Quelles activités ont le plus d'impact sur l'entreprise lors d'une interruption?
- / Quel est le temps de reprise nécessaire?
- / Quels ressources sont nécessaires

D0	D1	D2	D3	D4	D5
1H	4H	1J	2/3J	1S	2/3S

### Outils utilisés : BIA



Un questionnaire rempli et mis à jour par les métiers en collaboration avec les équipes PCA.

# Les risques

Risque : probabilité combinée avec les impacts

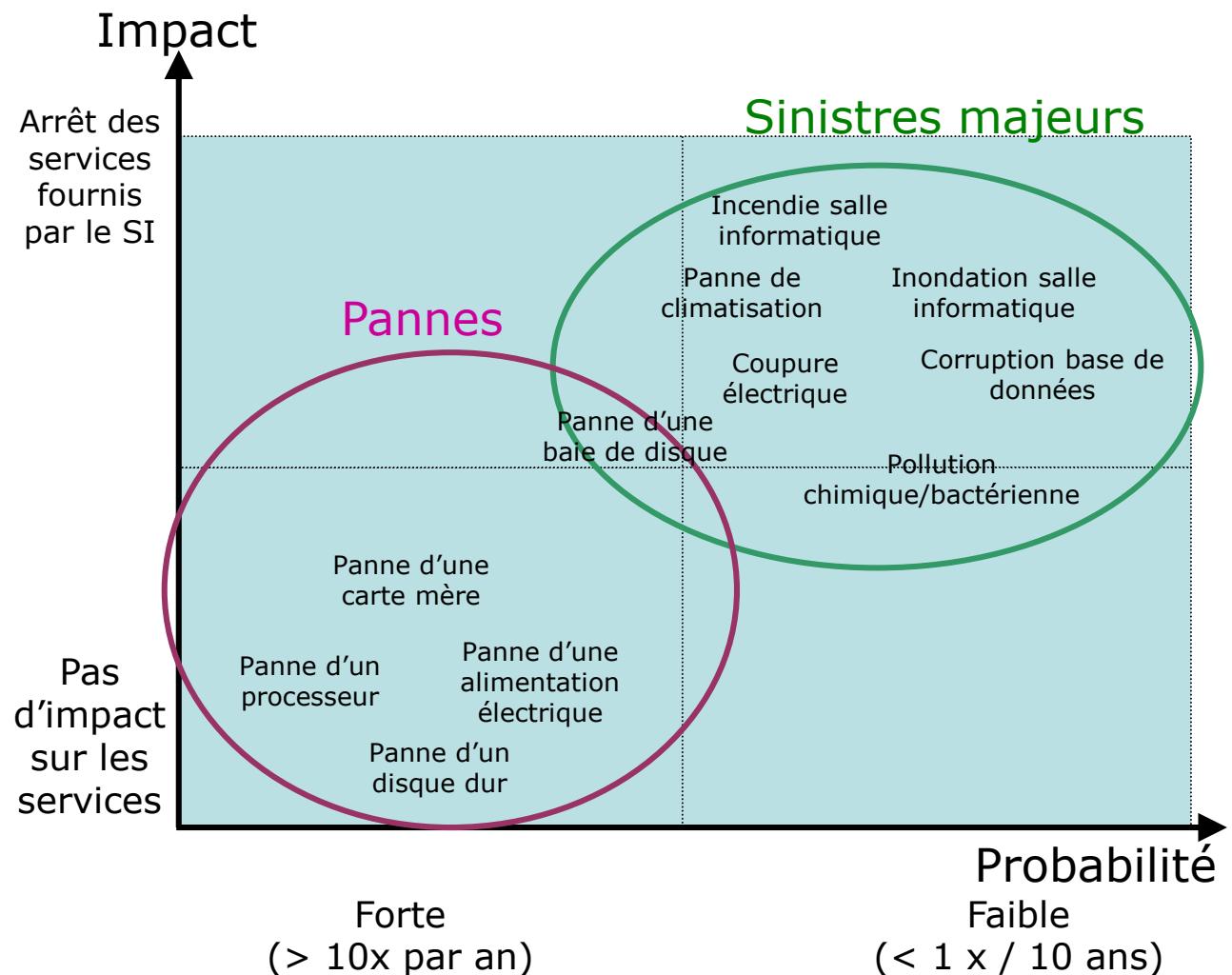
## Evénements subis

### / Courants (plus d'1x par an)

- Panne matérielle légère = déficience ou arrêt d'un composant technique
- Erreurs humaines
- Malveillance type virus
- Corruption des données

### / Exceptionnels

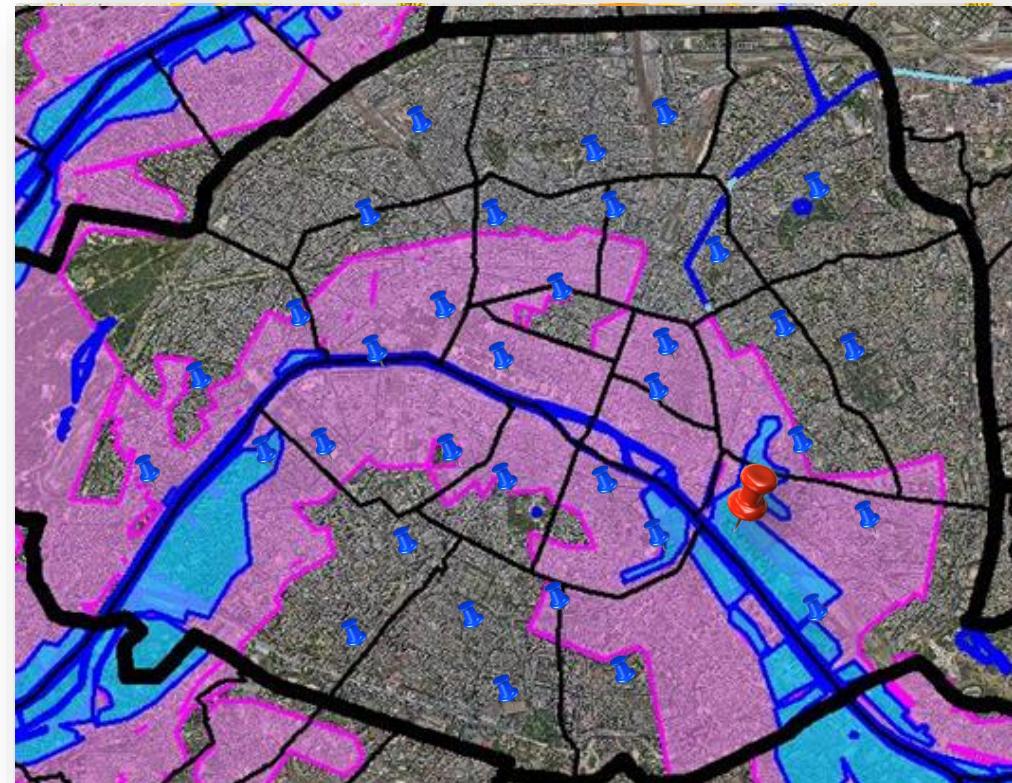
- Perte d'infrastructures en SPOF
- Suite d'erreurs humaines
- Attaque ciblée
- Sinistre majeur = perte durable du datacenter (technique, humain, ...)



## Exemple identification d'une menace

### Contexte

- / Banque
- / Siège près de la Gare de Lyon (*bâtiment de 10 étages*)
- / 1000 collaborateurs au siège
- / Beaucoup d'agences dans Paris pour la relation client et le retrait d'argent
- / Le SI est situé au sous-sol, à coté des installations électriques
- / Activités bancaires classiques



Légende



Agences

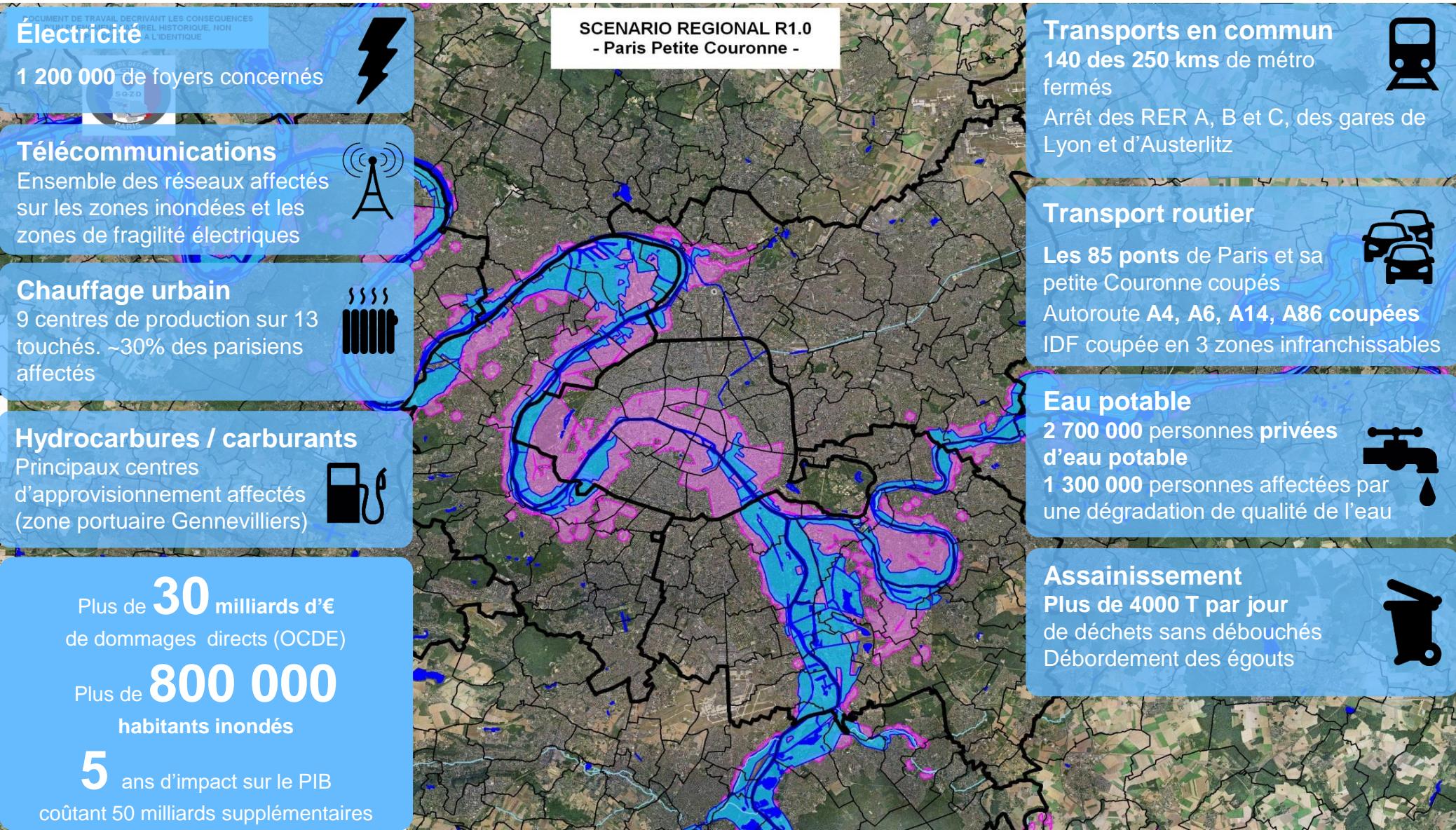


Siège



Quelle menaces ?

La crue de Seine est un choc extrême qui impacte l'ensemble des ressources critiques...



# Des menaces peuvent avoir des impacts multiples

**L'indisponibilité d'activités clés peut causer des impacts majeurs et multiples pour les organisations**

## Image

**Ex :** perturbation importante des activités entraînerait une dégradation de l'image de marque de la banque vis-à-vis du public et des autres acteurs de la place.

## Financier

**Ex :** la perturbation de certaines activités critiques (ex : salles de marchés) peut entraîner rapidement des impacts de plusieurs millions d'euros.

## Interne

**Ex :** incidents à répétition sur les systèmes informatiques pourraient entraîner des mécontentements clients en agences et une dégradation des conditions de travail des agents.

## Legal

**Ex :** la continuité des activités vitales des banques est rendue obligatoire par la réglementation (CRBF 97-02).

## Client

**Ex :** un incident informatique pourrait entraîner la perception avec retard des prestations sociales.

*Exemples d'impacts pour une grande banque*



# Construire une grille d'impact

## Contexte

Pour proposer une stratégie de secours informatique adéquate, il est nécessaire de **connaitre le besoin réel de secours** des métiers

## Éléments de réponse

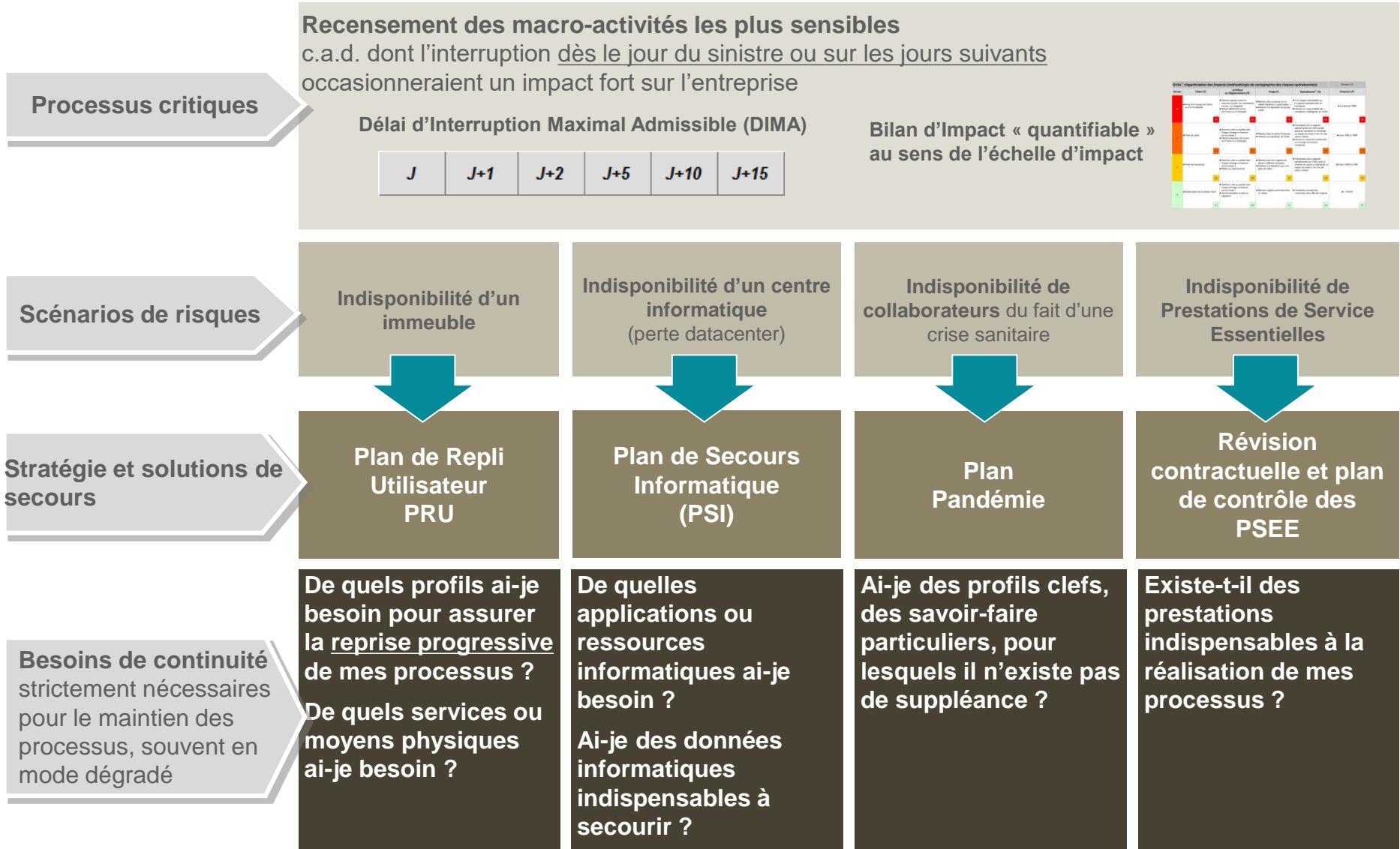
Niveau d'impact		0 - Négligeable	1 - Limité	2 - Significatif	3 - Grave	4 - Extrêmement grave
Impacts	Perte financière	Aucune ou négligeable	Inférieure à 10 k€	Inférieure à 100 k€	De l'ordre de 1M€	Fermeture d'un activité ou faillite de l'entreprise
	Atteinte aux vies humaines	Aucune	Aucune	Aucune	Accident sans perte humaine	Accident ou attentat avec pertes humaines
	Perte de productivité	Inférieure à 2h/Homme	Inférieure à 1j/Homme	Inférieure à 1 s/Homme	De l'ordre de plusieurs mois/Homme	Fermeture d'une activité
	Retard	Aucun	Inférieur à 5min	Inférieur à 1 heure	Retards multiple supérieur à 1 heure	Désorganisation du trafic
	Atteinte à l'image de marque	Pas de ressenti des clients	Ressentie faible des clients	Ressenti négatif d'un groupe de clients	Ressenti important de l'ensemble de la clientèle	Ressenti important de l'ensemble de la population

## Problématique

Comment évaluer de façon objective les besoins de secours des activités métiers ?

- / Grille d'impacts métier
- / Hiérarchisation des besoins de secours

# Le BIA (Bilan d'Impact sur l'Activité / Business Impact Analysis)



# Étape 2 : définir la stratégie pour le PSI (Plan de Secours Informatique)

## 2 Stratégie

Conception de **solutions générales**

**Cas métiers**

### 1 Définir les solutions de reprise possibles

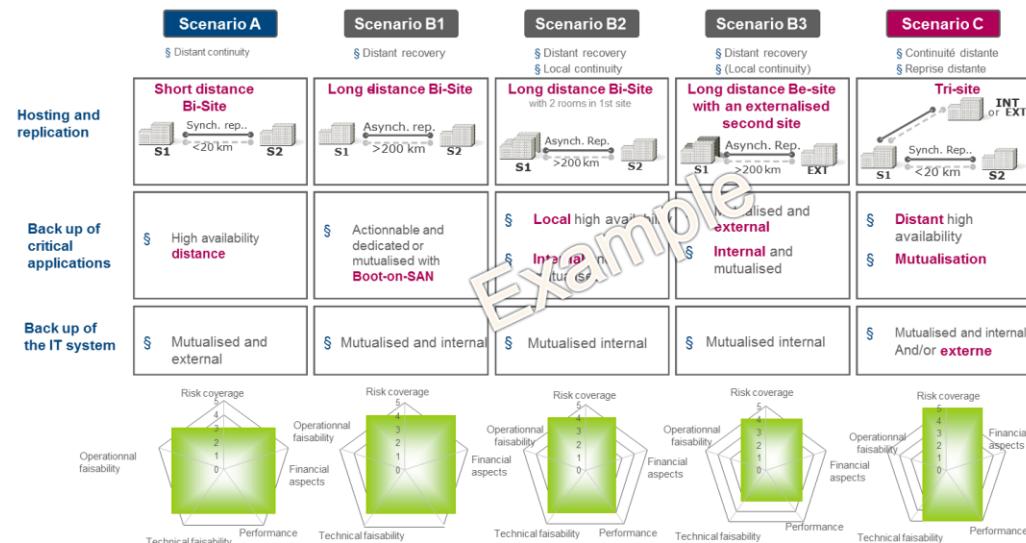


Pour chaque couche du SI, étudier les solutions de reprise disponibles

<b>Applications</b>	Dedicated hardware	Active (Clustering, loadbalancing..)	Activable	Dormant
	Hardware pooling	Internal pooling (Pré production, integration tests...)	External pooling (with a service provider)	
	Provided hardware	Order when the disaster occurrence	Settlement before disaster occurrence	
<b>Infrastructure services</b> (DNS, hypervisor...)	Data storage replication Synchronous/Asynchronous	Server replication	Backup VTL	
	Duplicated network	Distinct networks	Extended network	Mixed network
	Available sites	Internal or external hosting	Datacenter resilience	

### 2 Construire les scénarios et sélectionner les pertinents

Construire les scénarios de reprise possibles et les sélectionner en fonction des besoins et des coûts.



# Étape 2 : définir la stratégie pour le PCO

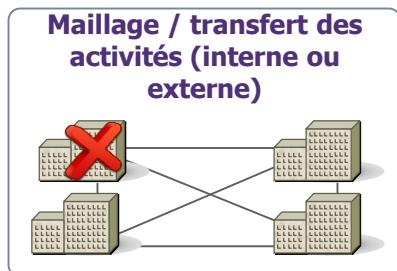
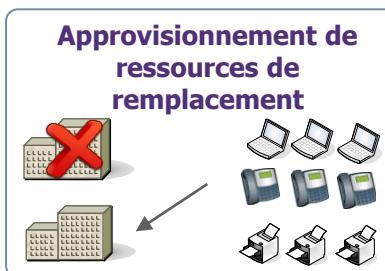
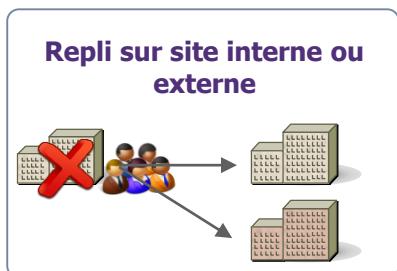
## 2 Stratégie

Conception de **solutions générales**

**Cas métiers**

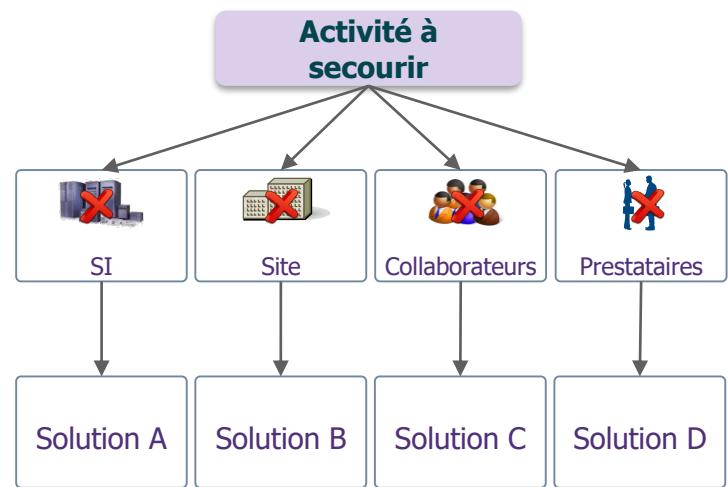
### 1 Définition de la « Boîte à outils » des solutions des secours

*Un panel de solutions à disposition des PCO pour apporter une réponse adaptée au sinistre*



### 2 Choix des stratégies

*Définition des solutions à appliquer pour chaque activité à secourir et cas de sinistre à traiter*



# Étape 3&4 : conception et mise en œuvre

## 3 4 Conception et implémentation

Organisation

**Infrastructure technique**

**Procédures de reprise du SI**

Site(s) de **secours informatique**

Organisation

**Moyens de secours**

**Procédures dégradées**

Site(s) de **repli utilisateurs**

### 1 Mise en œuvre des solutions techniques



- / Conception détaillée des solutions techniques
- / Commande du matériel et équipement du site informatique de secours
- / Configuration des solutions...

### 2 Documentation du secours informatique



- / Formalisation du plan d'activation globale du secours informatique
- / Formalisation des procédures de test techniques et fonctionnels du secours
- / Définition de l'organisation de crise SI...

### 1 Préparation du matériel



- / Préparer les sites de repli
- / Préparer les stations de secours
- / Sélection des fournisseurs
- / ...

### 2 Documentation



- / Méthode de management de crise
- / Manuel de méthodes alternatives
- / Mesures préventives
- / Définition de l'organisation de crise ...

# Étape 5 : Recette

5

## Recette

Démontrer l'efficacité des solutions techniques  
Démontrer la vraisemblance des procédures et de l'organisation

### 1 Test planning

Définir le périmètre du test, le réalisme, le timing et les critères de succès

2015            2016            2017

Test 1

Test 2

Test 3

### Périmètre

→ ***Quelles composantes du PCI/PCO ont besoin d'être testées ?***

Un périmètre trop ambitieux peut entraîner des problèmes de coordination et un échec du test.

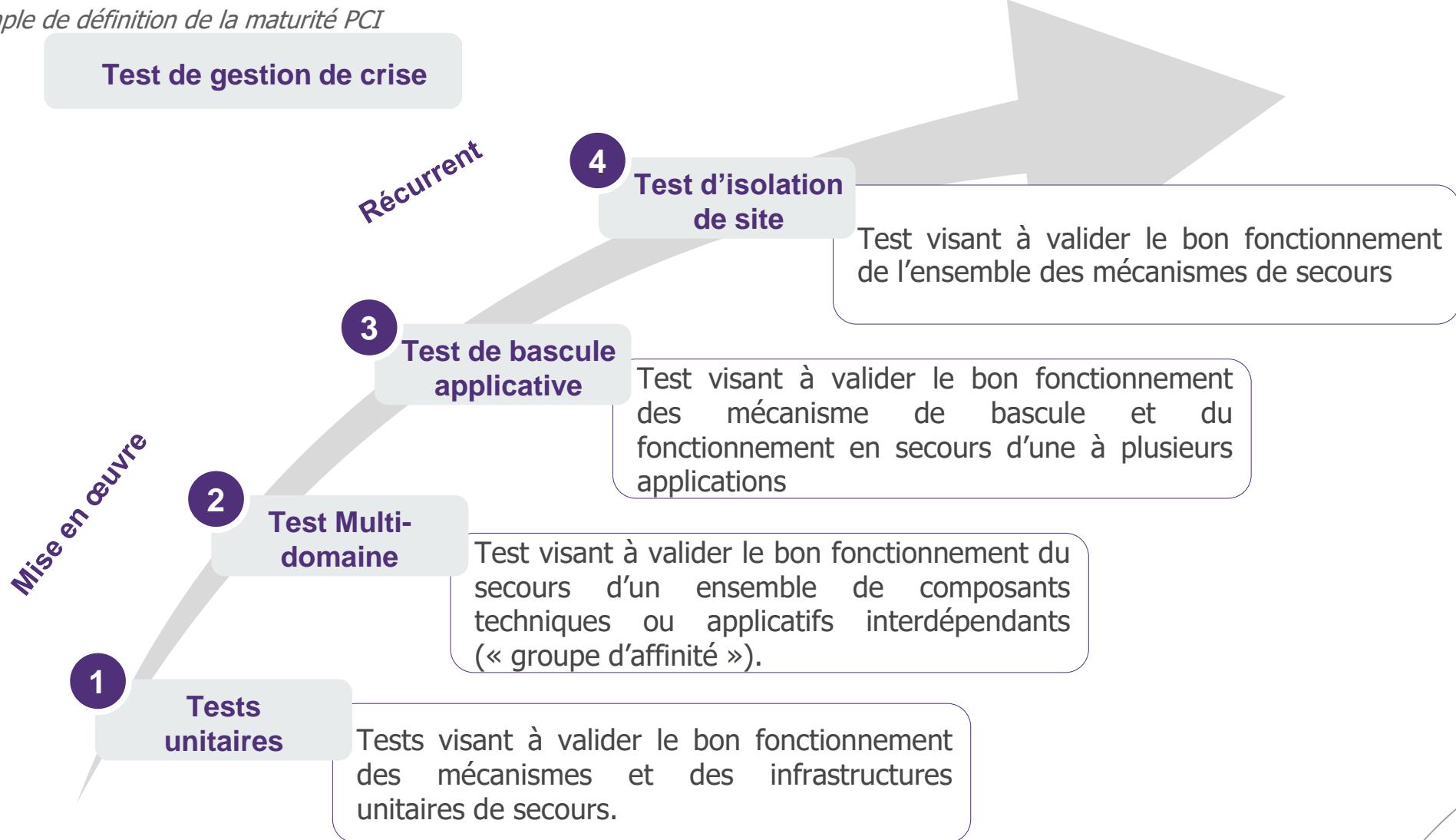
### Réalisme

→ ***Quelles sont les limites d'une simulation d'un sinistre ?***

- / Plus la simulation est réaliste, plus les résultats seront fiables.
- / Ex PSI : Un service garantit que les sauvegardes nécessaires sont disponibles, mais il ne garantit pas que les données sauvegardées sont suffisamment complètes pour une reprise d'une application.

# Cibler une approche progressive pour améliorer la maturité des test

Exemple de définition de la maturité PCI



# Définir des objectifs ambitieux et interpréter les tests correctement

## Qu'est ce qu'un test réussi ?

Un test qui n'identifie pas d'incohérences ou de dysfonctionnements doit être regardé avec précaution : soit le PCI est parfait... soit il ne correspond pas du tout !

En revanche, si le test « challenge » les équipes et les force à faire face à des situations incertaines, ce n'est pas nécessairement un échec...

***Selon le contexte, il faut trouver un équilibre entre les « actions à améliorer » (dues aux défaillances) et la « confiance » (en lien avec des tests réussis)***

## Pourquoi construire une simulation « réaliste » ?

Avec les tests PCI/PCO fréquents (au moins une fois par an) effectué à des larges échelles (1 métier, 1 site, etc.), il n'est pas possible de juger exactement le niveau d'efficacité du PCA, même si cela met en lumière des faiblesses.

Effectuer des petits tests (tests unitaires) empêche d'identifier des problèmes qui peuvent apparaître lors de réelles situations de crise (ex : communication lente).

Le test le plus pertinent est finalement celui qui se rapproche de cas réels : ce n'est pas une utopie, de nombreuses grandes organisations mènent ce type de tests.

→ ***Le test PCI/PCO réaliste est le seul moyen tangible de garantir un plan opérationnel.***

# Retour d'expérience : un exercice complet

## Préparation

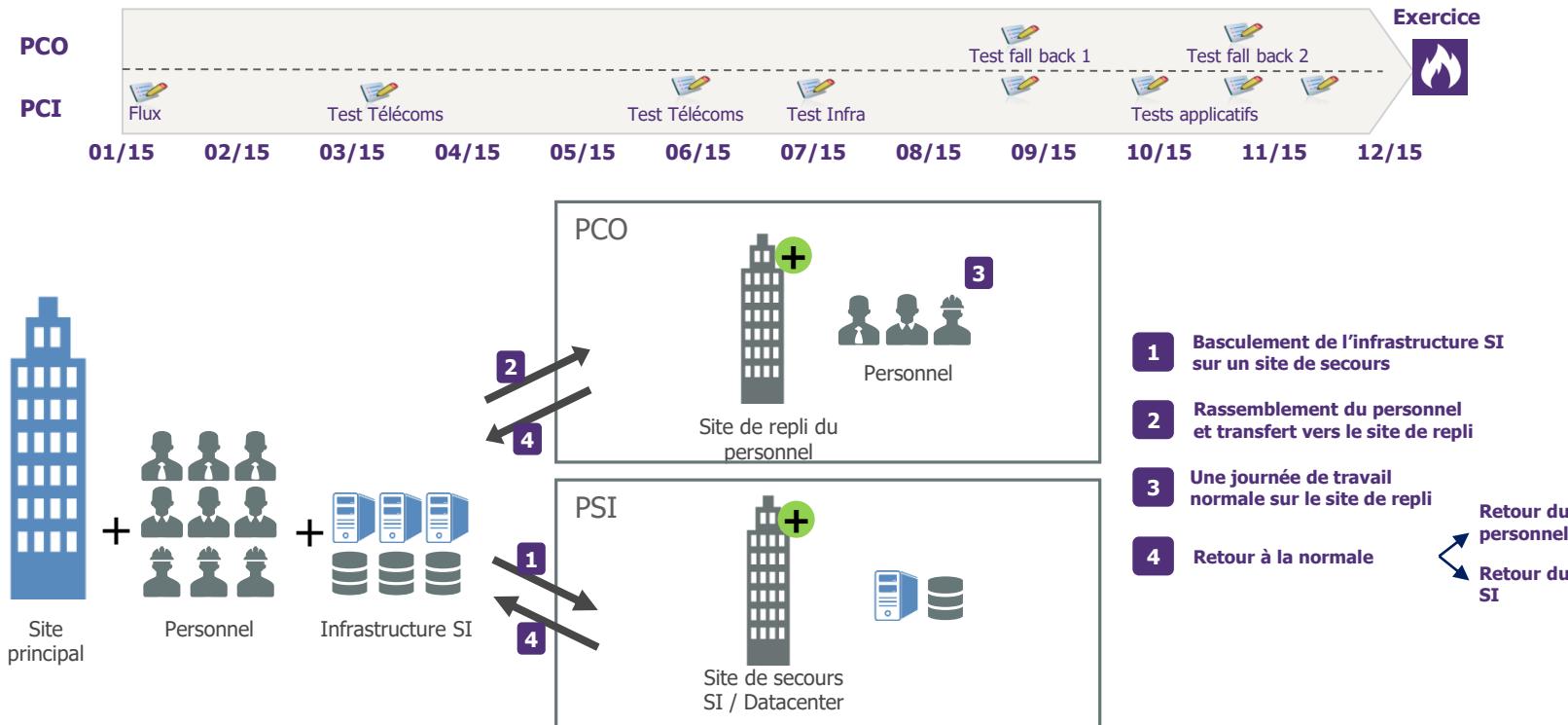
Un plan ambitieux incluant un large panel de tests

## Scénario de l'exercice

Un exercice exhaustif (basculement de la production et du personnel)

## L'exercice

10 jours de tests (et de stress...)



## Étape 5 : Maintenance et amélioration

5

## Maintenance

# Tests réguliers

## Mise à jour de la **stratégie de secours**

## Mise à jour des procédures techniques

## Mise à jour des procédures

## 1 Besoins métiers mis à jour

Mise à jour du BIA

## 2 Adaptation de la stratégie

Adapter la stratégie aux récents besoins métiers / tests.

### **3 Mise à jour des solutions et procédures**

Adapter les solutions et les procédures en accord avec la nouvelle stratégie et les résultats des tests.



### Serveurs d'application



## Routeur Wi-Fi



Serveurs BDD



## Switch

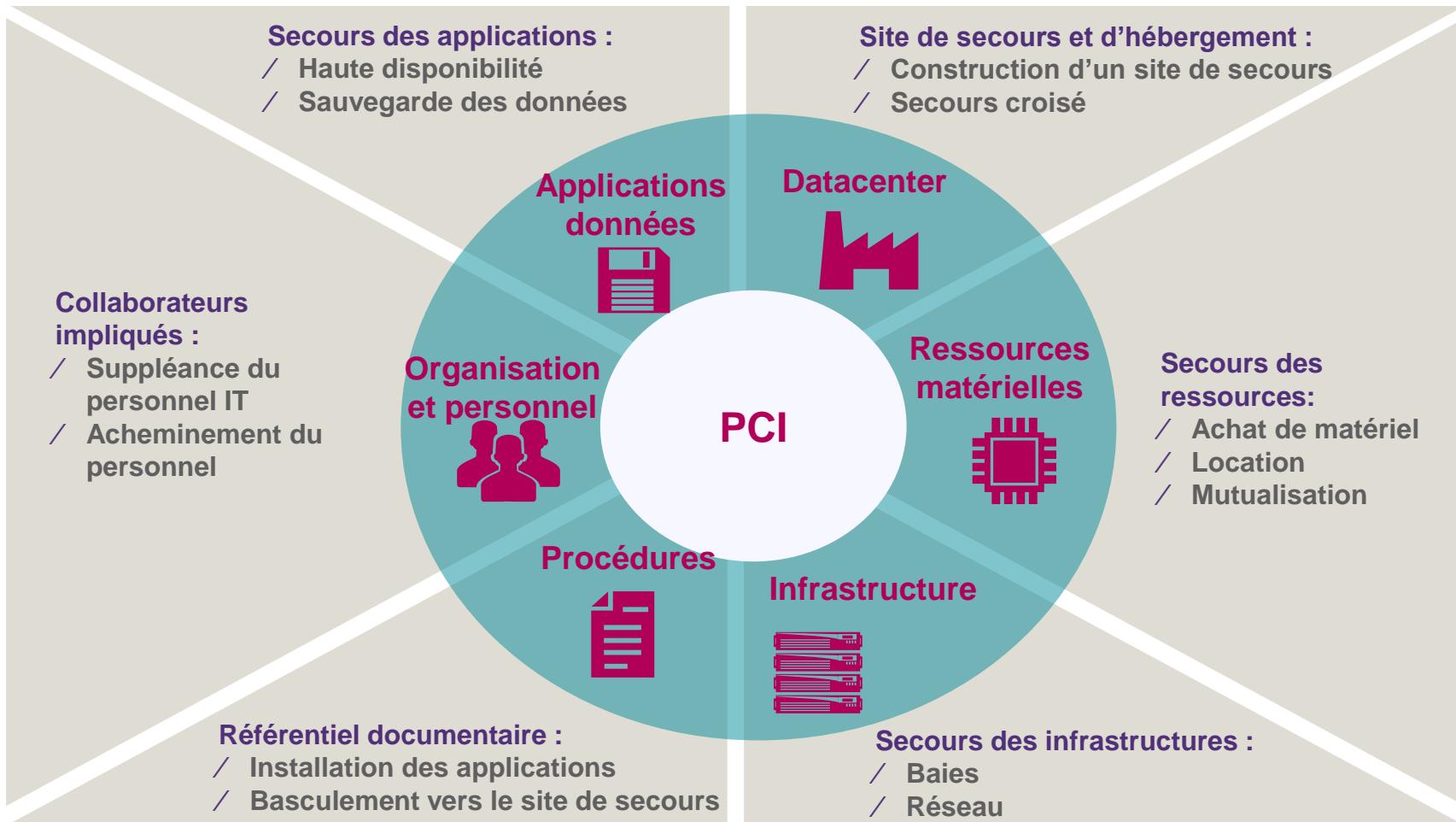
Server messagerie, serveurs imprimantes,  
serveurs de fichiers ...

# Agenda

1. Introduction à la continuité d'activité
- 2. Plans de Continuité Informatique
  2. 1 *Eléments constitutifs*
  2. 2 *Tendances*
  2. 3 *Exemple de mission PCI*
3. Plans de Continuité des Opérations
4. Gestion des incidents et des crises

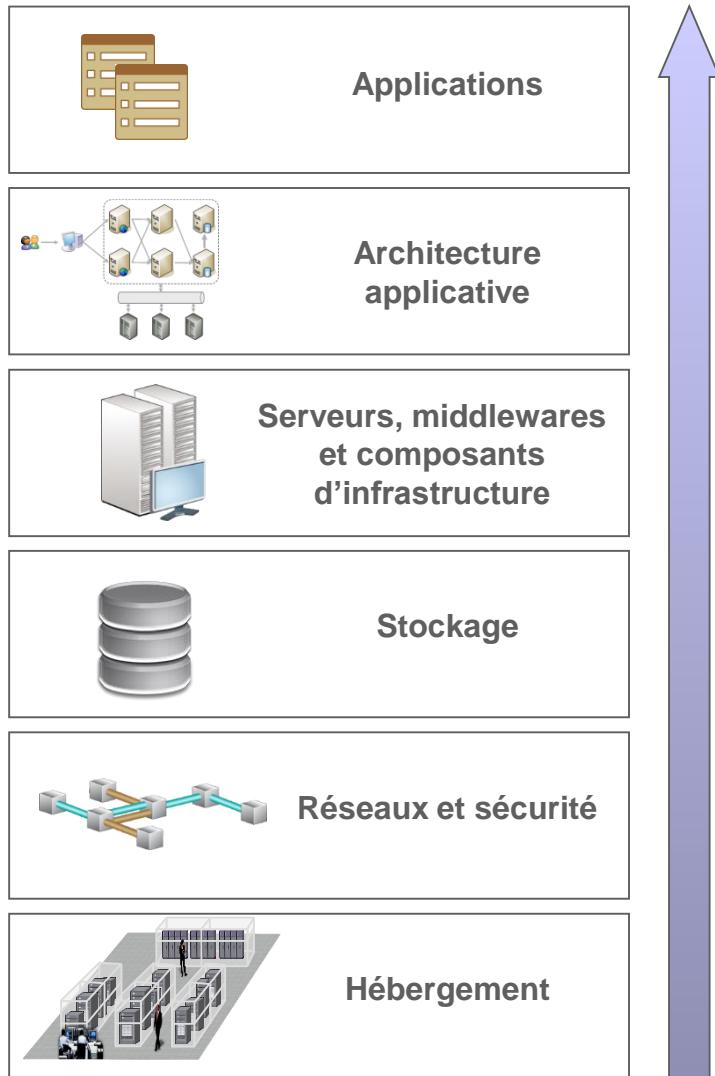
# Les composants d'un plan de continuité informatique

## Organisation de crise (Cellules Décisionnelle, de Gestion de la Crise...)



## Coordination / Maintenance du PCA (Responsables, correspondants...)

# Les composantes de la continuité



## Principes de conception

Définir une stratégie de secours consiste à :

- / Combiner en un ensemble cohérent, exploitable et maintenable...
- / ... des solutions variées définies pour chaque couche technique



## Tendance majeure du secours

Mise en œuvre progressive de solutions « actif/actif », en commençant par les couches basses du SI :

- / Pour implémenter rapidement un secours HD pour les applications récentes...
- / ... tout en permettant le maintien de solutions plus anciennes pour les autres

## Trois angles de vue

Un stratégie PCI permet de répondre à des besoins qu'il convient d'identifier.  
Trois angles de vue sont à examiner pour ce faire.

### Stratégie PCI

#### Risques

*Quelle est la couverture de risques souhaitée ?*

- / Panne ou sinistre local
- / Sinistre de site
- / Sinistre régional / Choc extrême

#### Performances

*Quelles sont les performances attendues ?*

- / Continuité de fonctionnement ou reprise d'activité ?
- / Délais de reprise
- / Fraîcheur des données

#### Activation

*Quel est le mode d'activation du secours souhaité?*

- / Bascule de tout ou rien en secours
- / Bascule modulaire par application

# Des questions amenant à des choix

Une combinaison de stratégies à déterminer en fonction de l'existant et du secours souhaité

Question ?

Couverture de risques



Choix

A. Stratégie d'hébergement

Performances de reprise



B. Stratégie de secours des serveurs et des données

Mode d'activation du secours

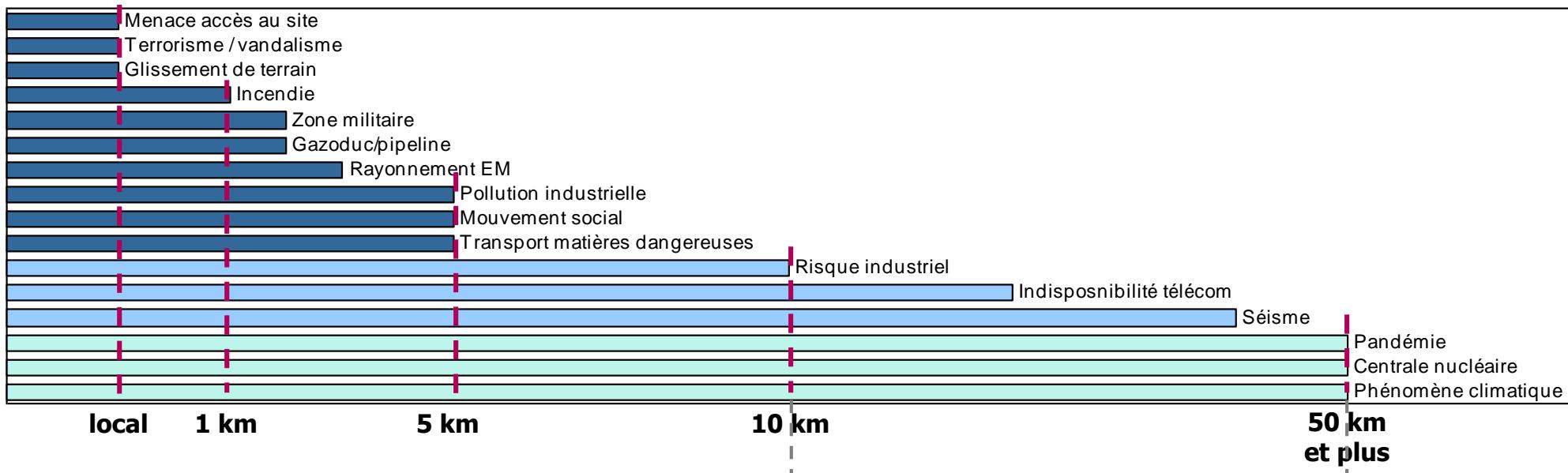


C. Stratégie d'activation

# Stratégie d'hébergement : couverture du risque (1/2)

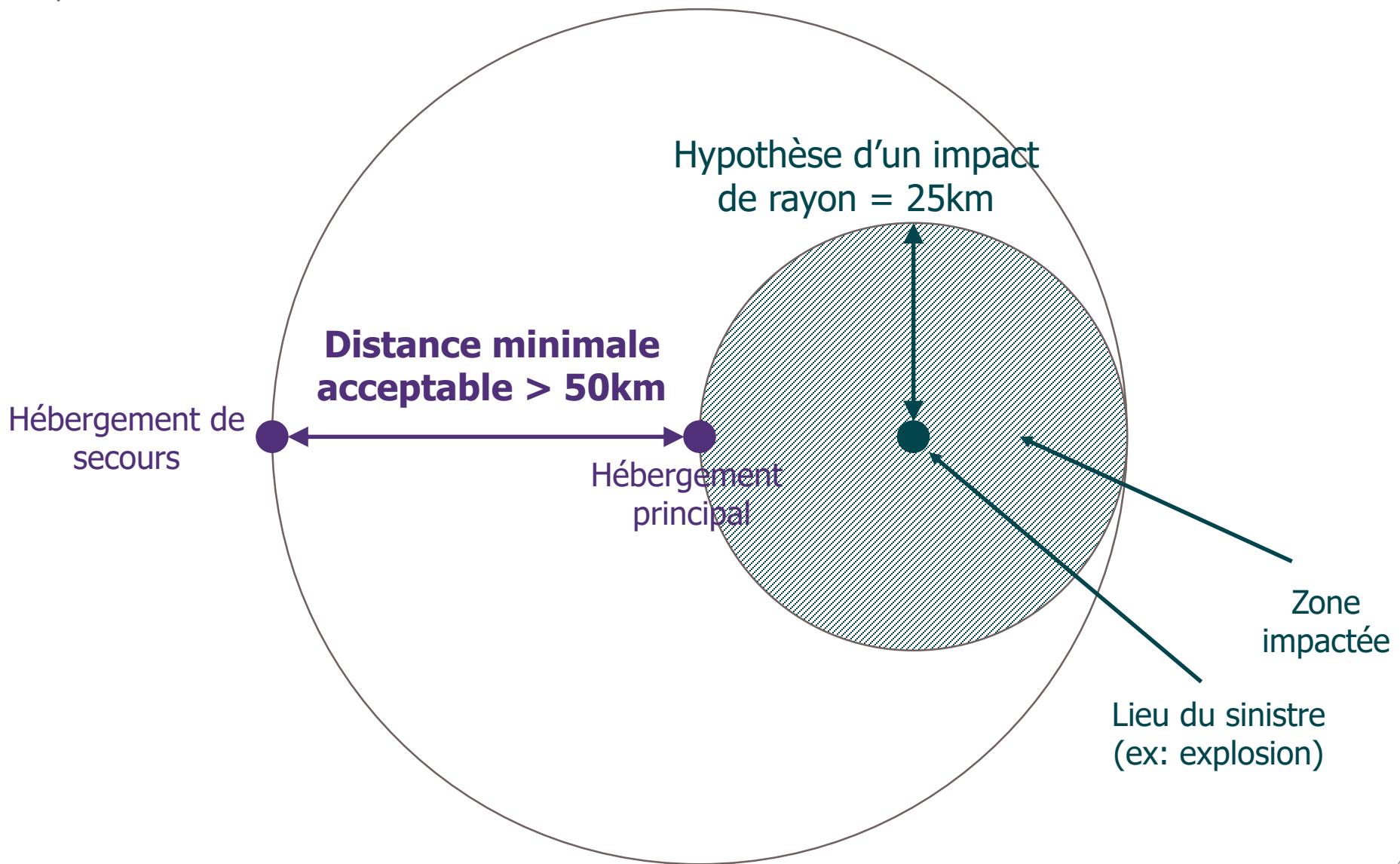
Exemple illustratif

## Risques extérieurs (ordres de grandeur illustratifs à recontextualiser au cas par cas)



## Stratégie d'hébergement : couverture du risque (2/2)

Exemple illustratif



# Stratégie de secours - A. Hébergement du secours

Limites de distances :

## Systèmes répartis complexes

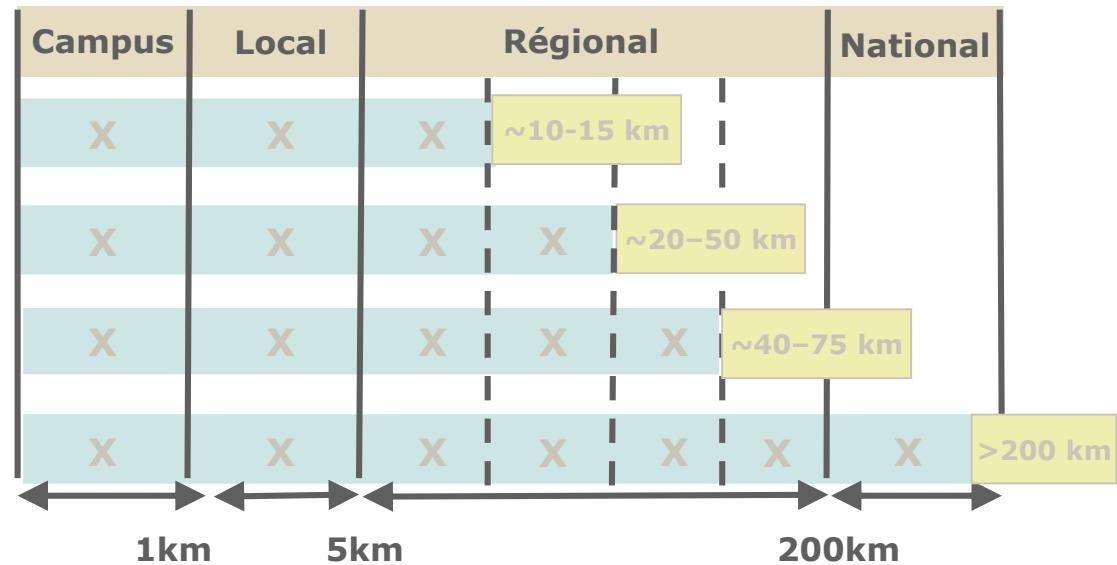
(clusters applicatifs : RAC, Sysplex)

## Systèmes répartis simples

(clusters système)

## RéPLICATION de données synchrone

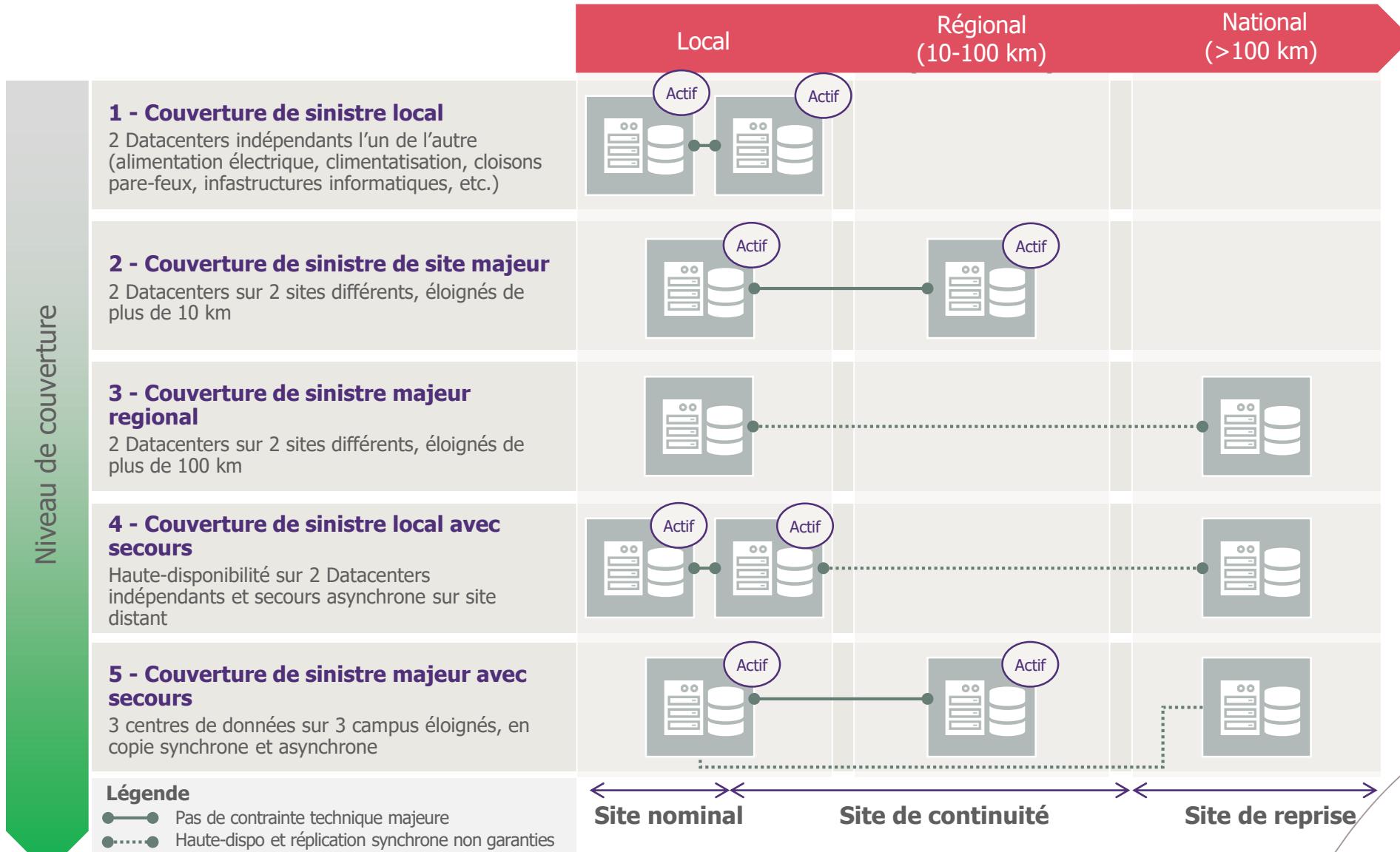
## RéPLICATION de données asynchrone



- / Les solutions de Haute Disponibilité s'appliquent principalement sur des distances courtes
  - › La distance maximale de faisabilité est variable d'une architecture à une autre
  - › Il est généralement nécessaire de tester les temps de réponse (impactés par la latence du réseau)
- / Pour une distance plus importante, les solutions de reprise rapide constituent la solution optimale
  - › Ex : solution de secours à chaud, basée sur une réPLICATION « seulement » asynchrone
- / Les solutions de Haute Disponibilité ne fournissent aucune protection contre la corruption logique
  - › Il est recommandé de maintenir en parallèle une solution complémentaire (potentiellement locale), basée sur des sauvegardes moins fréquentes

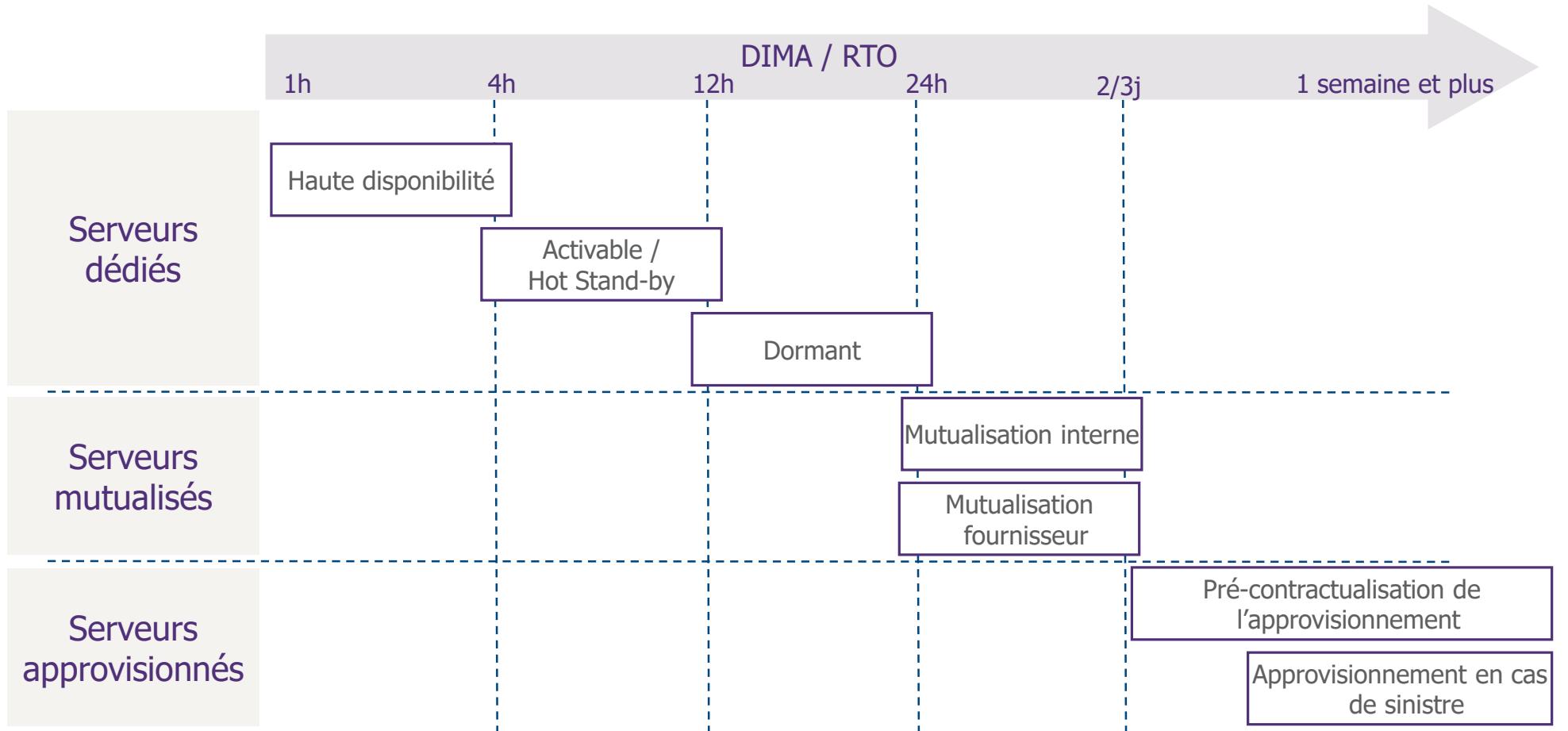
# A. Hébergement du secours

## Adapter l'hébergement du secours à la couverture de sinistre souhaitée



## B. Secours des serveurs

Adapter le secours des serveurs aux délais de reprise souhaités (DIMA / RTO)



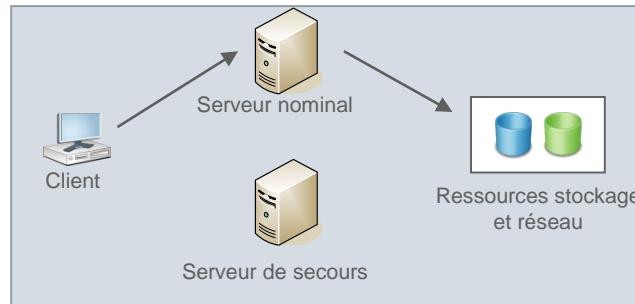
## B. Secours des serveurs : solutions de haute-disponibilité

### Solution de redondance

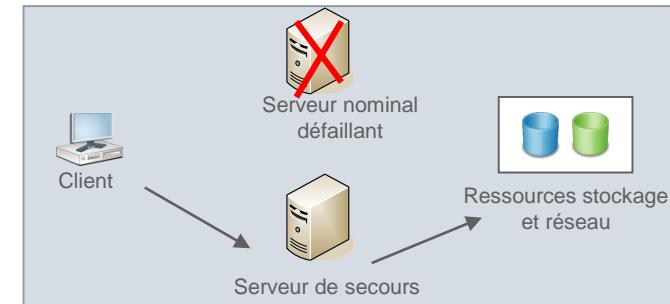
**Cluster système** : Une machine reprend les services d'une autre, défaillante, en se réappropriant ses ressources

- / Ex : cluster HACMP, cluster SUN HA, cluster MSCS, Sysplex IBM

#### Régime normal

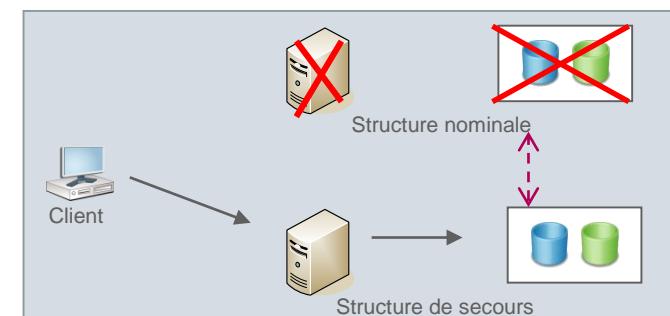
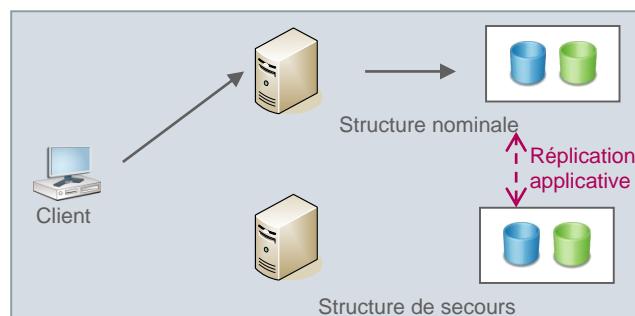


#### Régime de secours



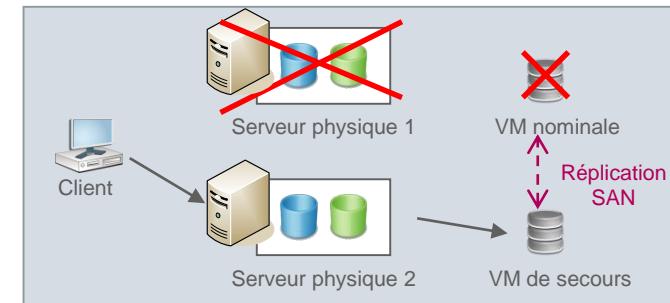
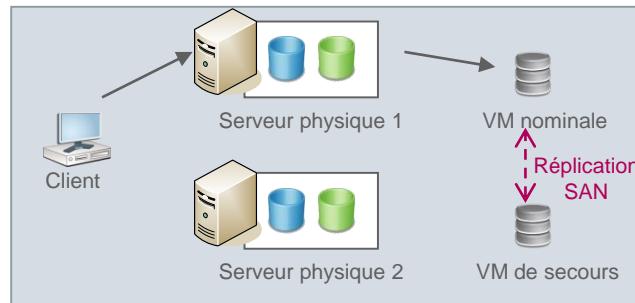
**Cluster applicatif** : Solution assurant la réplication des fonctions et/ou données pour assurer une redondance entre plusieurs machines

- / Ex. : Cluster WebSphere, Oracle RAC, Mirroring SQL Server



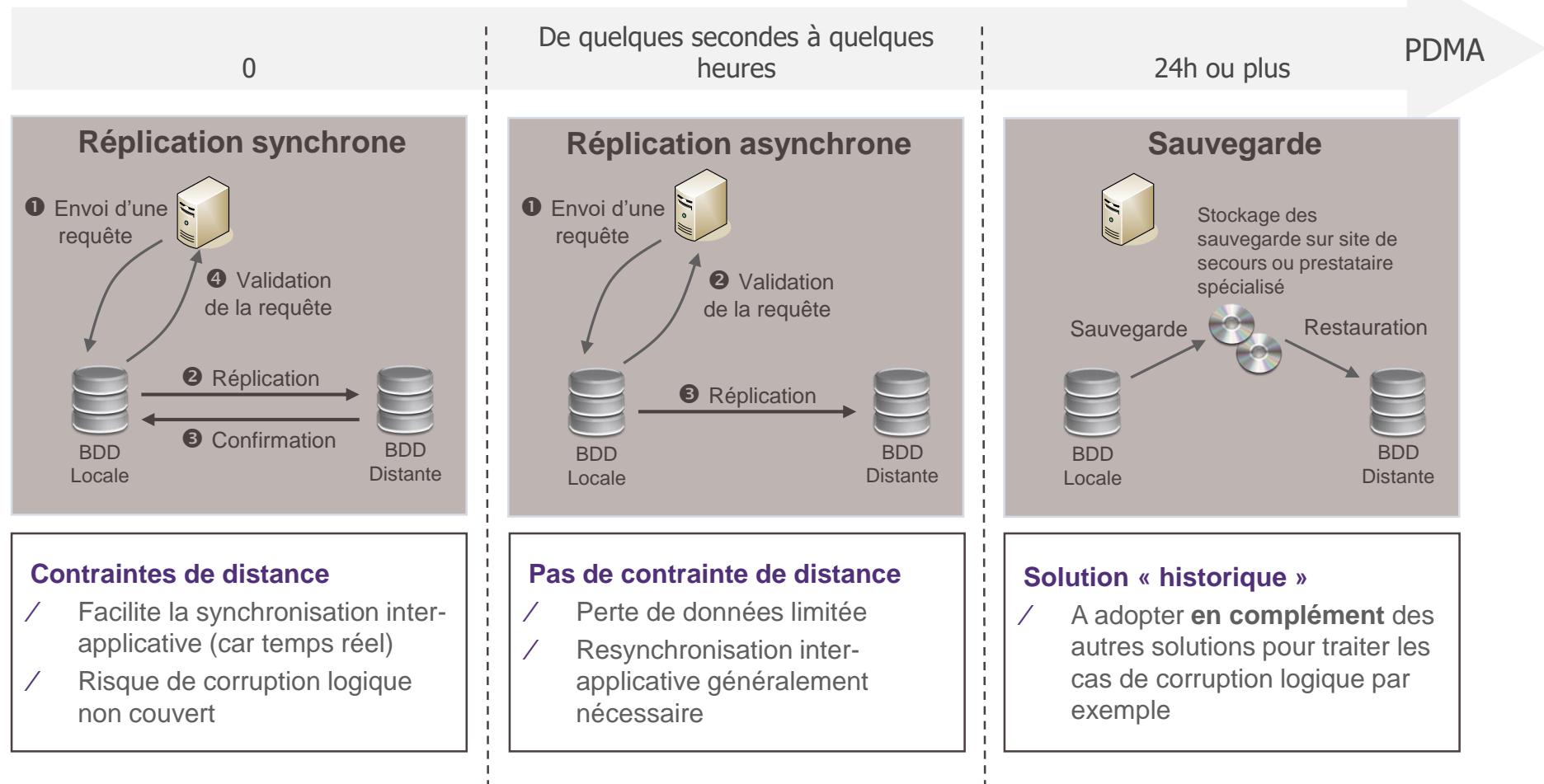
**Solutions de virtualisation** : Le secours est assuré en répliquant (via les mécanismes des baies SAN) la machine virtuelle (applications + données), qui peut être utilisée pour redémarrer en cas d'incident

- / Ex. : VMware



## B. Secours des serveurs : secours des données

Adapter le secours des données à la perte de données tolérée (PDMA, RPO)



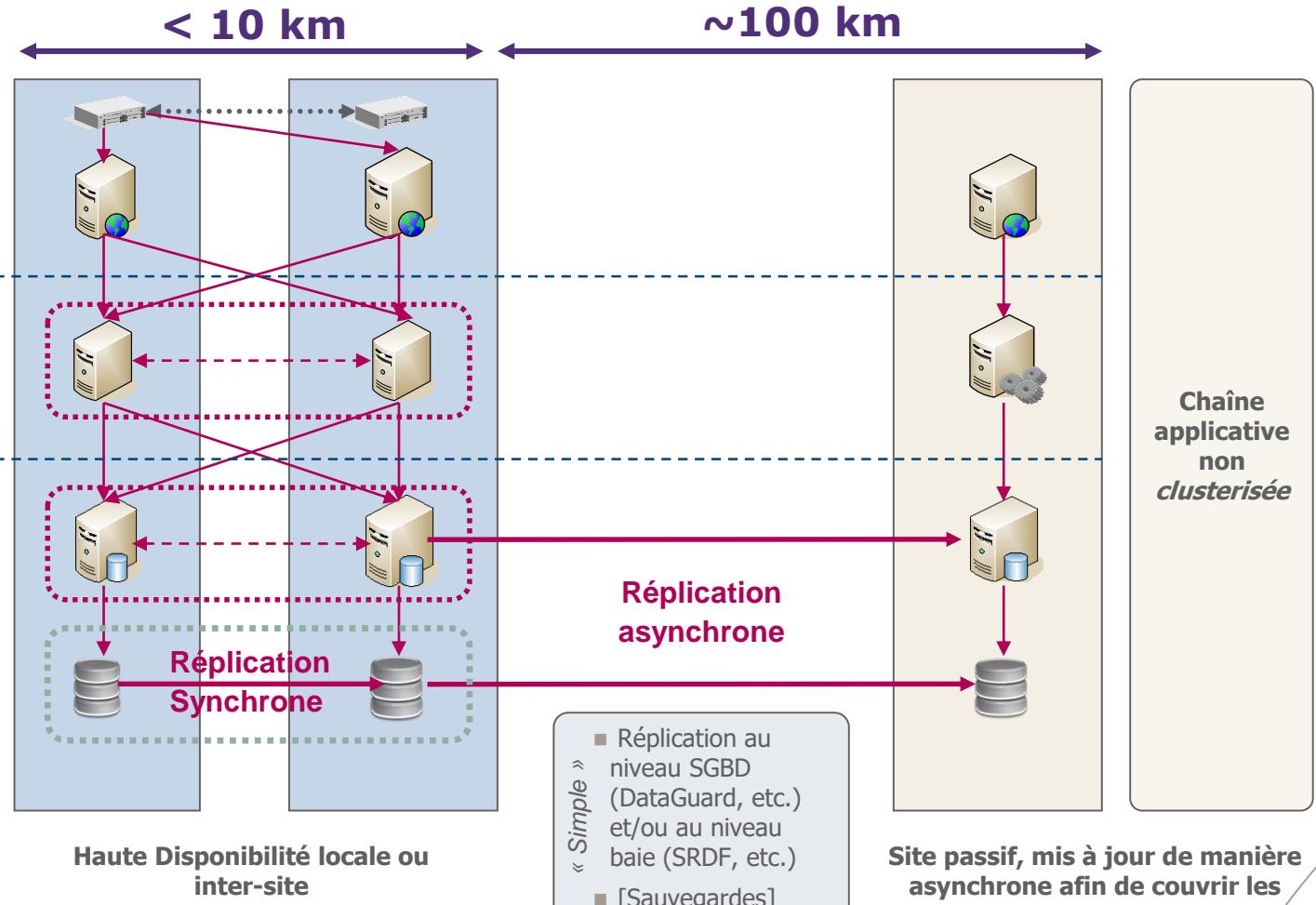
# Vision consolidée des différentes solutions suivant les besoins Métier (DIMA/PDMA)

		DIMA RTO	< 1h	1 à 4h	4 à 12h	12 à 48h	> 48h	> 1 semaine
PDMA RPO		Secours en haute-disponibilité		Secours activable	Secours dormant	Secours mutualisé	Secours approvisionné	
< Quelques secondes	Réplication Synchrone	Haute-disponibilité distante Synchrone		Ressources dédiées activables Synchrone	Ressources dédiées dormantes Synchrone	Ressources mutualisées Synchrone	Ressources approvisionnées Synchrone	
< Quelques heures	Réplication Asynchrone	Haute-disponibilité distante Asynchrone		Ressources dédiées activables Asynchrone	Ressources dédiées dormantes Asynchrone	Ressources mutualisées Asynchrone	Ressources approvisionnées Asynchrone	
< 1 journée	Sauvegarde			Ressources dédiées activables Sauvegardes	Ressources dédiées dormantes Sauvegardes	Ressources mutualisées Sauvegardes	Ressources approvisionnées Sauvegardes	
> 1 journée				Ressources dédiées activables Sauvegardes	Ressources dédiées dormantes Sauvegardes	Ressources mutualisées Sauvegardes	Ressources approvisionnées Sauvegardes	

# Exemple d'architecture pour une application 3-tiers

La continuité de fonctionnement et la reprise d'activité mettent en jeux des **solutions techniques différentes** en raison des **contraintes de distance** et des **types d'incident à couvrir**

Impact de la distance sur les solutions techniques



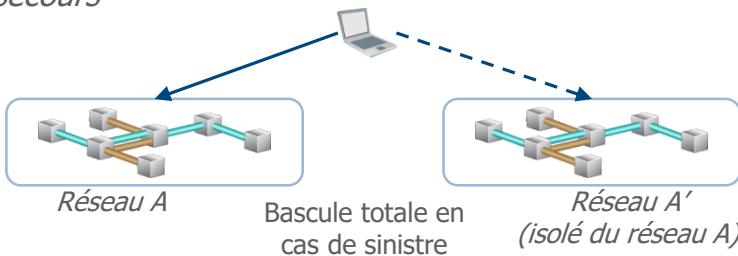
**Site passif, mis à jour de manière asynchrone afin de couvrir les cas de corruption logique**

## C. Stratégie d'activation

### Adapter l'interconnexion des sites au mode d'activation souhaité

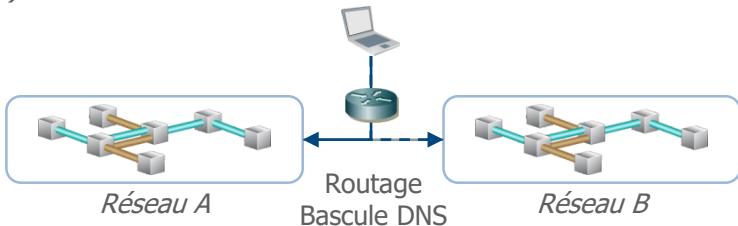
#### Stratégie « Reprise d'activité »

*Reproduction à l'identique du réseau sur le site de secours*

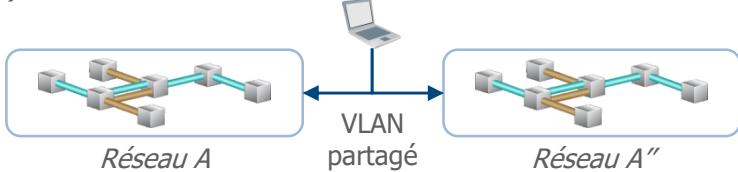


#### Stratégie « Continuité de fonctionnement »

##### 1) Réseaux distincts

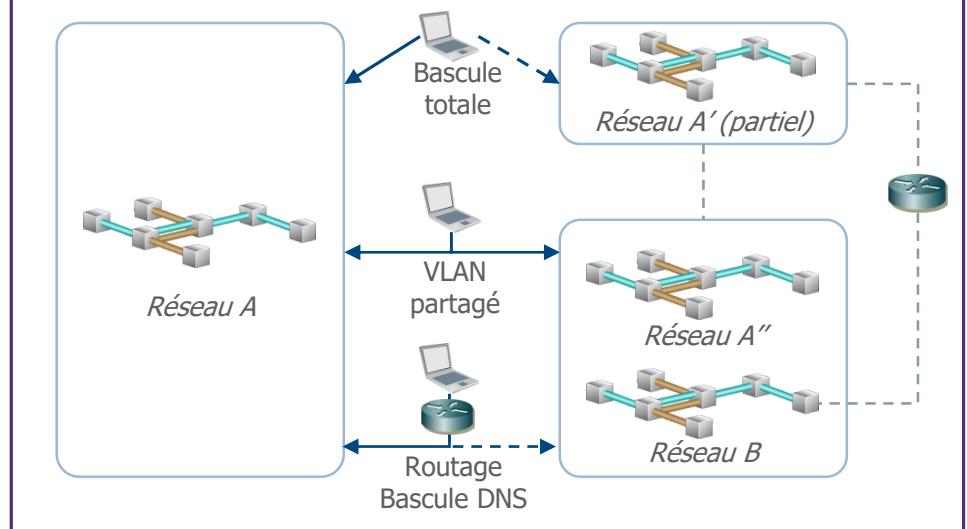


##### 2) « Datacenter virtuel »



#### Stratégie mixte

*Association des différents types d'interconnexion en fonction des solutions de secours retenues*



## C. Stratégie d'activation

Plusieurs stratégies d'activation, correspondant à des architectures réseaux différentes, sont envisageables :

### Activation « tout ou rien »

Réseau de secours identique et isolé du réseau nominal, possédant un plan d'adressage identique. L'activation du secours se fait par **bascule IP** : configuration des routeurs, pour rediriger les flux vers le réseau de secours (possédant la même adresse IP que le réseau nominal).

Le secours ne peut être activé de façon modulaire. Cette solution est la **solution historique** des plans de reprises informatiques

### Activation « modulaire »

2 typologies de solutions :

- 1) Le réseau de secours et le réseau nominal sont distincts l'un de l'autre. L'activation du secours se fait par **bascule DNS** : configuration des serveurs DNS pour rediriger les flux vers les adresses IP des machines de secours
- 2) Le réseau de secours et le réseau nominal sont sur des **VLAN partagés** (« datacenter virtuel ») entre les deux salles. Cette solution permet notamment l'implémentation de clusters.

Ces 2 typologies de solution permet une activation modulaire du secours

### Combinaison de solutions

La combinaison des solutions précédentes permet d'adapter le type d'activation du secours aux besoins exprimés par les métiers et à l'existant informatique

# Agenda

1. Introduction à la continuité d'activité
- 2. Plans de Continuité Informatique
  - 2. 1 *Eléments constitutifs*
  - 2. 2 *Tendances*
  - 2. 3 *Exemple de mission PCI*
3. Plans de Continuité des Opérations
4. Gestion des incidents et des crises

# Des enjeux de disponibilité et continuité de plus en plus importants...

**Transformation numérique** des métiers engendre une **augmentation de la valeur ajoutée** portée par le **SI**



**Interdépendance des SI** croissante avec une complexité toujours importante



**Pression réglementaire** continue  
(Banque, assurance, OIV...)



**Une volonté du métier d'avoir un SI « always on »**

# ...auxquels on répond partiellement...

La consolidation et sécurisation de l'hébergement, depuis 15 ans, a permis de **diminuer la probabilité** des sinistres (meilleure couverture des incidents locaux) ...

...mais a **augmenté leurs impacts** (périmètre impacté plus important)

Type de risques		Exemples de solutions	Localisation	Adoption
<b>Incident local</b> <i>Panne serveur, erreur de manipulation...</i>	Domaine de la disponibilité de services	<ul style="list-style-type: none"> <li>/ Redondance (cluster, répartition de charge...)</li> <li>/ Équipements de rechange</li> <li>/ Contrats de maintenance</li> </ul>	Locales	
<b>Sinistre de site</b> <i>Incendie, panne électrique...</i>	Domaine de la continuité de services	<ul style="list-style-type: none"> <li>/ Haute disponibilité inter-sites</li> <li>/ RéPLICATION synchrone</li> </ul>	2 à 30km	
<b>Sinistre régional</b> <i>Inondation, tempête...</i>		<ul style="list-style-type: none"> <li>/ Moyens de reprise dédiés ou mutualisés</li> <li>/ RéPLICATION asynchrone</li> </ul>	>100k m	

# ... et imparfaitement...

Type de risques	Adoption	Efficacité	
<b>Incident local</b> <i>Panne serveur, erreur de manipulation...</i>			<ul style="list-style-type: none"> <li>/ Problématique du quotidien de la production ...</li> <li>/ ... mais des incidents encore trop fréquents pour les métiers</li> </ul>
<b>Sinistre de site</b> <i>Incendie, panne électrique...</i>			<ul style="list-style-type: none"> <li>/ Une vision insuffisamment métier : absence de vision bout en bout des processus métier</li> <li>/ Une multiplicité des solutions techniques difficiles à maintenir et maîtriser</li> <li>/ Une orientation infrastructure sans vision application</li> <li>/ Des tests sans résultat probant ne permettant pas d'augmenter le niveau de confiance</li> <li>/ Un coût perçu comme prohibitif</li> </ul>
<b>Sinistre régional</b> <i>Inondation, tempête...</i>			<ul style="list-style-type: none"> <li>/ Une vision insuffisamment métier : absence de vision bout en bout des processus métier</li> <li>/ Une multiplicité des solutions techniques difficiles à maintenir et maîtriser</li> <li>/ Une orientation infrastructure sans vision application</li> <li>/ Des tests sans résultat probant ne permettant pas d'augmenter le niveau de confiance</li> <li>/ Un coût perçu comme prohibitif</li> </ul>

**Une adoption et une efficacité des solutions proportionnelles aux incidents passés**

... qui nécessitent une transformation de la production,  
pour construire un PCI plus efficace

Un impératif pour la DSI...

...pour répondre aux enjeux  
de la Direction Générale

1

## Industrialiser et être agile

- / Étendre la couverture de risques
- / Rationaliser et industrialiser les solutions

2

## Avoir enfin confiance...

- / Réaliser régulièrement des tests probants
- / Assurer une vision Métier cohérente

3

## ... tout en réduisant les coûts

- / Optimiser l'utilisation du secours
- / Limiter les coûts de licences

# Le cloud public: une nouvelle tendance en matière d'hébergement



- / Le cloud public est une infrastructure partagée, ouverte à tous
- / 3 principaux types de services s'appuient sur ce type d'infrastructure



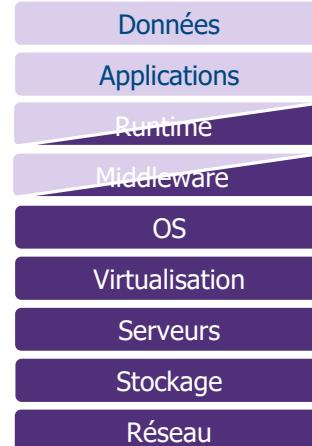
## SaaS *Software as a Service*

Fournit à l'utilisateur des interfaces d'applications Web, mobiles ou bureau via internet



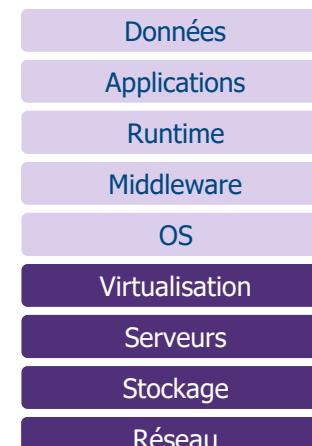
## PaaS *Platform as a Service*

Fournit via Internet des environnements de développement et de déploiement pour les services applicatifs



## IaaS *Infrastructure as a Service*

Fournit des ressources informatiques pour les équipes SI



Office 365



Et bien d'autres !



Microsoft Azure  
Google Cloud Platform

# Le secours du SaaS : le fournisseur choisit, ou non, de l'inclure



## Le secours est inclus

Chez les acteurs leaders (Office 365) et certains acteurs de taille intermédiaire (Evernote) :

- / Le fournisseur dispose d'un site secondaire
- / Une sauvegarde est mise en place (éventuellement via une option payante)

## 3 tendances se dégagent



## Sauvegarde mais pas de plan de secours

Chez certains acteurs de taille intermédiaire (Zervant, Sellsy ...) :

- / Sauvegardes régulières et sur plusieurs sites distants des données
- / Elles peuvent servir pour le secours mais ce processus n'est pas explicitement abordé



## Aucune prise en charge d'un moyen de secours

Chez les acteurs de taille modeste (Winflotte, Pro-Artis ...) :

- / Pas de sauvegarde
- / Pas de plan de secours ni de possibilité d'y souscrire via une option

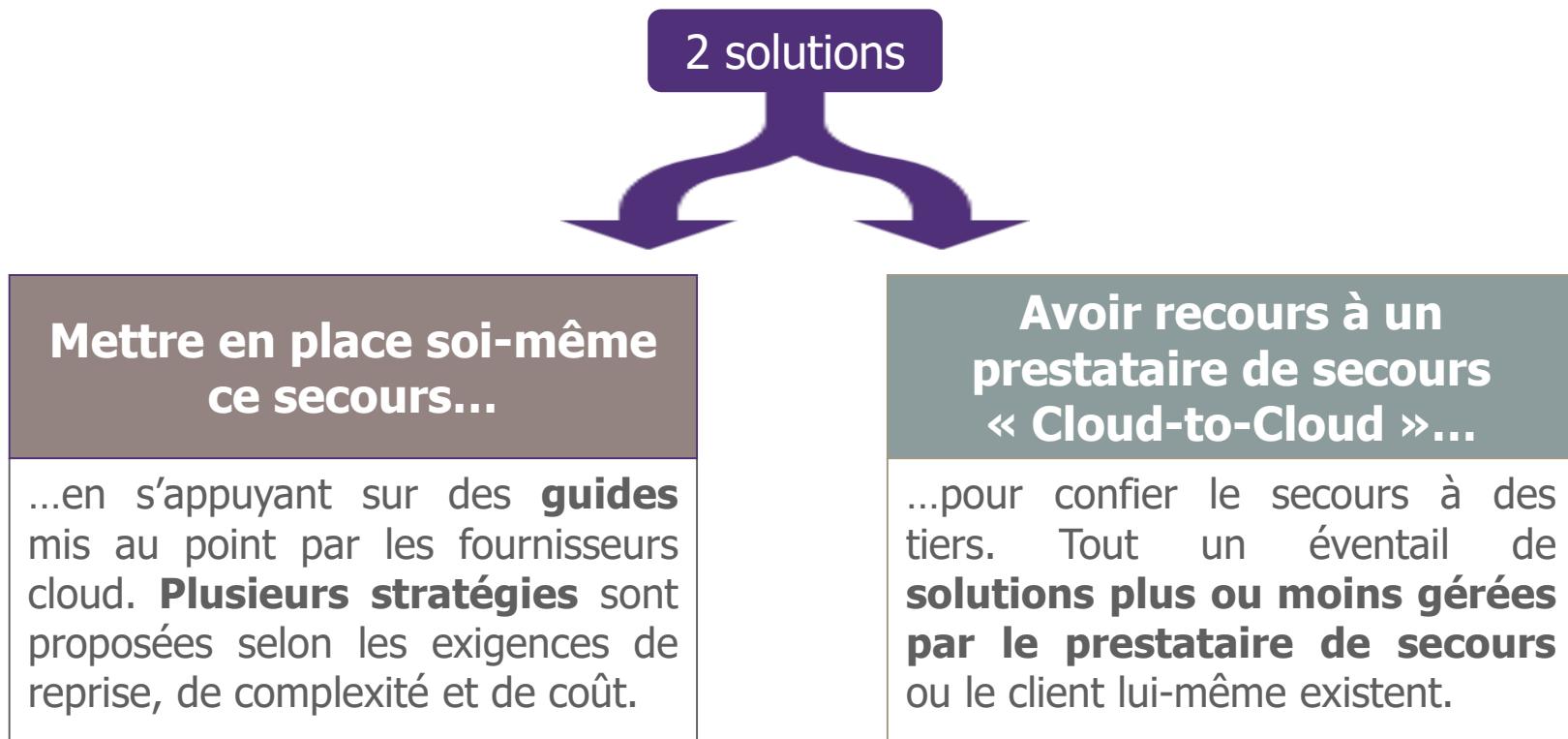


Il est important d'**étudier et négocier les garanties du contrat** en terme de secours.

# Le secours du IaaS/PaaS : plus de marge de manœuvre pour le client

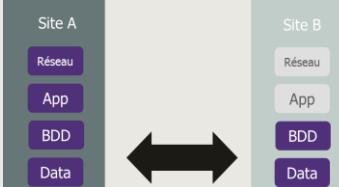
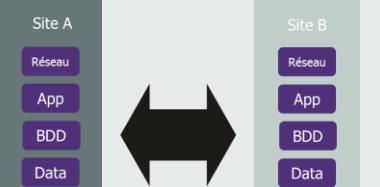
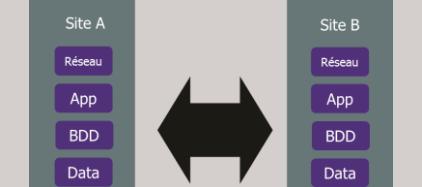
**Le secours n'est pas pris en charge** par les fournisseurs cloud.

Les **mêmes choix que pour le secours de site traditionnel** s'offrent à l'utilisateur.



Azure prévoit de proposer une option, courant 2017, pour assurer le secours des machines virtuelles hébergées chez eux.

# Détails des principales stratégies de secours par le client

	Sauvegarde et Restauration	Veilleuse	Secours à chaud	Multi-site
Concept	 <p>Elle consiste en une simple copie des données vers une autre région du cloud.</p>	 <p>Seul le <b>noyau critique</b> de fonctionnement du système (BDD) tourne en permanence.</p>	 <p>La <b>version minimale d'un environnement fonctionnel s'exécute en permanence</b> dans le cloud.</p>	 <p><b>2 sites identiques</b> traitent chacun la moitié des requêtes. Les données des 2 sites sont entièrement répliquées.</p>

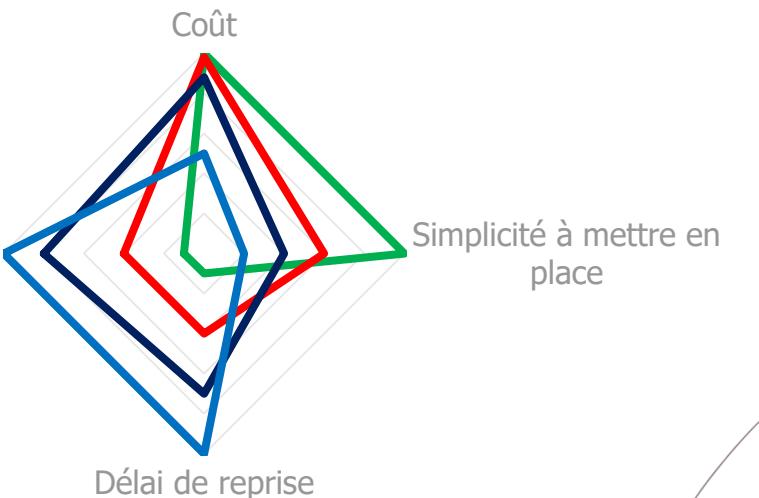
## Critères de comparaison

- / **Coût** : Tient compte du coût de mise en place de la solution et de l'utilisation de celle-ci
- / **Simplicité** : La nuance est faite entre la mise en place de la solution et son déploiement
- / **Délai de reprise** : Temps nécessaire à la reprise après sinistre
- i** La perte de données n'est pas un critère différenciant car elle dépend du système de réPLICATION.

## Comparaison des solutions

- Sauvegarde/Restauration
- Veilleuse
- Secours à Chaud
- Multi-site

Simplicité à déployer en cas de sinistre



# Agenda

1. Introduction à la continuité d'activité
- 2. Plans de Continuité Informatique
  - 2. 1 *Eléments constitutifs*
  - 2. 2 *Tendances*
  - 2. 3 *Exemple de mission PCI*
3. Plans de Continuité des Opérations
4. Gestion des incidents et des crises

# Contexte et objectifs

## Contexte

Augmentation continue de la criticité du SI d'une institution.

Fusion de deux organismes et évolution des applications informatiques



## Objectifs

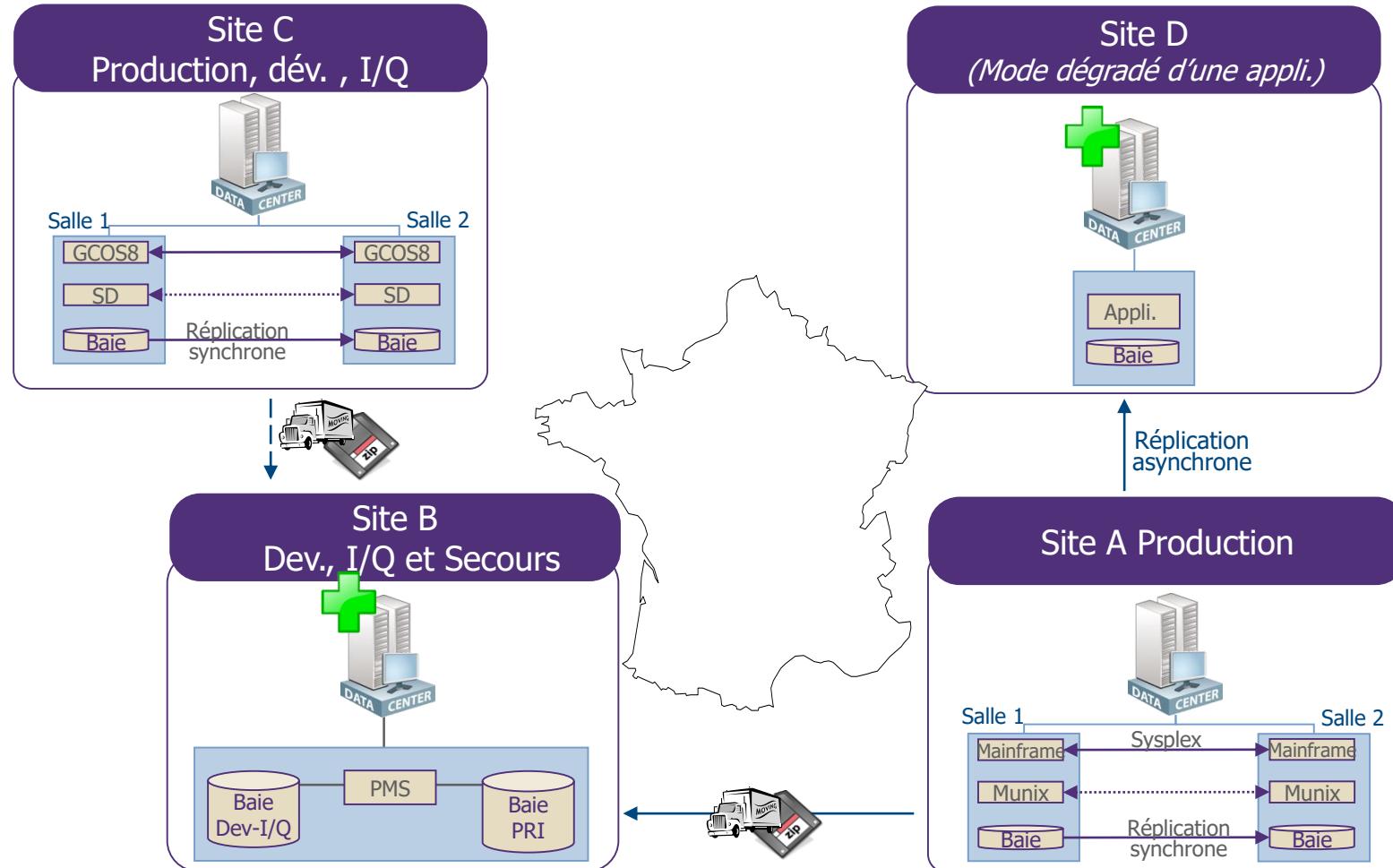
Besoin de redéfinir une politique de secours adaptée au nouveau contexte

A. Une couverture de risques appropriée

B. Un périmètre secouru répondant aux besoins Métiers

C. Des moyens de secours adaptés aux enjeux

# Le secours informatique existant

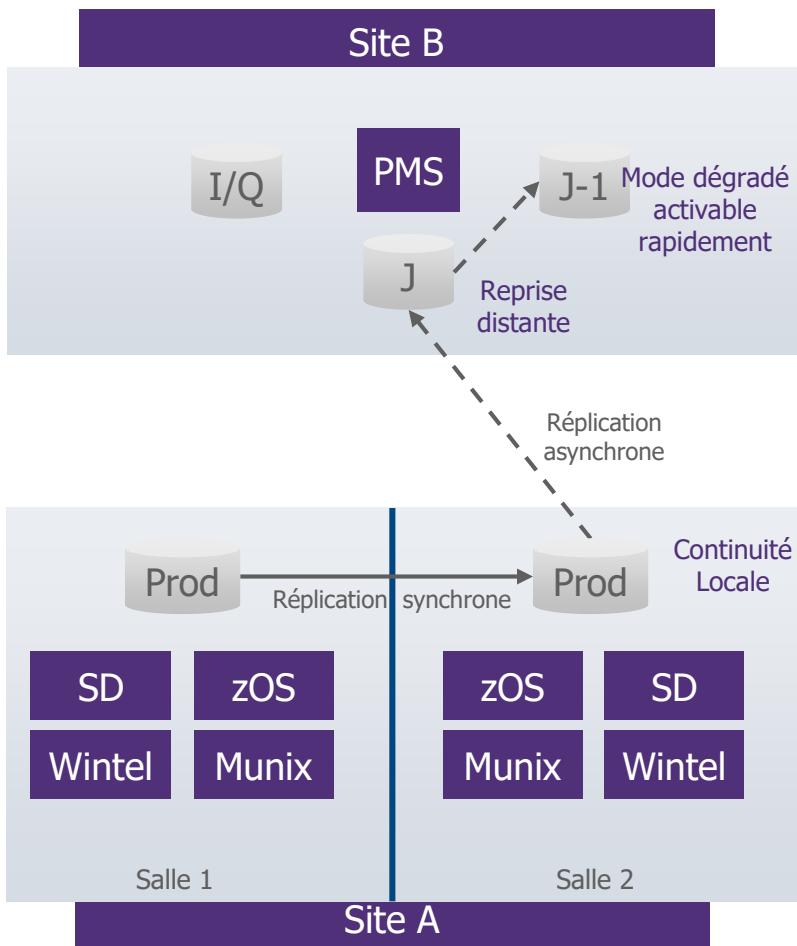


NB :  
Il existe par ailleurs des applications hébergées sur des sites complémentaires

3 types de solutions de secours : **continuité locale entre salles** (sur les sites A et C), **reprise distante** du site A (sur site B) et **mode dégradé d'accès à des données** (sur site D)

# Scénario proposé à court-moyen terme : « Secours interne »

Un « bi-site » éloigné avec le 2<sup>nd</sup> site hébergeant les infrastructures de reprise distante et mode dégradé



Scénario A - Secours interne		
Délais d'activation du secours	+	Activation reprise distante sous 2 jours Solution dégradée sous qq heures
Couverture de risques	+	Risque social DSI non couvert
MCO et tests	+	Une adhérence aux plateformes I/Q mais une autonomie de PE dans la mobilisation des ressources
Durée de mise en œuvre	-	Intégration du site C dépendante de la sortie de GCOS, de la désimbrication prod / IQ et du plan de déménagement
Facilité de mise en œuvre Continuité et Reprise	=	Des socles déjà existants à industrialiser et étendre
Facilité de mise en œuvre du mode dégradé	-	Une solution à construire
Acceptabilité sociale	++	Maintien du site de développement et I/Q existant
Optimisation des infrastructures	+	Mutualisation sur la PMS (Reprise distante, Mode dégradé)
Coûts (Restant à valider)	€	Mutualisation maximale de la PMS

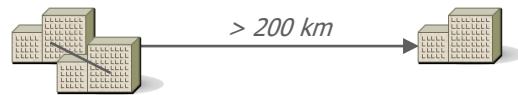
# Scénario d'évolution proposé à moyen-long terme

2017

2020 - 2021

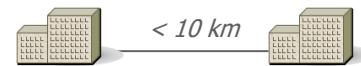


## Scénario « Secours interne »



Site interne : continuité locale sur deux salles      Site interne : reprise distante, mode dégradé, développement et I/Q

## Scénario « Trois sites »



Site interne : production      Nouveau site interne : Production et Continuité locale



Site interne : Développement, I/Q, reprise distante, et mode dégradé

Une 1<sup>ère</sup> étape permettant de répondre rapidement au besoin de consolidation du secours...

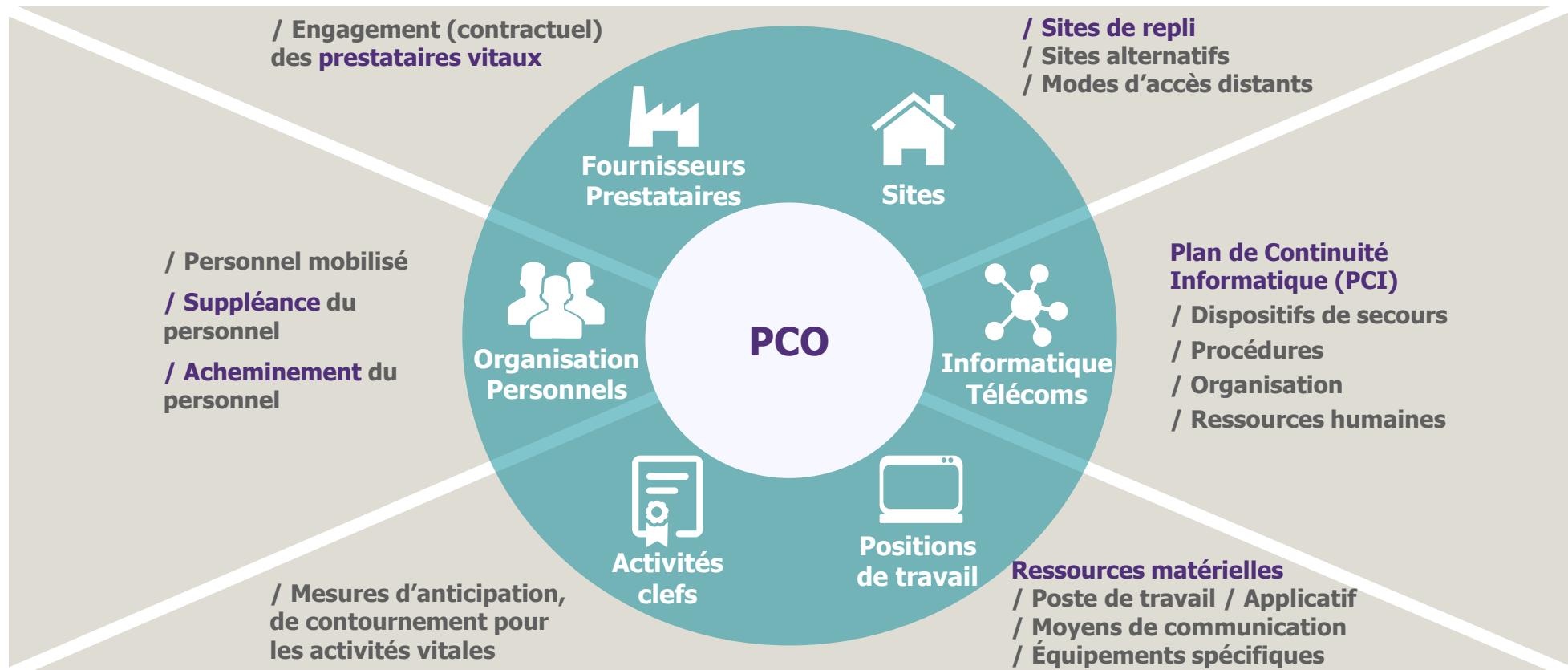
... et qui pourra évoluer vers une stratégie 3 sites dans le cadre d'une extension du site A par la construction d'un nouveau site

# Agenda

1. Introduction à la continuité d'activité
2. Plans de Continuité Informatique
- 3. Plans de Continuité des Opérations
  - 3. 1 *Eléments constitutifs*
  - 3. 2 *Tendances*
  - 3. 3 *Exemple de mission PCO*
4. Gestion des incidents et des crises

# Rappel : les différentes composantes d'un PCA

## Organisation de crise (Cellules de crise, moyens, procédures, ...)



## Coordination / Maintenance du PCA (Responsables, correspondants, ...)

# Objectifs et cas de sinistres traités

**Le Plan de Continuité des Opérations vise à poursuivre les activités critiques de l'entreprise (éventuellement en mode dégradé) en cas d'indisponibilité de ressources dont elles ont besoin.**

Afin de limiter les coûts en mutualisant les solutions, les entreprises raisonnent souvent sur la nature de l'impact plutôt que sur la menace.

4 grands types d'impacts sont généralement considérés :



Indisponibilité du système d'information



Indisponibilité d'un site hébergeant du personnel



Indisponibilité de collaborateurs



Indisponibilité des prestataires critiques

# Indisponibilité du SI : travailler en mode dégradé



- › Lister les activités métier qui sont **vitales** et pour lesquelles des solutions palliatives à l'absence de SI seront mises en place



- › Formaliser des solutions de secours pour assurer la **continuité métier** durant la crise



- › Identifier les prérequis techniques/organisationnels à **mettre en place de manière anticipée** pour assurer le bon fonctionnement des solutions de secours en cas de crise

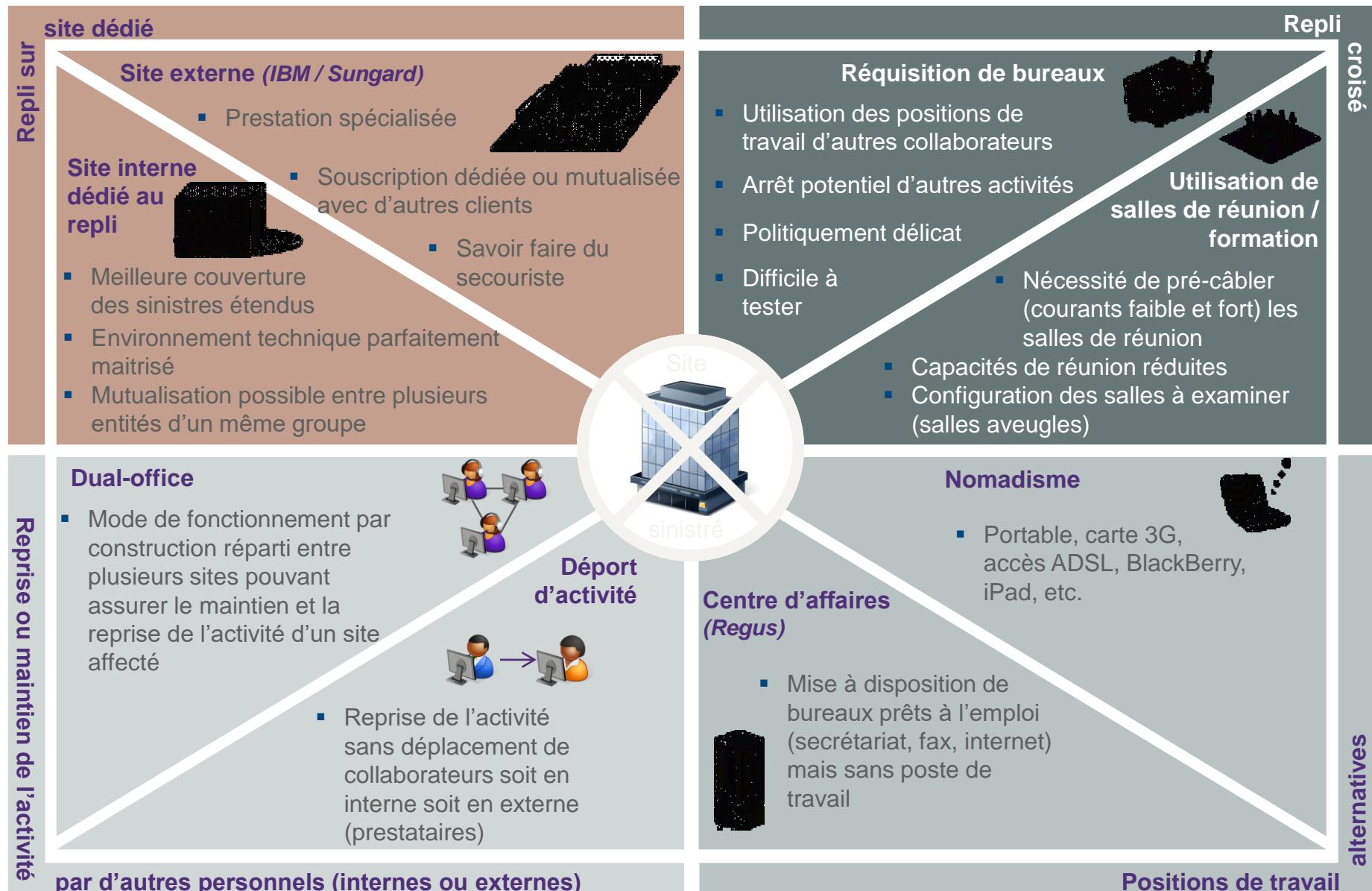


- › **Tester et mettre à jour régulièrement** les solutions de secours de chaque activité vitale

La capacité de pouvoir travailler en mode dégradé en l'absence de SI dépend des activités métiers (paie, vente, logistique, ...).

Les solutions palliatives peuvent être entièrement manuelles, nécessiter un minimum de moyens bureautique (ex : un ordinateur connecté à Internet), voire nécessiter l'accès à des données métiers régulièrement stockées dans le Cloud (ex : commandes passées la veille).

# Indisponibilité de site : des solutions multiples



# Mise à disposition des postes de travail - Différentes stratégies possibles

Coût

Stocks de postes dédiés au secours et installés sur les sites de repli

Stocks de postes mutualisés et « installés de façon générique »

Stocks de postes mutualisés à installer et fournir au moment du sinistre

Équipement de collaborateurs en nomadisme de façon nominale

Approvisionnement de matériel à installer

Réquisition de matériel sur d'autres activités



## Avantages

Déclenchement rapide. Pas de perturbation du fonctionnement nominal des collaborateurs.

MCO\* facilité et diminution des coûts via la mutualisation.

Mutualisable entre les différentes activités sinistrées.

Déclenchement rapide. Permet de mutualiser avec le traitement de la pandémie.

Pas de coûts récurrents.

Coûts récurrents et de déclenchement faibles.



## Inconvénients

MCO\* complexe. Très coûteux.

Forte diminution du niveau de sécurité.

Gestion des configurations complexe mais indispensable pour un déclenchement rapide.

Nécessite que les collaborateurs ramènent leur PC à domicile le soir afin de couvrir le maximum de scénarios de sinistre.

Ne convient pas pour des délais de reprise exigeants.

Risques de tension avec les collaborateurs réquisitionnés. Long à déployer si l'on ne veut pas diminuer le niveau de sécurité.



Combiner les solutions de mise à disposition en fonction des délais de reprise et des coûts

# Indisponibilité de collaborateurs

## Quelques solutions pour le scénario le plus couramment envisagé : la pandémie

En amont

Au moment de la crise



**Amélioration de la polyvalence des équipes** (formation des collaborateurs, formalisation des processus de fonctionnement critiques, ...)



**Définition du plan de continuité pandémie grippale**



**Préparation des solutions de travail à distance** (augmentation des stocks de roulement de PC, préparation et test des kits de connexion à distance, ...)



**Mise en place de mesures sanitaires renforcées** (nettoyage des locaux plus fréquents, distribution de masques, consignes sanitaires aux collaborateurs, fermeture des RIE, ...)



**Restriction des accès aux sites** (selon l'ampleur de la crise, restriction des accès uniquement aux collaborateurs internes à l'entreprise, puis uniquement aux contributeurs d'activités critiques devant exercer sur site)



**Recours à l'intérim** (pour le remplacement de collaborateurs malades ou s'occupant de proches, plutôt sur des postes peu qualifiés)



**Priorisation des activités** (focalisation des collaborateurs sur les activités critiques, pour pallier à l'absence de personnel ou aux mesures de restriction des accès aux sites)



**Gel des prestations de services non critiques** (arrêt des prestations externes non indispensables pour le bon fonctionnement de l'entreprise)



**Recours au télétravail** (pour éviter la propagation du virus sur les sites de l'entreprise et/ou pallier à une fermeture sanitaire ou des perturbations dans les transports)



**Adaptation des horaires de travail** (pour pallier aux perturbations dans les transports publics et permettre aux collaborateurs de prendre soin de proches malades)



**Limitation des déplacements** (limitation des déplacements entre plaques régionales pour éviter la propagation du virus entre sites)

# Indisponibilité de fournisseurs - Solutions les plus courantes

En amont

- / Intégration du critère de criticité des prestations dans la stratégie achats
  - > Intégration de clauses PCA dans les contrats avec les prestataires critiques
  - > Développement de bonnes relations avec les fournisseurs et prestataires en situation de quasi monopole et/ou difficiles à remplacer
  - > Sécurisation des prestations critiques via l'utilisation en situation nominale de deux prestataires
- / Internalisation de l'activité si le maintien de l'externalisation est jugé trop risqué

En cas de défaillance  
de prestataire

- / Si plusieurs prestataires en situation nominale, transfert de l'ensemble des tâches aux prestataires non-impactés
- / Changement de prestataire
- / Internalisation provisoire de l'activité

# Agenda

- 1. Introduction à la continuité d'activité
- 2. Plans de Continuité Informatique
- 3. Plans de Continuité des Opérations
  - 3. 1 *Eléments constitutifs*
  - 3. 2 *Tendances*
  - 3. 3 *Exemple de mission PCO*
- 4. Gestion des incidents et des crises

# De nouveaux usages et solutions qui impactent le PCO

**Impacts sur les stratégies de fourniture du matériel**



**BYOD**  
*(Bring Your Own Device)*

**Virtualisation du poste de travail**



**Extension des frontières de l'entreprise**

**Impacts sur les acteurs à impliquer**



**Cloud computing**

**Impact sur les modalités d'accès aux applications**

...

**Développement du télétravail**

**Impacts sur les modes de fonctionnement nominaux**

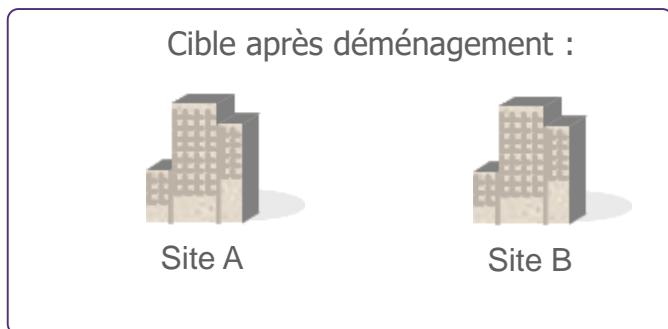


# Agenda

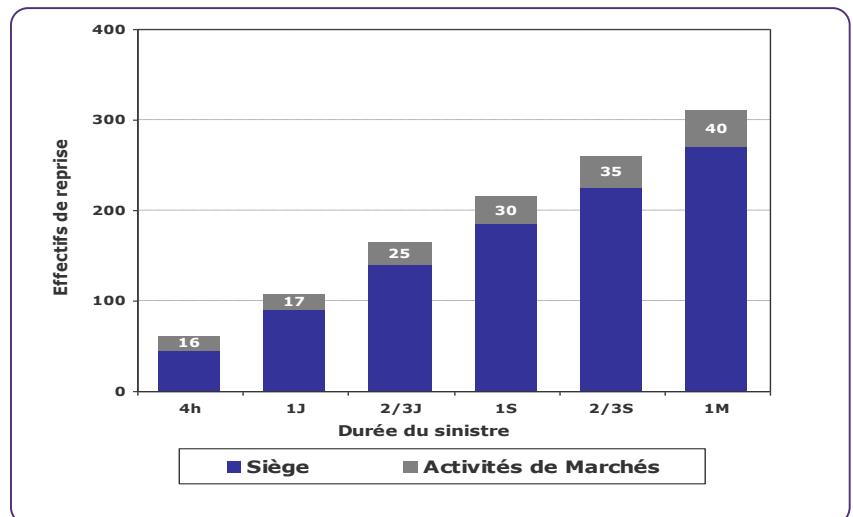
- 1. Introduction à la continuité d'activité
- 2. Plans de Continuité Informatique
- 3. Plans de Continuité des Opérations
  - 3. 1 Eléments constitutifs
  - 3. 2 Tendances
  - 3. 3 Exemple de mission PCO
- 4. Gestion des incidents et des crises

# Contexte et démarche

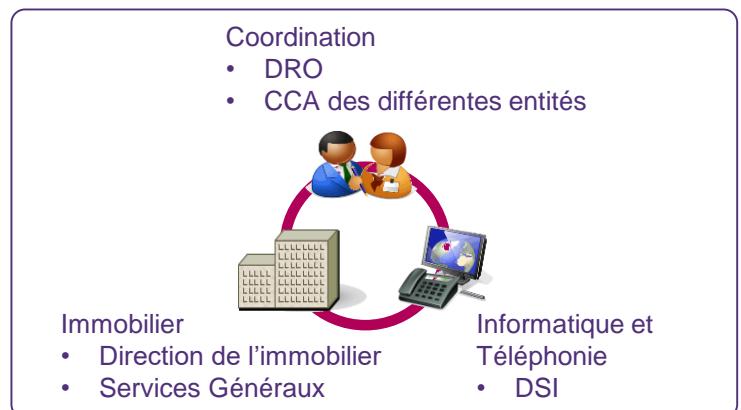
- / Une campagne BIA récente  
de 60 positions sous 4h à 300 positions à 1mois, toute activité confondue
- / 1 solution de repli historique chez un prestataire pour les activités de marché et la comptabilité
- / Aucun dispositif pour les effectifs du Siège



➔ Mise en place d'un GT « Stratégie de repli du Siège »



/ Un déménagement en préparation, à cible 2018



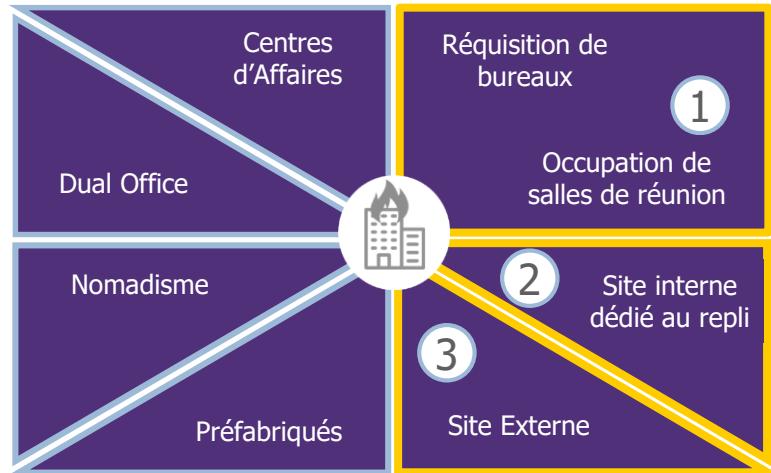
# Modules de repli à combiner

## 8 modules de repli à combiner pour créer une stratégie de repli adaptée



- / Des solutions à écarter dans le contexte :
  - > Nomadisme (règle de sécurité SI)
  - > Préfabriqués (pas de parking, peu de confort)
  
- / Des populations différentes → séparation de la population en 3 catégories :
  - > Les activités de marché
  - > Le Directoire
  - > Les activités de Siège

# Etude de 3 stratégies de repli pour les activités de Siège



## Cinq critères d'analyse :

- / Coûts d'investissement et récurrent
- / Couverture des risques
- / Réponse au besoin
- / Maintien en conditions opérationnelles
- / Mise en œuvre de la solution

1

### Repli Croisé entre Site A et Crossing

- / Indépendance des sites, notamment pour l'informatique locale
- / Salle de réunion aveugles
- / Ratio d'occupation des salles de réunion : 1/2
- / Répartition des activités critiques entre les sites, non homogène (90 et 160 effectifs à replier)
- / Câblage courant fort et faible des salles de réunion
- / Crue de Seine et double sinistre, Sèvres et Crossing, non couverts
- / Problématique de stock de PC et déploiement

Investissement      Récurrent

150 k€

&lt;50 k€/an

2

### Repli sur un site interne dédié au repli

- / Utilisation du patrimoine immobilier de XXX : Site C, 2 500 m<sup>2</sup> vacants (ou presque)
- / Site de repli « Groupe XXX »
- / Centres / agences, Filiales
- / Mutualisation avec la Formation (site actif)
- / Accès au site et capacité hôtelière
- / Coût d'investissement et récurrent important
- / Problématique de stock de PC et déploiement

Avec la formation :

2,3 M€

700 k€/an

Sans la formation :

1,8 M€

650 k€/an

+ travaux propriétaires :  
1,5 M€

3

### Repli chez un prestataire

- / Sinistres de place non couverts
- / Taux de mutualisation à 15

~100 k€

200 k€/an

# Agenda

- 1. Introduction à la continuité d'activité
- 2. Plans de Continuité Informatique
- 3. Plans de Continuité des Opérations
- ▶ 4. Gestion des incidents et des crises
  - 4.1 La théorie
  - 4.2 Exemple d'exercice de crise

# Qu'est-ce qu'une crise ?

## Une crise est ...

- / Une situation **soudaine**, souvent **brutale, inattendue**, aux **conséquences** potentiellement **très graves** pour l'entreprise et pour laquelle les **mécanismes** et réactions **habituels** sont **inadaptés**

## Ses origines sont extrêmement variées

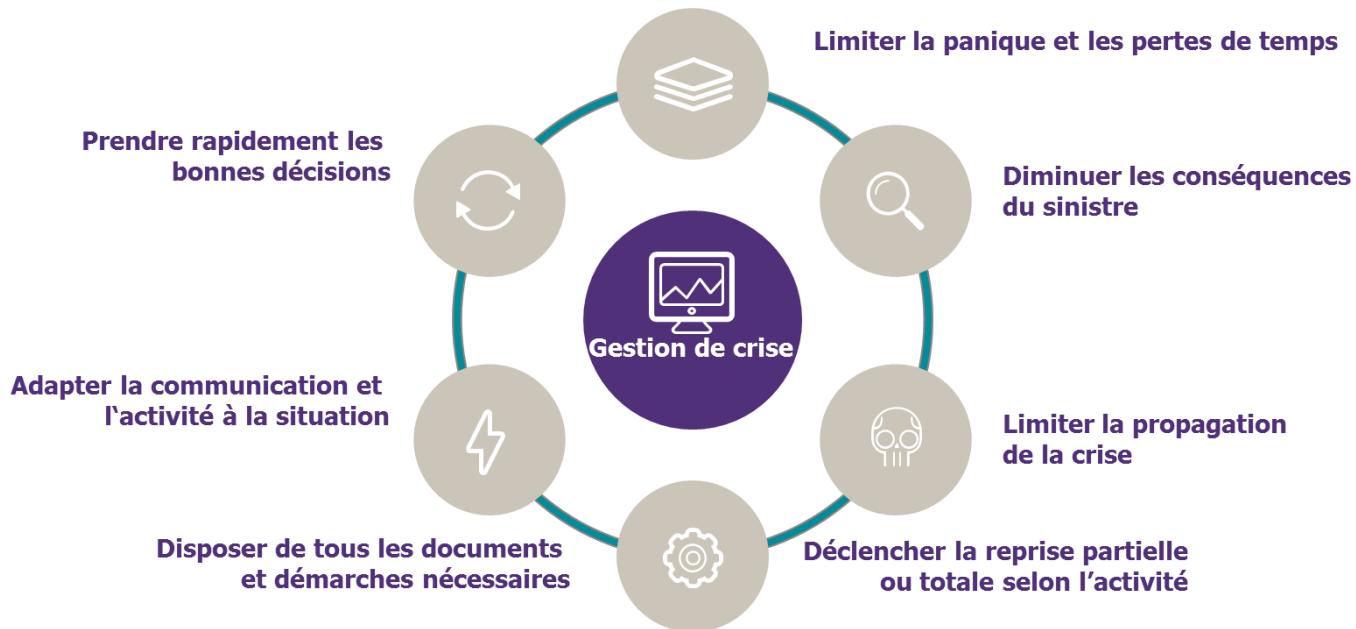
- / **Naturelles** inondations, tempêtes, grands froids, légionellose, épidémies...
- / **Environnementales** incendies, explosions liées à des infrastructures ou sites à risque...
- / **Humaines** défaillance de processus, erreur humaine, malveillance, attentat...
- / **Technologiques** panne informatique, défaillance matérielle, virus, cyber-attaque...

## Des événements affectant trois dimensions

- ① Périmètre géographique
- ② Dimension humaine/organisationnelle
- ③ Patrimoine informationnel



# Gérer une crise efficacement nécessite de se préparer en amont



## Malgré des facteurs aggravants...

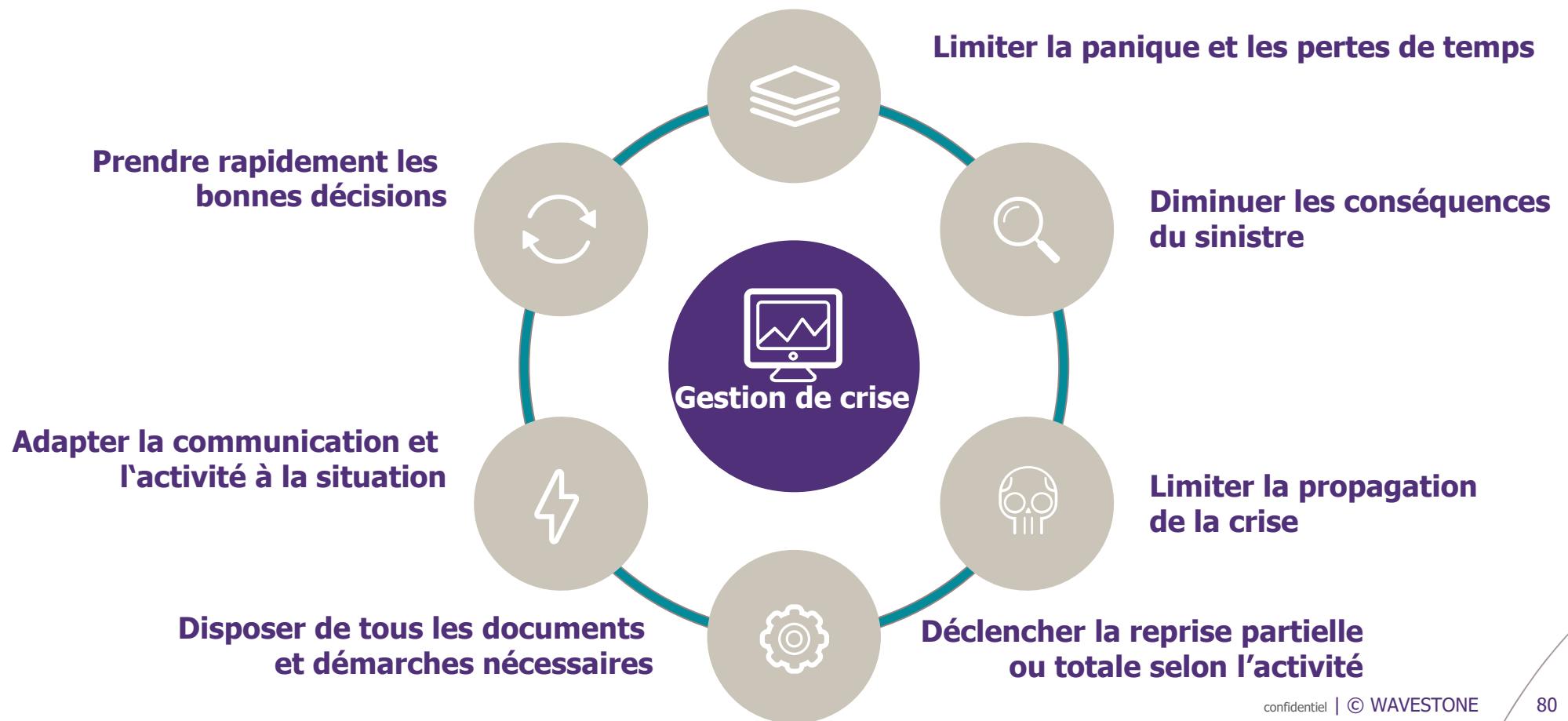
- / Cascade des événements additionnels (médias, pouvoirs publics, partenaires de l'entreprise...)
- / Pressions importantes, internes comme externes
- / Capacités individuelles altérées par le stress pouvant provoquer une montée de la subjectivité

**Il est essentiel de mettre en place un dispositif de crise préparé, entraîné, et maintenu dans la durée**

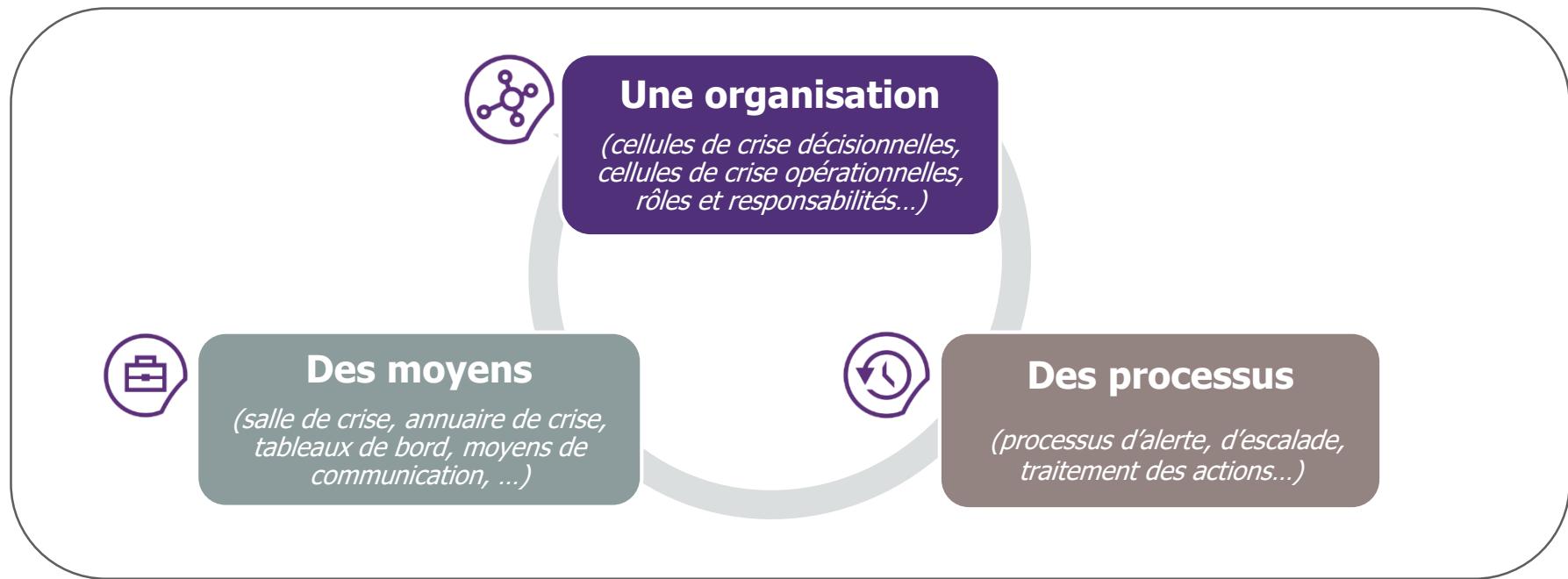
# Pourquoi mettre en place une organisation de gestion de crise ?

**Pendant une crise, les membres de l'entreprise doivent:**

- / Être rapides et efficaces
- / Savoir garder leur sang-froid
- / Prendre les bonnes décisions au bon moment



# La gestion de crise est axée sur trois piliers



## / Une organisation et des processus

- > Un **mode de gouvernance spécifique** pour prendre toute décision nécessaire à la préservation des intérêts de l'entreprise
- > Une déclinaison en plusieurs « **cellules de crise** » répondant à différents enjeux

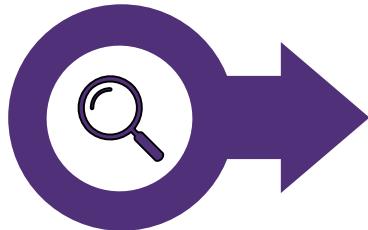
## / dotés de moyens et d'outils

- > Locaux pour la tenue des réunions des cellule / outils de communication
- > Documents de crise (checklists, annuaires, main courante, ...)
- > Plan de communication, plan de continuité d'activité (PCA), plan de secours industriel, ...

# Processus de gestion de crise

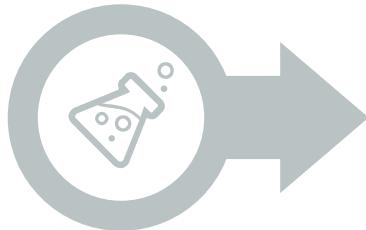


Le processus de gestion de crise se décline en quatre phases



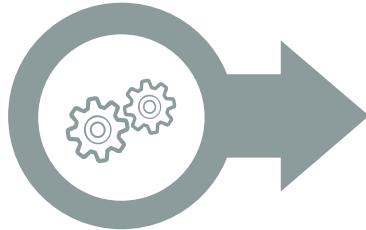
## Détection et Alerte

- / Détection : outils de supervision d'incident
- / Alerte : outils dédiés à la communication d'information interne



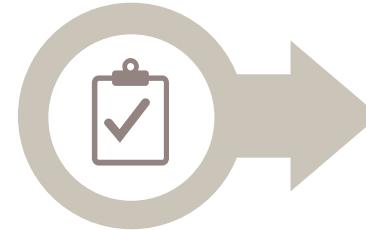
## Qualification

- / Identification des causes
- / Evaluation du temps de traitement
- / Communication de cette information aux parties prenantes



## Déclenchement et traitement

- / Implementation des solutions
- / Activation ou non du plan de secours
- / Préparation au retour à la normale



## Sortie de crise

- / Analyse de la résolution de crise
- / Communication aux partenaires et parties prenantes internes
- / Définition et suivi des plans d'amélioration

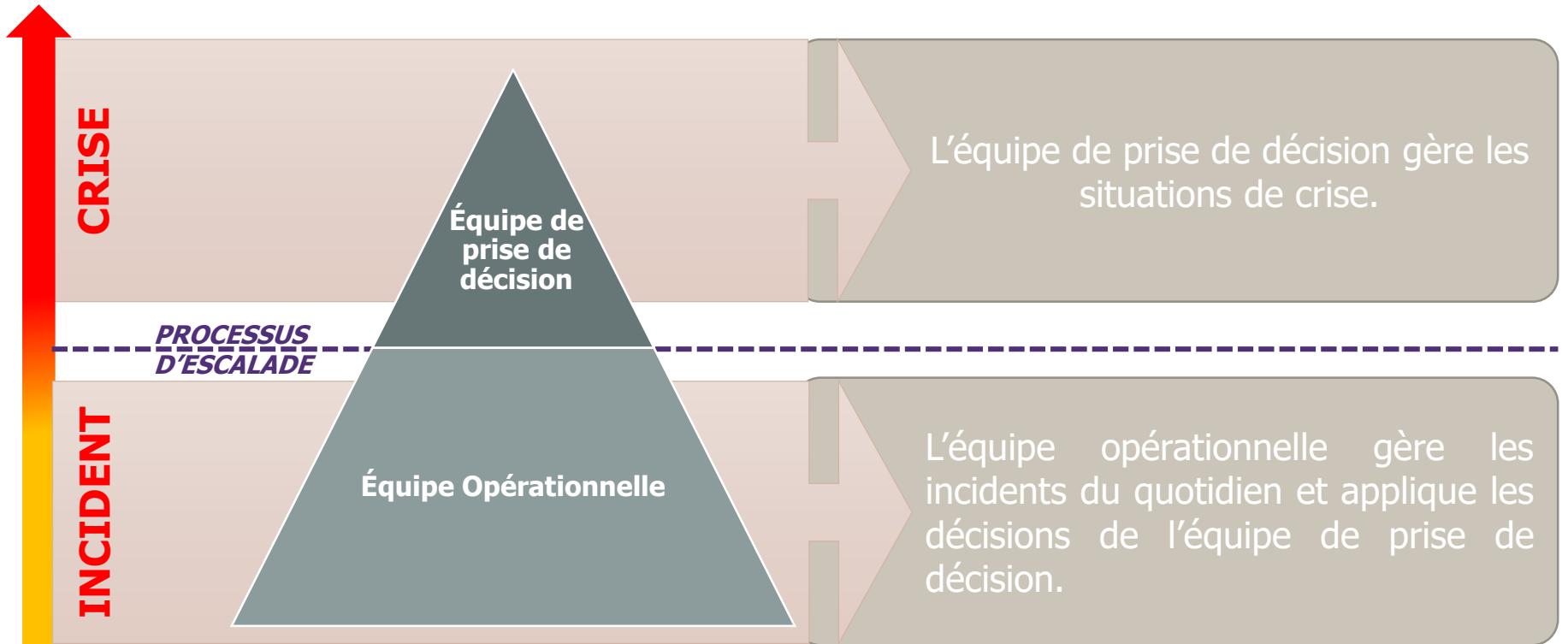


Note : A l'étape de qualification, un incident peut se révéler être une crise.

# Gestion des incidents et des crises



Une fois l'événement communiqué, la décision d'activer la gestion des crises est prise par l'équipe de décision. Lorsqu'il est activé, il s'appuie sur l'équipe opérationnelle pour la mise en œuvre de solutions sélectionnées.



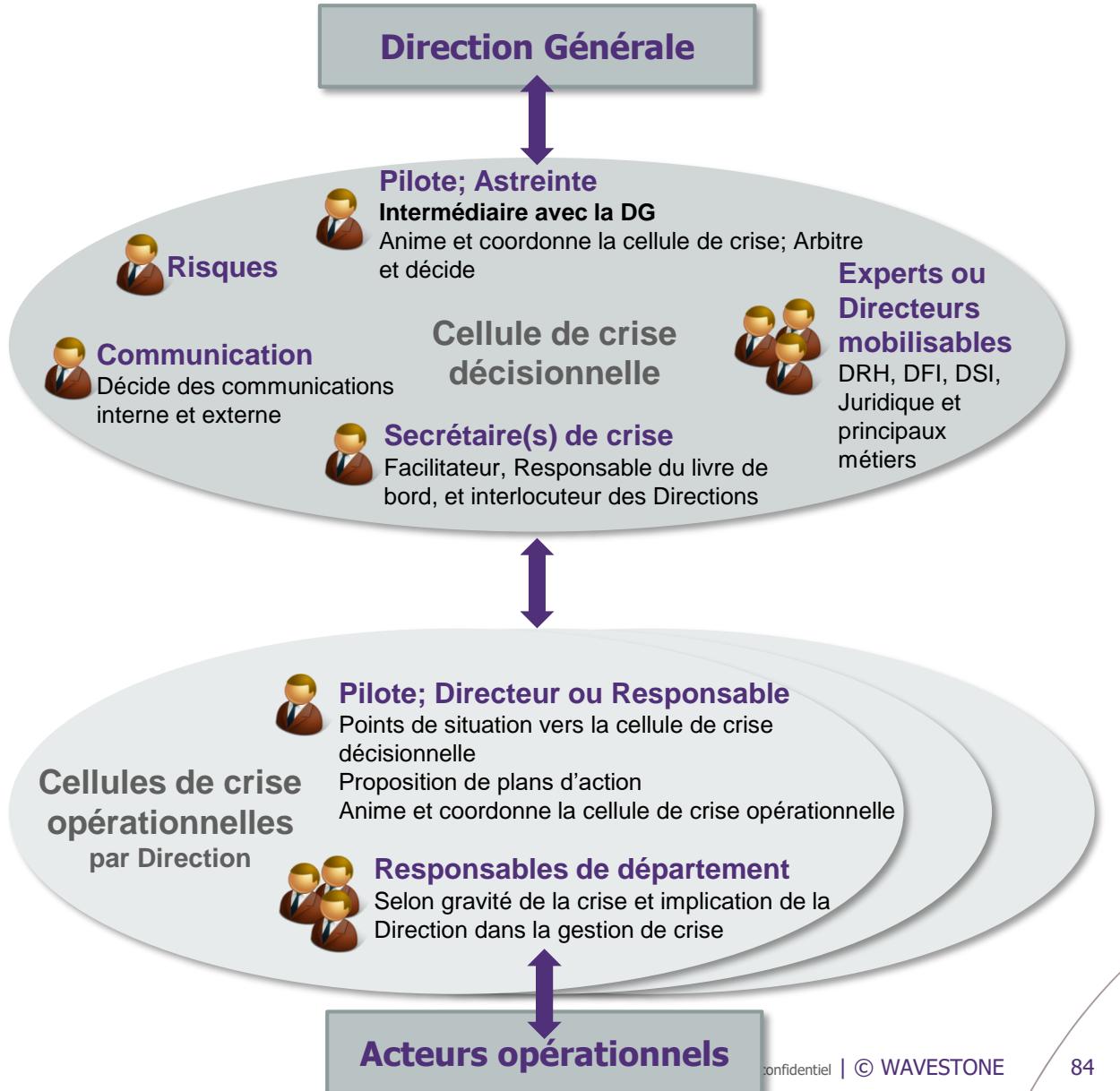
# Modèle d'organisation de gestion de crise

Décisionnel

- / Décisions et contrôles (dont déclenchement et sortie de crise)
- / Suivi et pilotage de la crise
- / Interlocuteur de la cellule de crise et autres cellules de crise Métiers
- / Assure la communication vis-à-vis de l'externe

Opérationnel

- / Analyse et évaluation de la situation
- / Appréciation et anticipation des impacts
- / Proposition de plan d'actions à la CD
- / Reporting régulier à destination de la CD
- / Pilotage et coordination des acteurs opérationnels
- / Sollicitation des experts en fonction de la nature de la crise

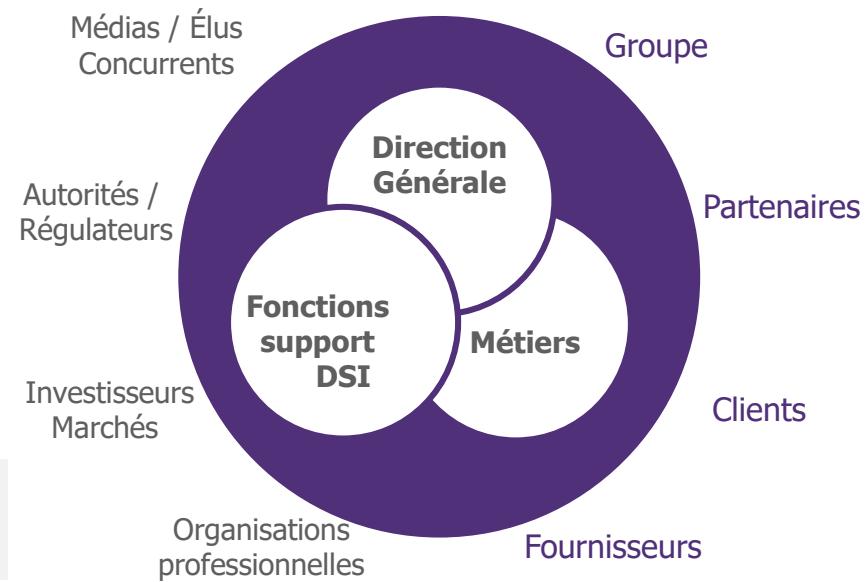


# La communication, un élément clé de la gestion de crise

## Conserver la capacité à bien communiquer...

- / Être **maître de sa stratégie de communication**
  - > **Reconnaissance** : accepter la crise le plus rapidement possible. Communiquer clairement et fermement.
  - > **Refus** : Minimiser les effets de la crise à condition d'être le seul interlocuteur à disposer des données.
  - > **Report de la responsabilité** : reporter la responsabilité. Orienter les faits vers d'autres acteurs.
  - > Etc.
- / S'assurer de la **cohérence et pertinence des messages**
- / Maintenir le lien entre toutes les parties prenantes de la crise
- / **Adaptation des messages** aux différentes populations cible

## ... au travers d'interfaces de communication identifiées et exercées



- / Maitriser les interfaces de communication **internes** (*Communication faite par le directeur général, par le management de proximité, etc.*)
- / Maitriser les interfaces de communication **externes** (*Communication presse, site web, etc.*)

# Exemple d'outils nécessaires à la gestion d'incidents et de crise



La gestion des incidents et des crises repose sur les **moyens suivants**

## Des outils de surveillance et d'alerte

Outil de détection



Outil d'alerte

## Des moyens de communication

Téléphone(s)  
Audioconf.



Fax



Mobiles



Ordinateur(s)  
Accès réseau(x)



## De la documentation

Annuaire de crise

Procédure d'escalade



Procédures (alerte...)



Main courante

## Des locaux dédiés

Salle « sur site »



Salle « hors site »  
inaccessibilité du site nominal



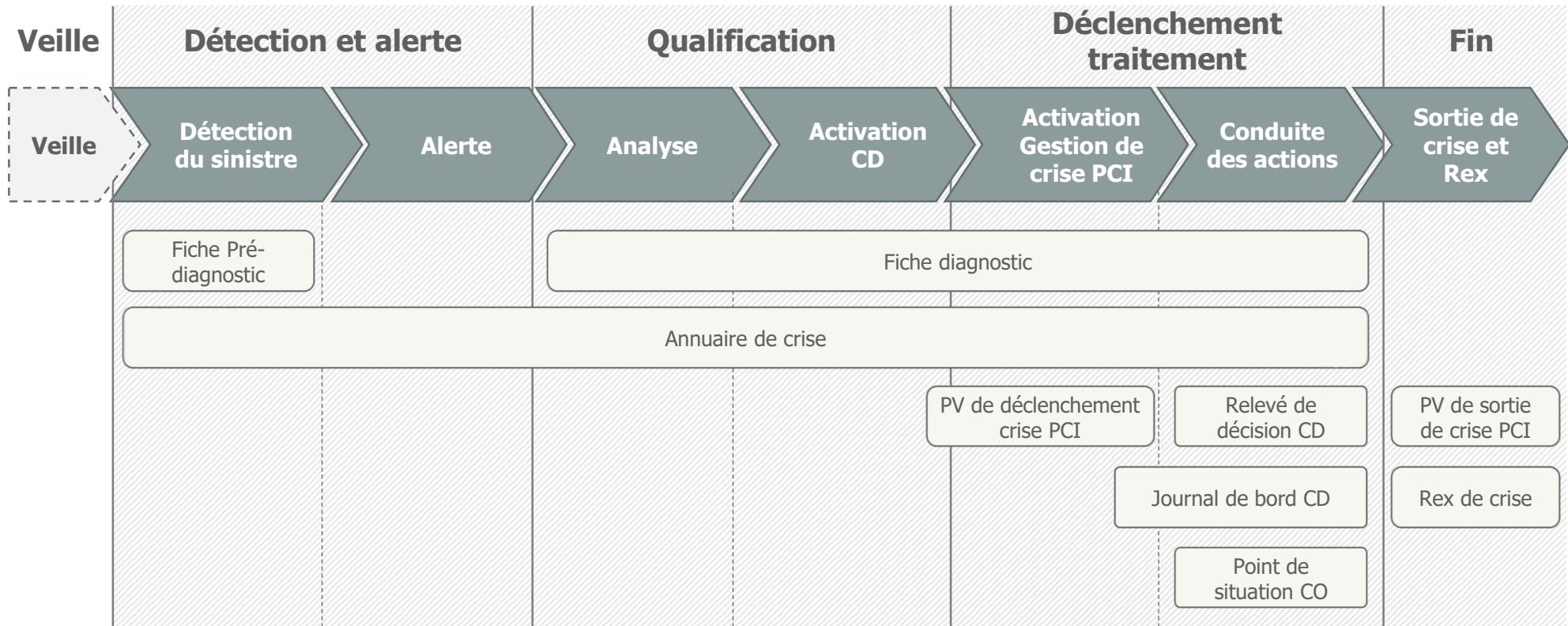
Incident

Crise

# Exemple de documentation de crise

**Pour chaque étape, des documents doivent être disponibles pour servir de support à la gestion de crise.**

**Ils sont consignées dans un classeur de crise mis à disposition des cellules de crise DSU.**



Légende :

Documentation

# Système documentaire

**Pour être efficace, le référentiel documentaire se doit d'être pragmatique, éprouvé et à jour et décliné de façon opérationnelle par acteurs**



# Agenda

- 1. Introduction à la continuité d'activité
- 2. Plans de Continuité Informatique
- 3. Plans de Continuité des Opérations
- ▶ 4. Gestion des incidents et des crises
  - 4.1 *La théorie*
  - 4.2 *Exemple d'exercice de crise*

# Un exercice pour sensibiliser à la cybercriminalité...

## 3 objectifs de l'exercice...

Travailler sur la **détection et la qualification** d'un incident technique en « incident de sécurité »

Vérifier que les **campagnes de sensibilisation** réalisées portent leur fruit (connaissance des symptômes et des procédures)

Sensibiliser les équipes à travers l'exercice et faire des personnes impliquées des **ambassadeurs du sujet**

## ...Pour 3 enjeux de la filière SSI

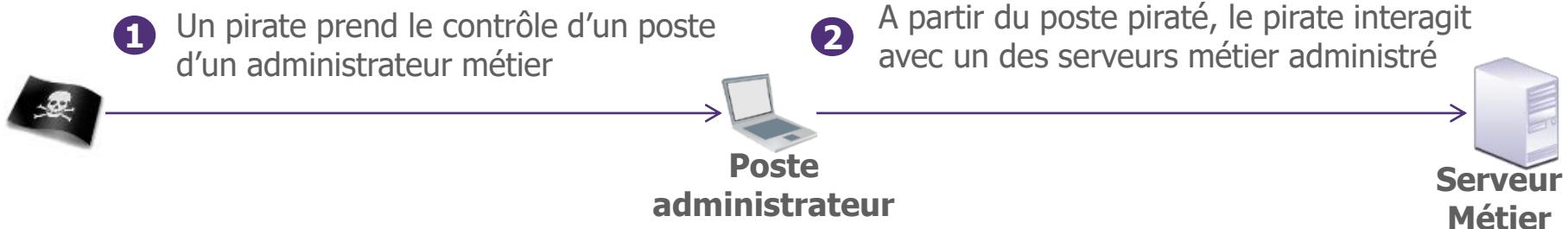
La SSI souhaite vérifier que l'équipe ciblée sait différencier incident de sécurité et incident d'exploitation

La SSI souhaite apporter du poids à son travail de sensibilisation à la sécurité

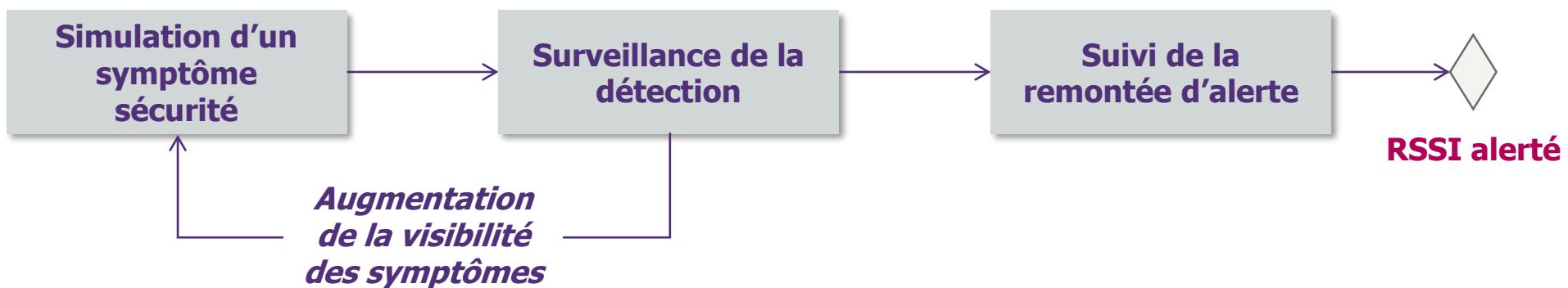
La SSI souhaite que les acteurs et les cibles parlent « Sécurité » suite à l'exercice

L'exercice est réalisé techniquement sans prévenir les cibles...

## Le scénario considéré est le suivant :



## Et sera simulé ainsi :



## Ce qu'il s'est passé...

Envoi de symptômes techniques bureautiques gradués sur deux jours



**Un utilisateur les supprime : Pas de réaction...**



**Quelques utilisateurs voient l'alerte : Pas de réaction...**



**Personne ne voit les fichiers : Pas de réaction !**



**Quelques utilisateurs voient les alertes : Pas de réaction !!**



**Les utilisateurs commencent à discuter...**



**L'incident est enfin qualifié et remonté correctement !**

## Ce qu'il s'est passé...

Stimulations par téléphone, graduées, sur un jour



**L'utilisateur ne voit rien...**



**L'utilisateur supprime les fichiers : pas de remontée d'alerte !**



**L'utilisateur prévient son manager...**



**L'utilisateur remonte l'alerte...**

# Quel bilan tirer de cet exercice ?

## Points forts

Détection et qualification de l'incident

- / L'incident sécurité a été **détecté et qualifié** par les utilisateurs ciblés

Remontée d'alerte sécurité

- / **Réaction positive** des utilisateurs ciblés qui ont bien **remonté les alertes**

Réaction et application des bonnes pratiques sécurité

- / Les utilisateurs ont eu **certains bons réflexes face aux attaques**  
(regarder les logs de connexions, investiguer sur l'incident)

## Axes d'amélioration

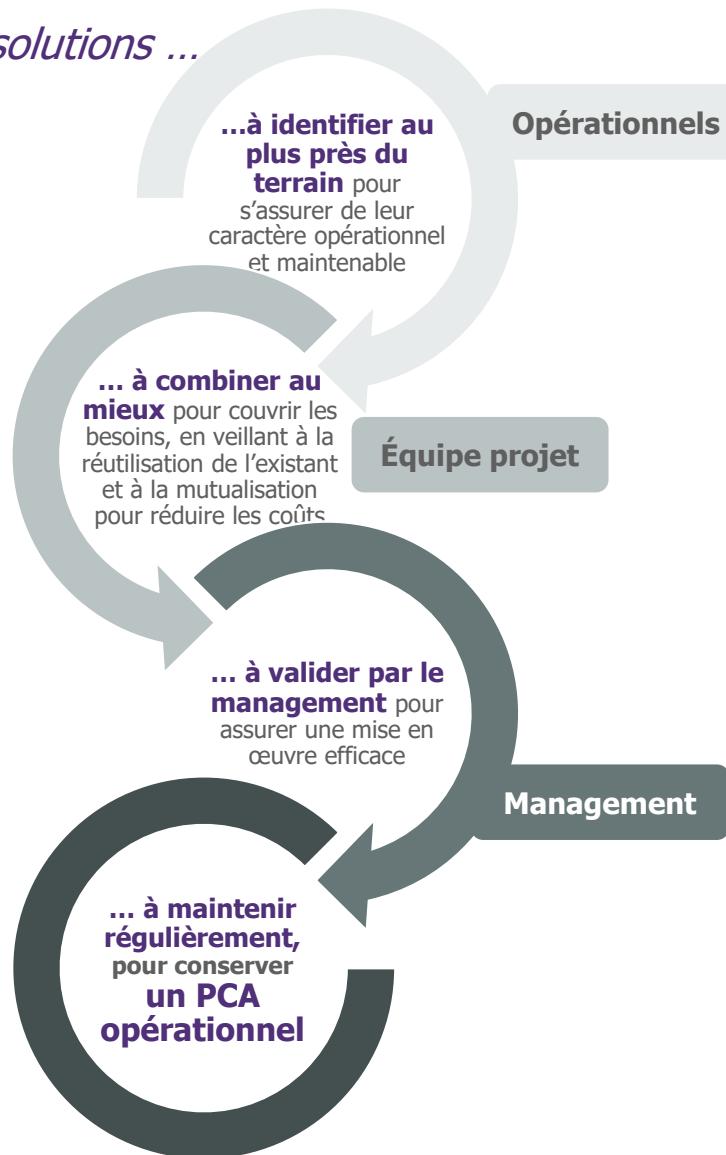
Seuls les signaux forts ont suscité une réaction des utilisateurs, à la fois côté serveur et bureautique

- / Il a fallu **un temps de réaction** avant la remontée
- / Certaines remontées **ne sont pas prévues par les procédures de remontée d'alerte sécurité**

- / Une partie des actions menées est **contraire aux bonnes pratiques** (suppression de fichiers impliquant la suppression de certaines traces utiles)

# Facteur clé de succès : définir une stratégie partagée par tous intégrée

*Des solutions ...*



**Opérationnels**

**PCA  
efficient**

**Management**

**Équipe projet**

**3 visions à faire converger pour assurer un PCA conforme aux besoins, opérationnel et maintenable**

# Conclusion

1

Le **PCA est nécessaire** pour savoir réagir à des incidents graves qui pourraient arriver

2

Le **PCA est un compromis** entre les coûts et la couverture de risque souhaitée

3

Le PCA doit être **un processus continu** et non un projet ponctuel

*Il doit rester efficient, « aligné » sur les besoins d'une entreprise, son organisation, ses processus, ses architectures, et ses infrastructures*



**Axel PETERSEN**  
Manager

**M** +33 (0)6 22 02 61 20  
Axel.Petersen@wavestone.fr

wavestone-advisors.com  
@wavestone\_

PARIS

LONDON

NEW YORK

HONG KONG

SINGAPORE \*

DUBAI \*

BRUSSELS

LUXEMBOURG

GENEVA

CASABLANCA

LYON

MARSEILLE

NANTES

\* Partenaires stratégiques

WAVESTONE

