Au-delà des mesures de prévention, le Plan de Continuité d'Activité une nécessité

François TÊTE

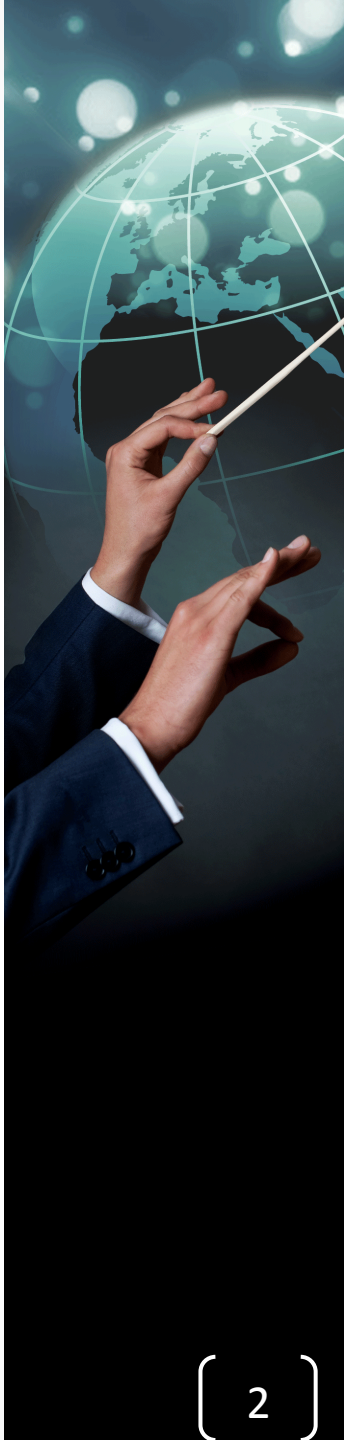
Consultant

-Président d'honneur du CCA –

Mardi 4 novembre 2014 ***Stand U 28***

Sommaire

- **Concepts**
- Mise en œuvre d'un PCA
- Maintien en condition opérationnelle

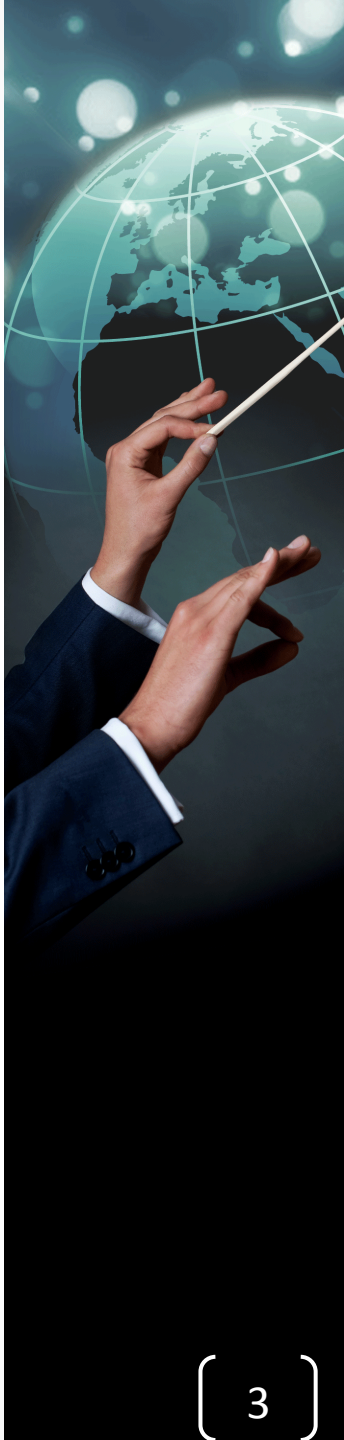


Le fonctionnement d'un organisme reste vulnérable

- Face au caractère imprévisible et fortement évolutif des causes de sinistre, les mesures préventives ne sont pas suffisantes.

- Des enchaînement d'événements mineurs peuvent conduire à des sinistres pouvant bloquer le fonctionnement d'un organisme. Loi de Murphy (1949).

- Il est nécessaire d 'anticiper en prévoyant une riposte pour faire face, par une stratégie de continuité :
  - de prévention (limiter les causes de sinistre) et,
  - de protection (limiter les conséquences)



Les risques pouvant impacter la continuité d'activité d'un organisme

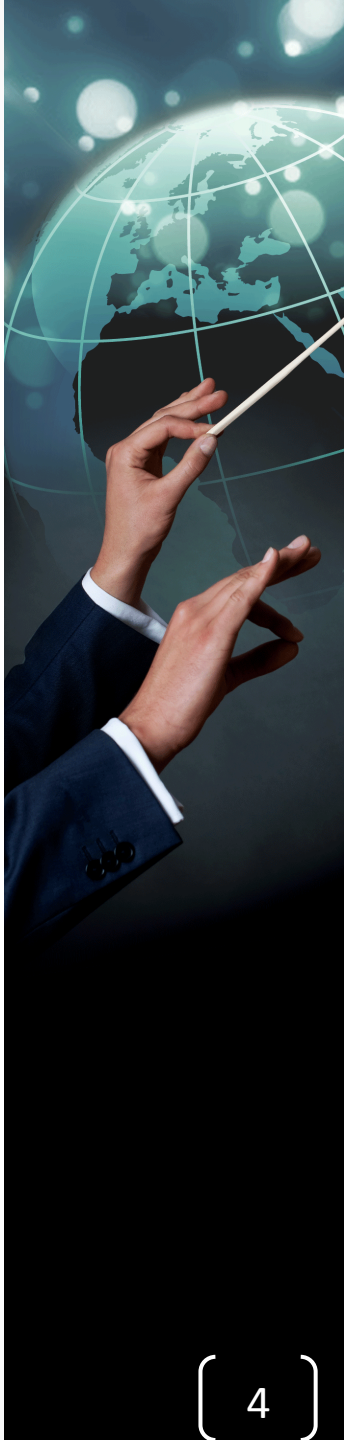
- Les causes peuvent être humaines, naturelles, accidentelles.

  - **Site ou bâtiment ou impraticable** : incendie, blocage des accès quelle qu'en soit la cause, coupure alimentation électrique secourue, mauvaises conditions sanitaires (eau, chauffage), …

  - **Ressources humaines indisponibles** : intoxication alimentaire, pandémie grippale, impossibilité de se déplacer , ...

  - **Informatique / téléphonie indisponible** : incendie, coupure du réseau, panne, attaque virale, perte d'intégrité de données, déni de service, ...

  - **Défaillance de fournisseur critique ou de fournisseur de fournisseurs :** transporteur, mainteneur, …

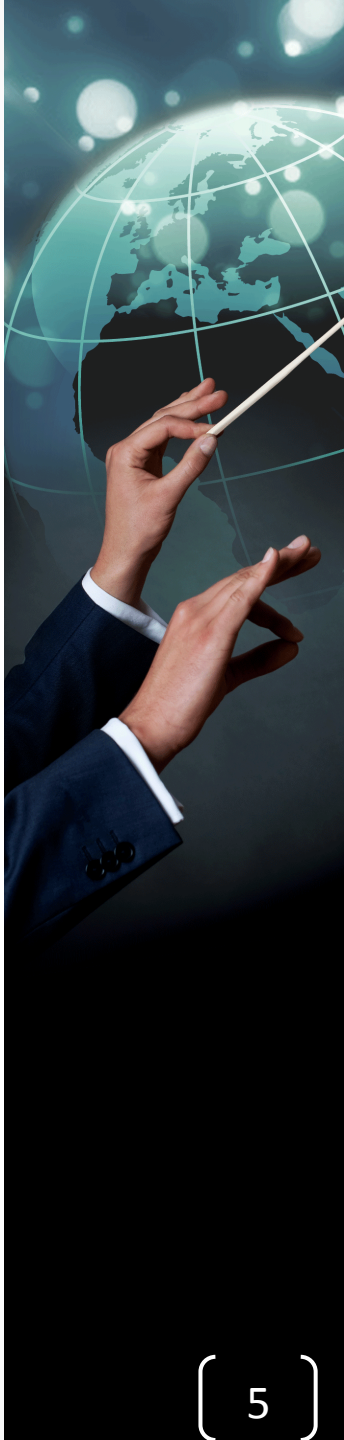


Quelques cas récents de sinistres

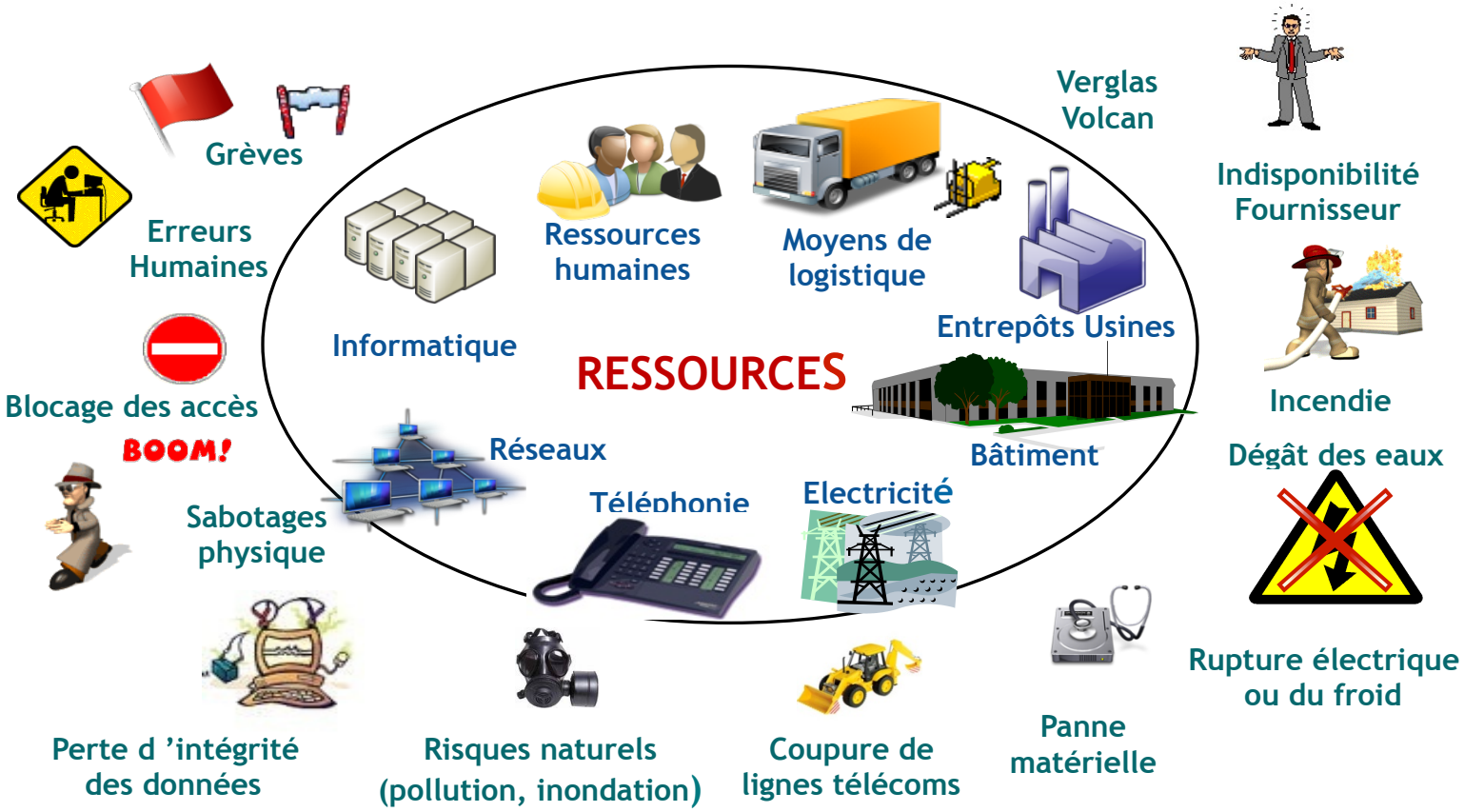
- 12 mars 2014 : panne de climatisation dans un data center parisien, vraisemblablement due à une panne logicielle et une erreur humaine

- Février 2013 : INTERMARCHE - déclenchement de leur alerte incendie en salle machine, perte de la majorité de leur baies de stockage: apparemment, la fréquence du son émis par les alarmes aurait créé un phénomène de résonance qui aurait provoqué une détérioration de la grande majorité des disques à l'intérieur des baies.

- 2012 : panne totale d'alimentation électrique dans un data center SNCF, malgré la double alimentation électrique, trois groupes électrogènes, des onduleurs, …



Quelques types de risques pouvant impacter des ressources d'un organisme

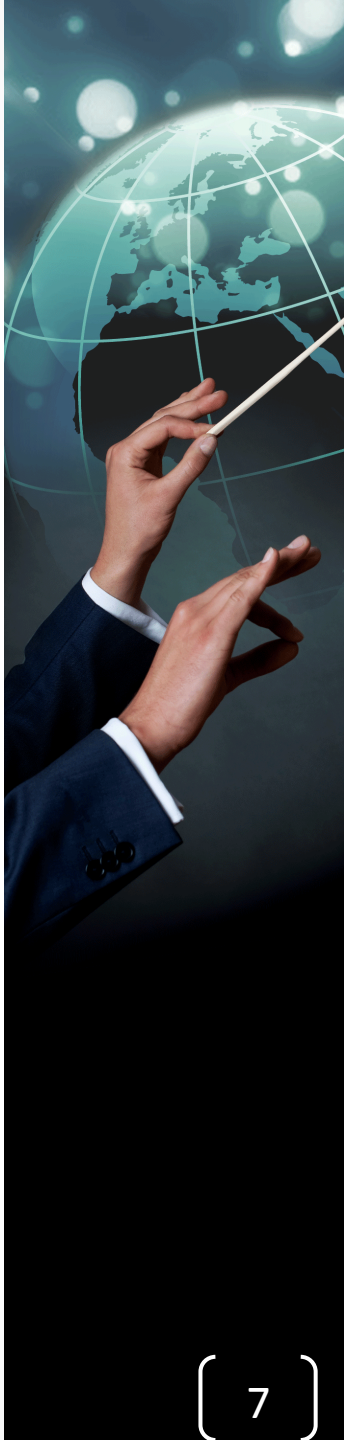


Les stratégies de continuité d'activité

- Réduction des causes de risques :
  - mesures de prévention : sécurisation, contrôle, surveillance

- Réduction des conséquences d'un risque :
  - Mesure de protection
  - Gestion de crise
  - Plans de continuité d'activité

- Il ne s'agit pas d'empêcher la survenance, mais de se donner les moyens d'absorber le choc, selon un partage entre deux stratégies :
  - Robustesse : sans trace visible
  - Résilience : avec des impacts visibles

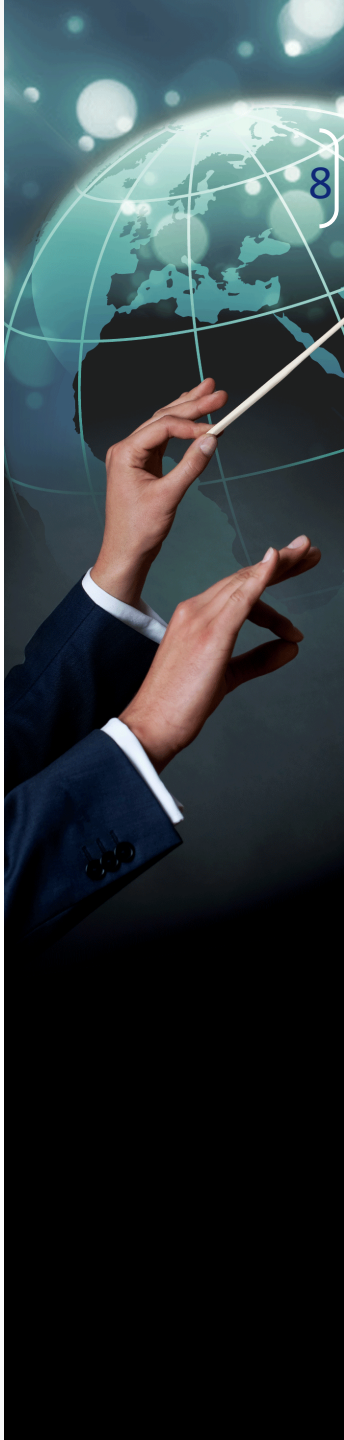


CCA

Les multiples conséquences d 'un sinistre en terme d'impacts

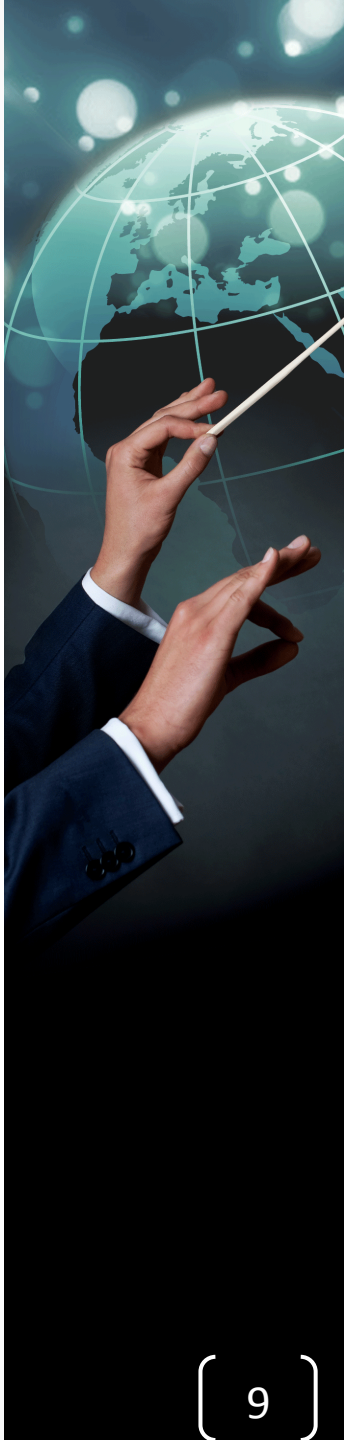
- **Pertes financières,**
  - Manque à gagner, perte de trésorerie, pénalités de retard...
- **Pertes d'images,**
  - Perte de confiance, perte de clientèle...
- **Pertes de productivité,**
  - Rupture du processus décisionnel, désorganisation liée au fonctionnement dégradée, surcharge pour rattraper le retard, ...
- **Pénalités contractuelles ou réglementaires,**
  - Non respect des obligations, ...

.



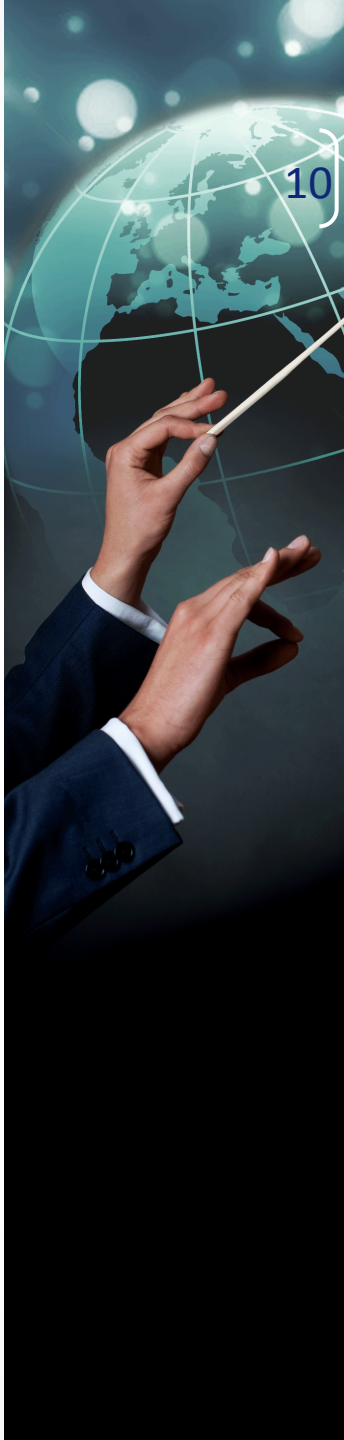
Objectifs de la continuité d'activité

- Assurer la continuité des activités essentielles
- Limiter :
  - les conséquences d'un sinistre auprès des clients,
  - l'impact financier
  - la perte d'image
- Être en conformité avec la réglementation
- Revenir à une situation normale aussi rapidement que possible
- Disposer d 'un argument commercial de plus en plus demandé
- Répondre aux demandes des clients
- Répondre aux demandes des actionnaires



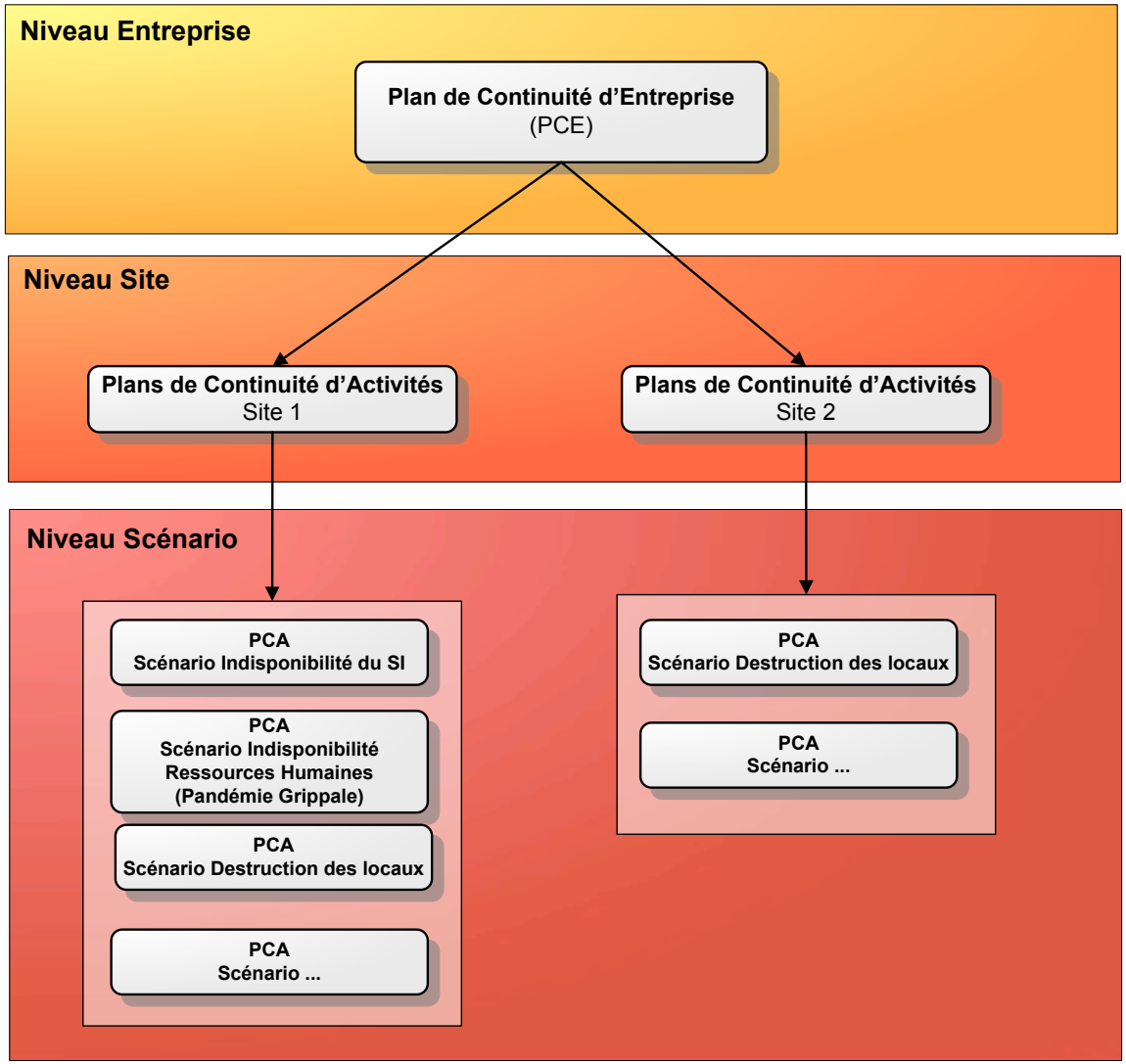
La définition officielle du PCA

- Un Plan de Continuité d'Activité (PCA) est un ensemble de mesures visant à assurer, selon divers scénarios de crises, y compris face à des chocs extrêmes et le cas échéant de façon temporaire, en mode dégradé, des prestations de services essentiels de l'entreprise puis la reprise planifiée des activités **(journal officiel de la République Française du 26 février 2004).**
- Procédures documentées servant de guide aux organismes pour répondre, rétablir, reprendre et retrouver un niveau de fonctionnement prédéfini à la suite d'une perturbation (Norme ISO 22301)



CCA

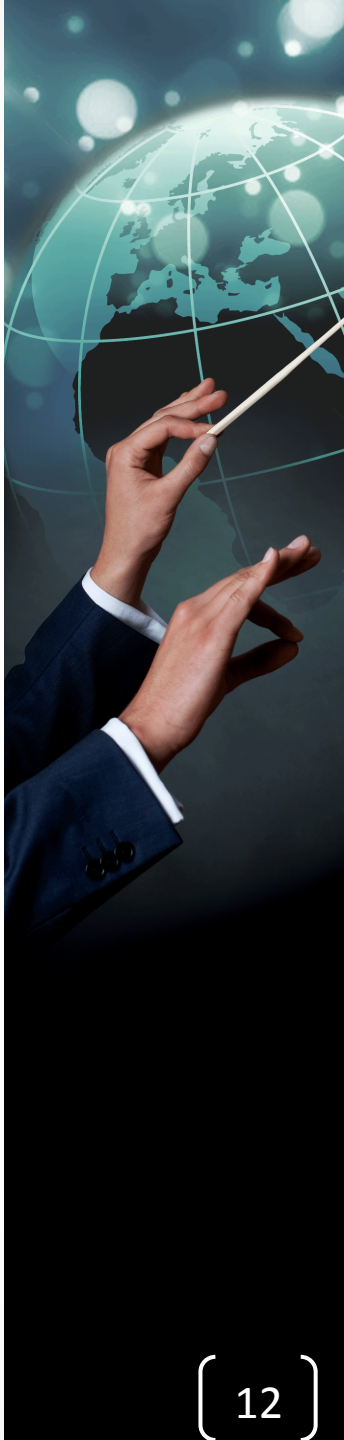
Le Plan de Continuité d'un organisme



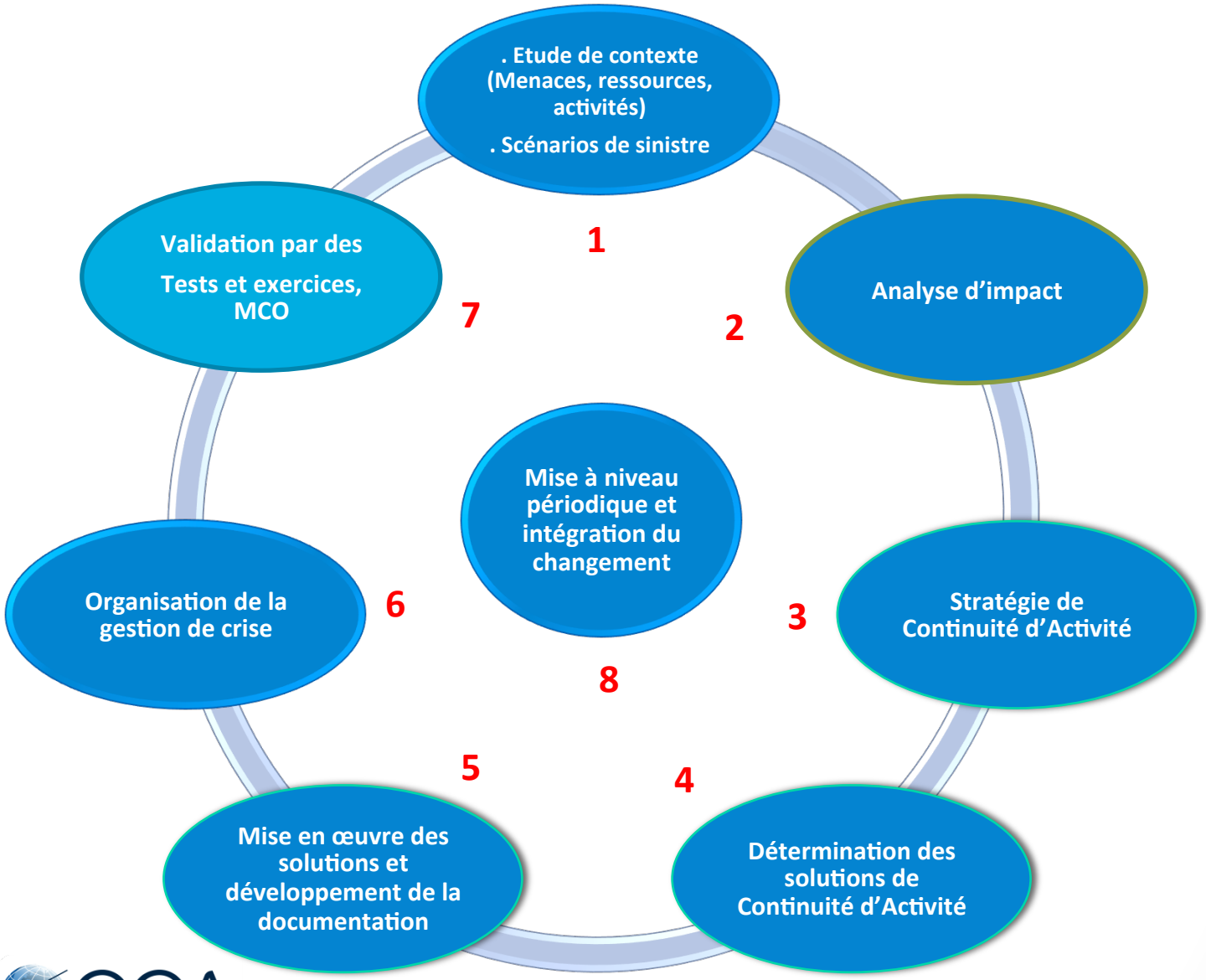
Source : CCA Lexique structuré de la Continuité d'Activité

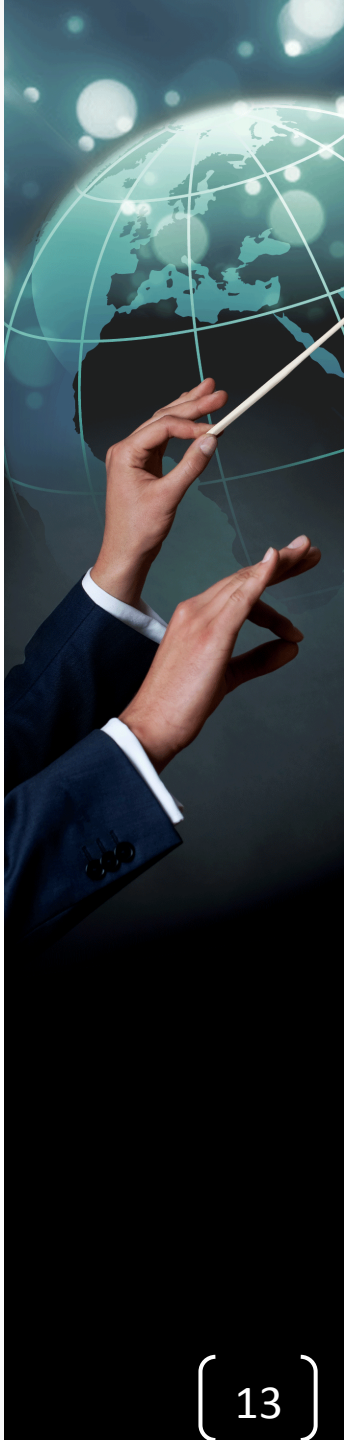
Sommaire

- Concepts
- **Mise en œuvre d'un PCA**
- Maintien en condition opérationnelle



Démarche type de mise en place d'un PCA



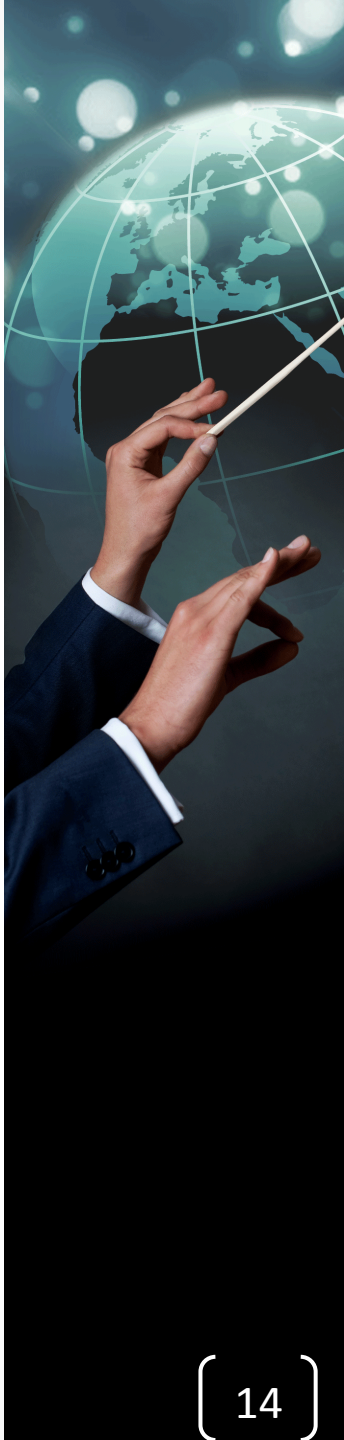


CCA

Expoprotection 2014 stand U28

Quelques principes de base

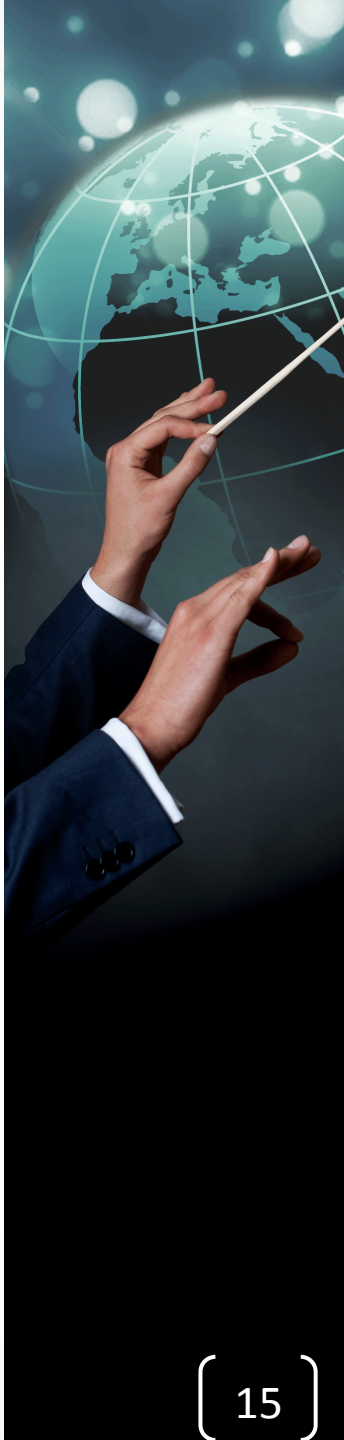
- Avoir la garantie d'accès à des ressources de secours informatique et de repli des utilisateurs
- Avoir un plan prêt à exécuter le jour du sinistre
- Avoir la garantie d'avoir toutes les compétences nécessaires en nombre suffisant
- Savoir réaliser des exercices de validation probants
- Savoir évoluer et maintenir le plan en condition opérationnelle
- Savoir intégrer la continuité d'activité dès la mise en place de nouveaux projets



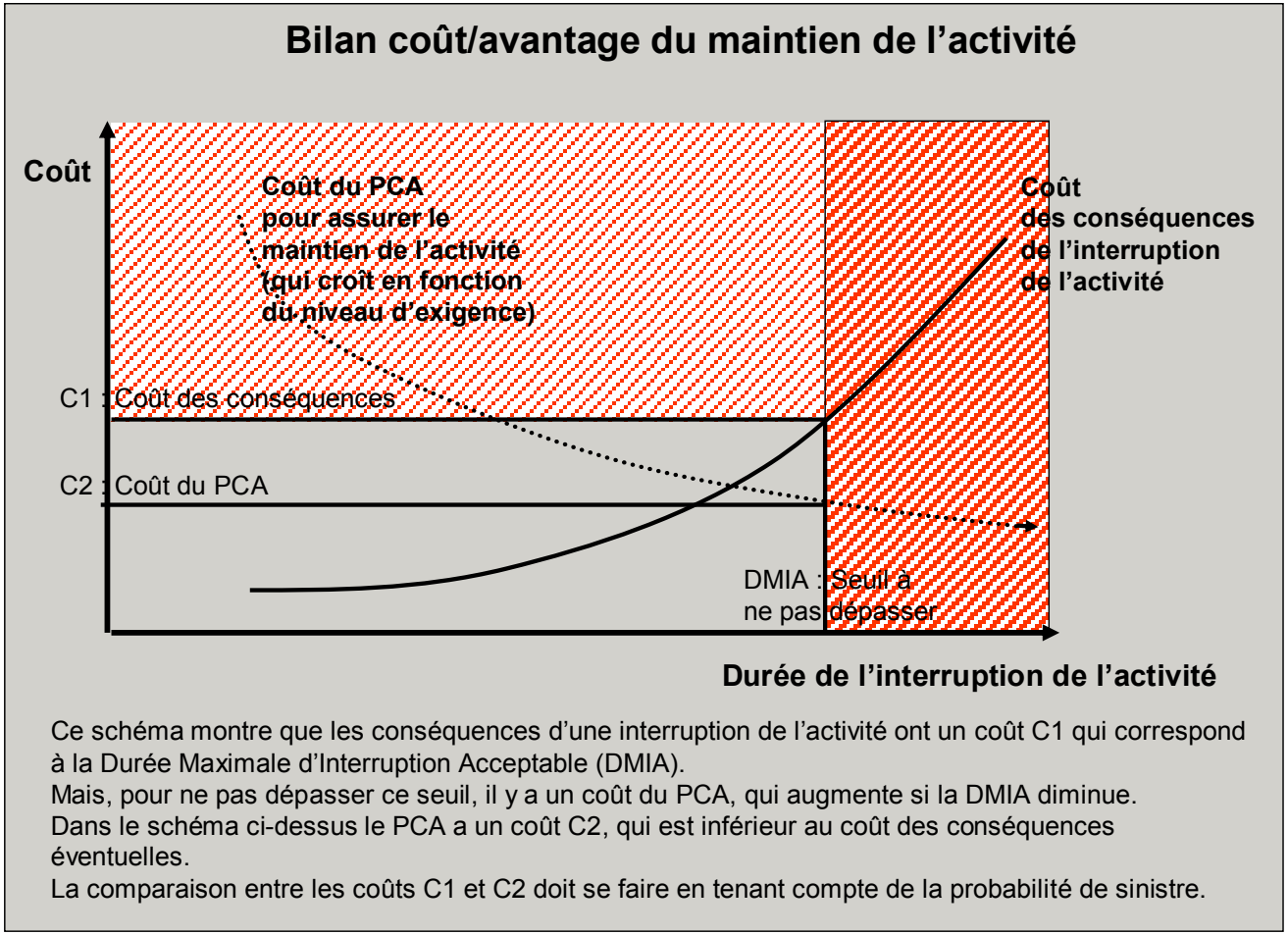
Les besoins de continuité demandés par les métiers

- Les métiers doivent exprimer leurs besoins de continuité par activités :
  - Durée Maximale d'Interruption Admissible (DMIA)
  - Perte Maximale de Donnée Tolérable (PMDT)
  - Nombre de position de travail sur les sites de repli, les ressources humaines, matérielles…

- Ces besoins doivent être justifiés par le chiffrage des impacts produits en terme de pertes financières, d'image, de productivité et de manquement à la réglementation.



Le coût du PCA versus le coût des conséquences



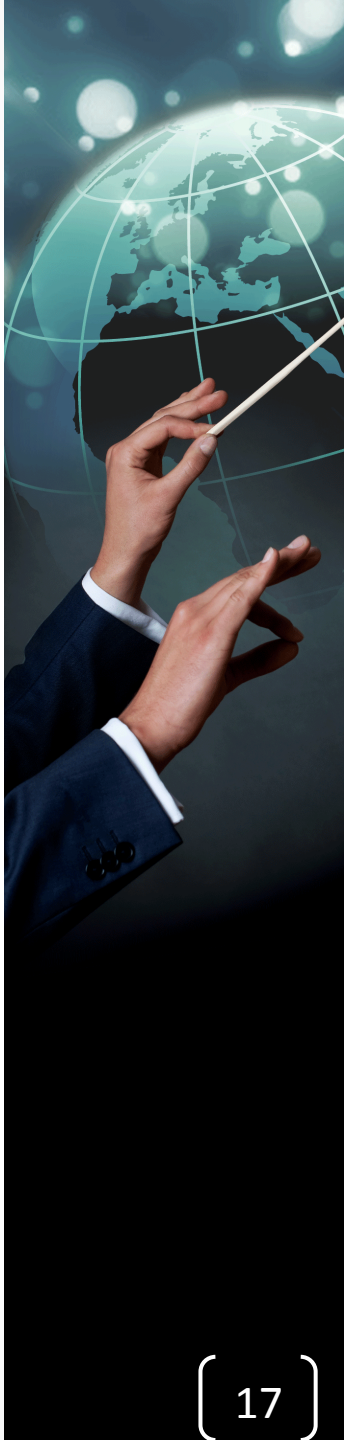
Ce schéma montre que les conséquences d'une interruption de l'activité ont un coût C1 qui correspond à la Durée Maximale d'Interruption Acceptable (DMIA).
Mais, pour ne pas dépasser ce seuil, il y a un coût du PCA, qui augmente si la DMIA diminue.
Dans le schéma ci-dessus le PCA a un coût C2, qui est inférieur au coût des conséquences éventuelles.
La comparaison entre les coûts C1 et C2 doit se faire en tenant compte de la probabilité de sinistre.

CCA

Source : Guide pour réaliser un PCA du SGDSN

Les composants d'un PCA

- Une organisation ad hoc de gestion de crise
- Des personnes entraînées
- Des mesures préventives
- Des solutions de secours informatique
- Des solutions de repli pour les utilisateurs
- Des plans et des procédures formalisés
- Des tests et des exercices de validation probante
- Une organisation de maintien en condition opérationnelle

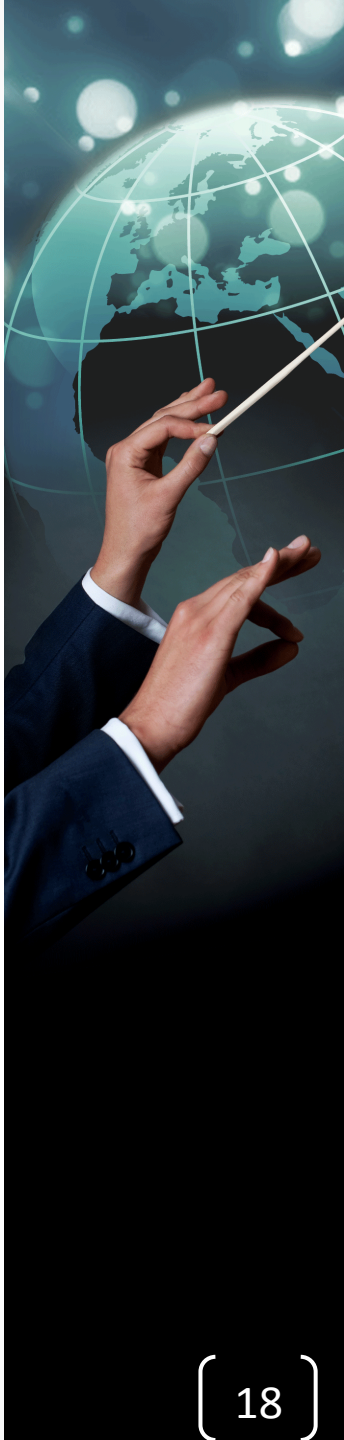


Des solutions de repli des utilisateurs

- Une solution de repli provisoire de niveau 1 : sites opérationnels connectés rapidement au réseau :
  - Locaux de l'entreprise proche, non soumis aux mêmes risques,
  - Locaux mutualisés loués contractuellement à un prestataire spécialisé et disponible dans un délai de quelques heures.

- Une solution de repli de niveau 2 : sites de repli prédéterminés, non opérationnels, à connecter au réseau et mis en place après le sinistre pour secourir l'ensemble des activités de l'organisme

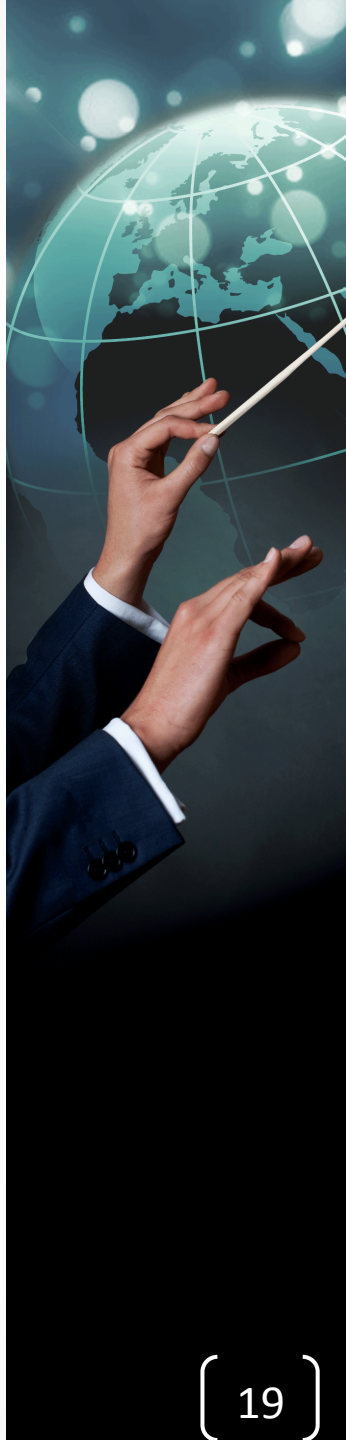
- Le Travail Occasionnel A Distance (TOAD) au domicile du salarié.



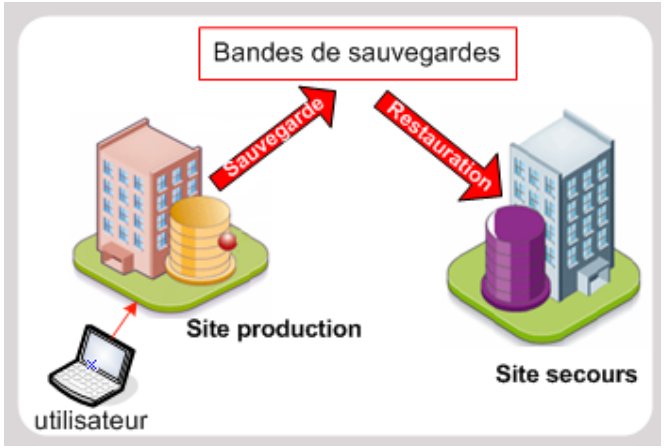
Des solutions de secours informatiques

- Un site informatique de secours interne à l ’organisme :
  - deuxième site informatique distant dédié ou non au secours

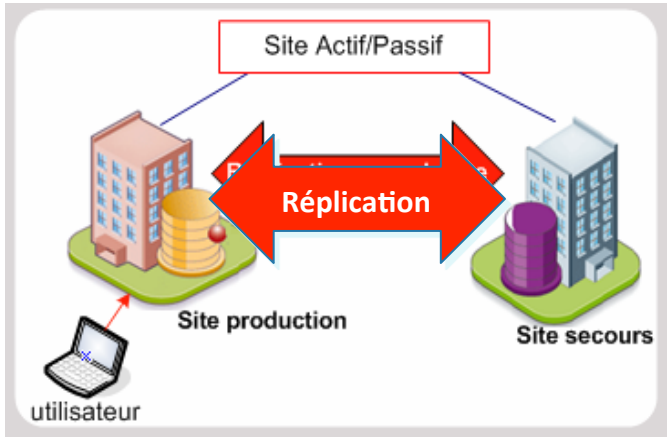
- Un site informatique de secours externe à l ’organisme **:**
  - site mutualisé de fournisseur de moyens de secours. Mais attention aux sinistres régionaux impactant plusieurs entreprises
  - site de secours ultime distant pour pallier un sinistre régional
  - site mutualisé entre sociétés d ’un même groupe



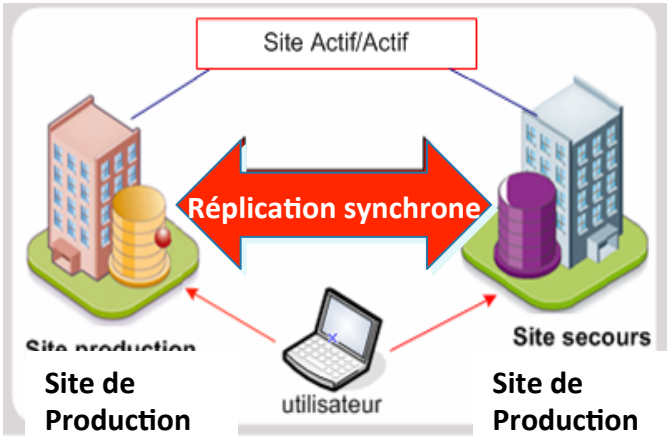
Les grands types de secours informatique



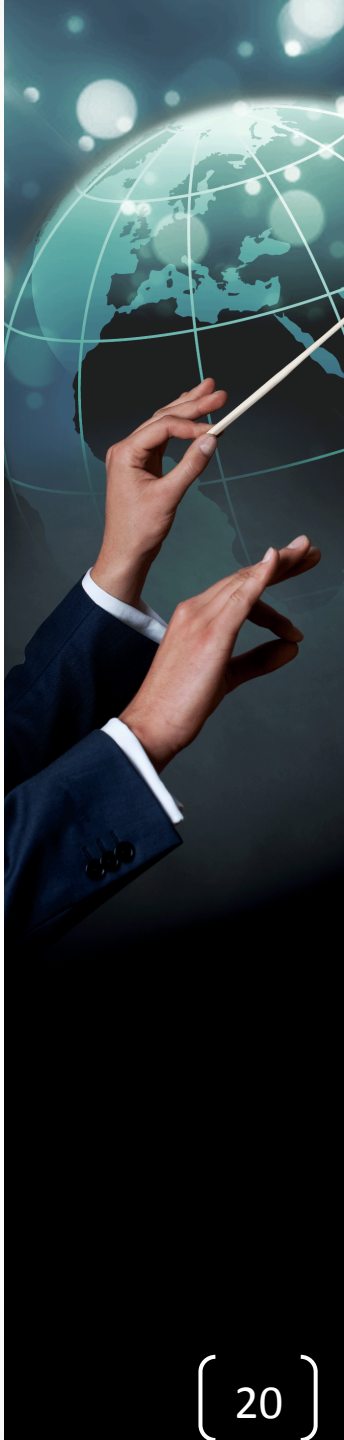
Secours à froid



Secours à chaud



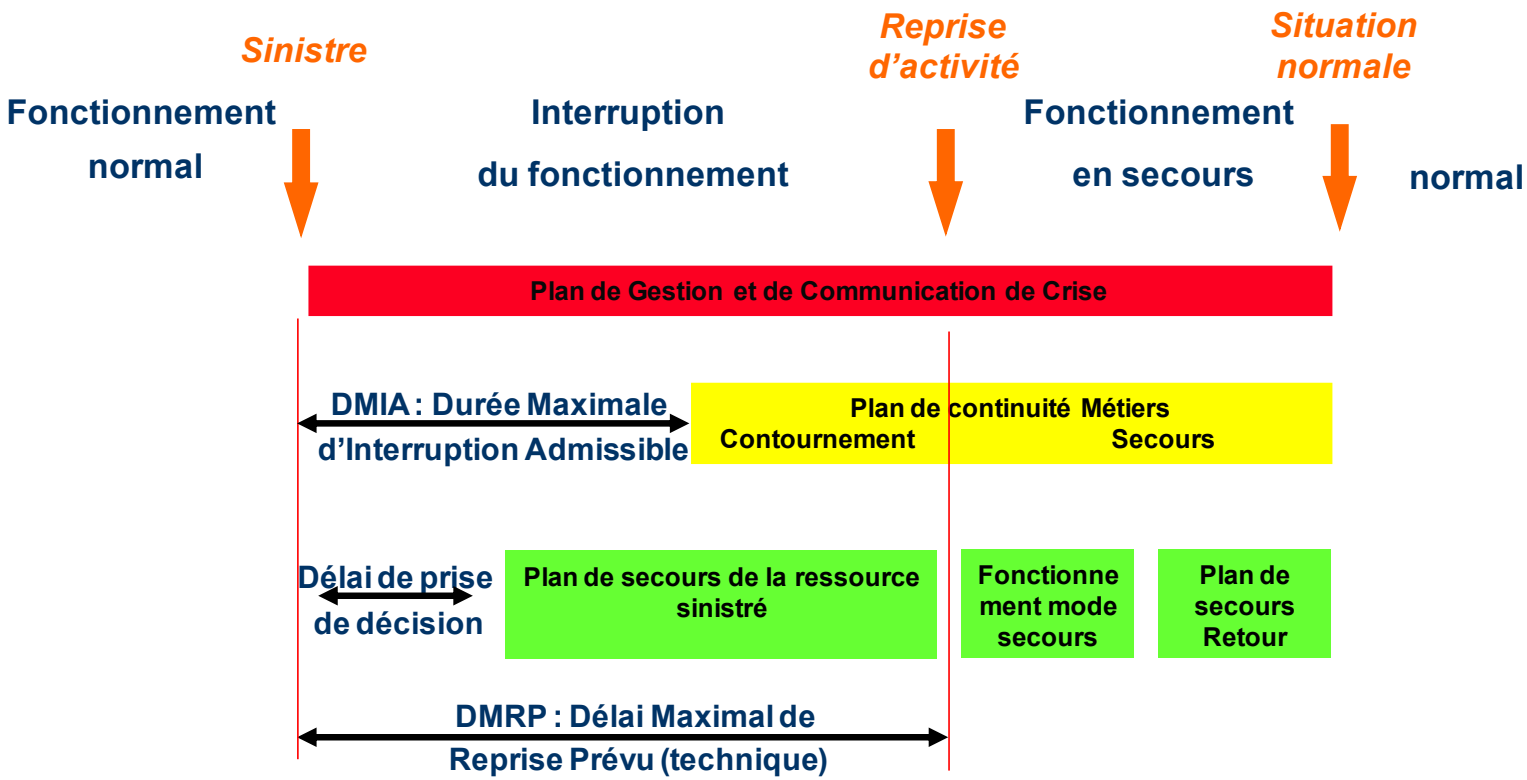
Haute Disponibilité



CCA

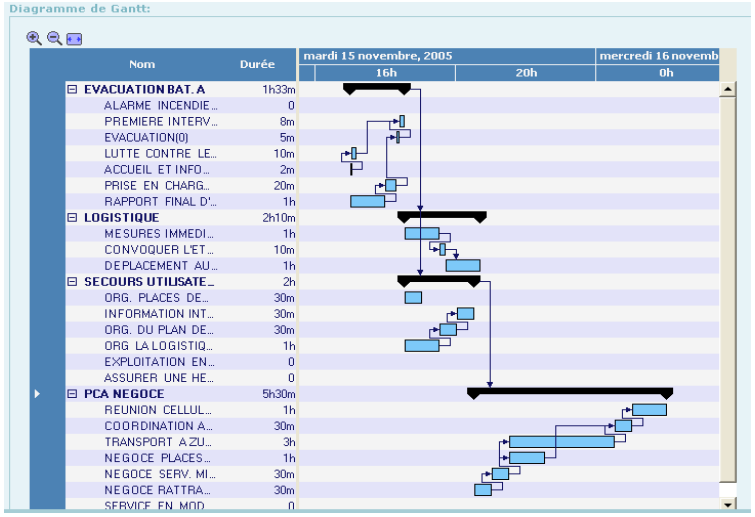
Expoprotection 2014 stand U28

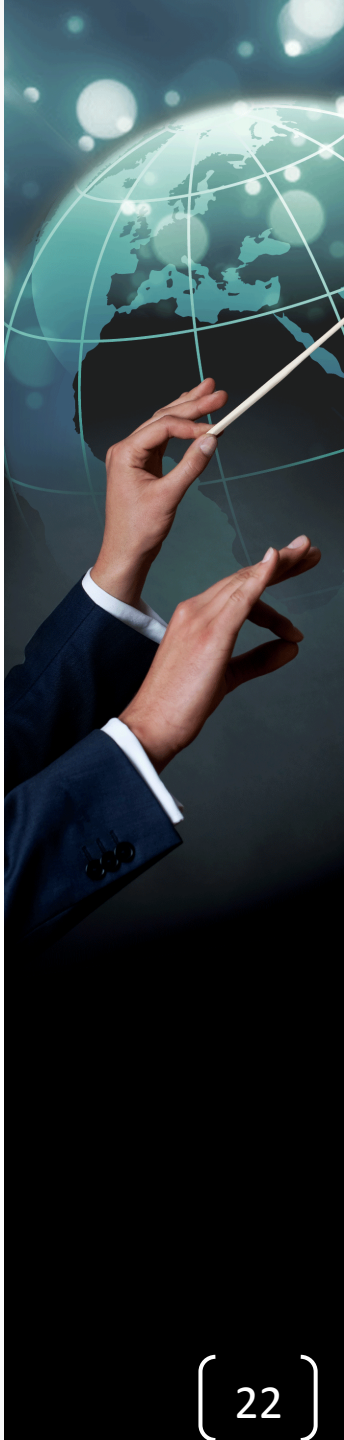
Synoptique du déroulement d'un PCA



Pilotage du PCA : nécessité d'un logiciel

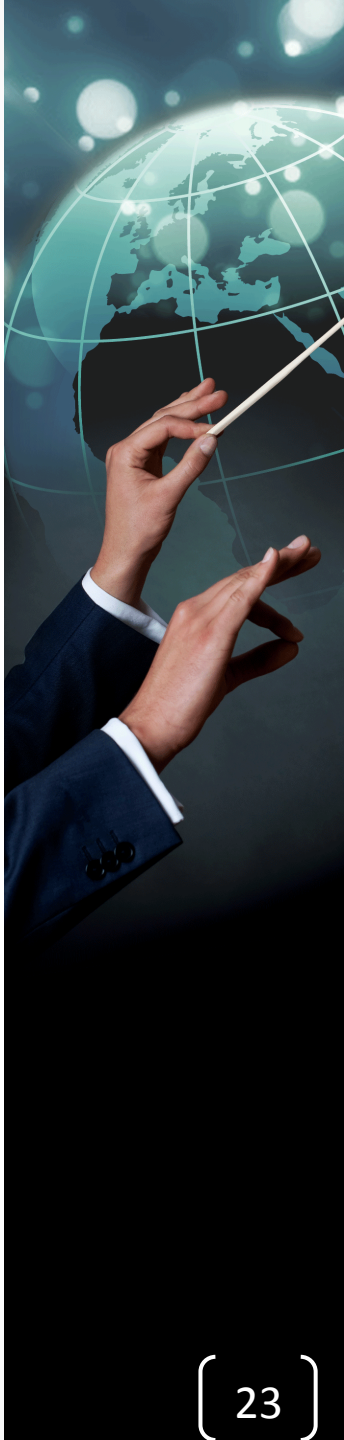
- Phase : EVACUATION BAT. A
  - Action : ALARME INCENDIE BATIMENT A
  - Action : PREMIERE INTERVENTION DU GPI(0)
  - Action : EVACUATION(0)
  - Action : LUTTE CONTRE LE FEU INITIALE(0)
  - Action : ACCUEIL ET INFORMATION AUX POMPIERS DU SIS(0)
  - Action : PRISE EN CHARGE DES PERSONNES EVACUEES(0)
  - Action : RAPPORT FINAL D'INTERVENTION(0)
- Phase : SECOURS UTILISATEURS
  - Action : ORG. PLACES DE TRAVAIL AU SITE DE SECOURS
  - Action : INFORMATION INTERNE TP
  - Action : ORG. DU PLAN DE SECOURS TP
  - Action : ORG LA LOGISTIQUE DU PERSONNEL(1)
  - Action : EXPLOITATION EN MODE SE SECOURS
  - Action : ASSURER UNE HELP LINE
- Plan de secours : Indisponibilité de la ressource Router sortie 1
  - Phase : LOGISTIQUE
    - Action : MESURES IMMEDIATES RH
    - Action : CONVOQUER L'ETAT MAJOR DE CRISE
    - Action : DEPLACEMENT AU SITE DE REPLI UTILISATEURS





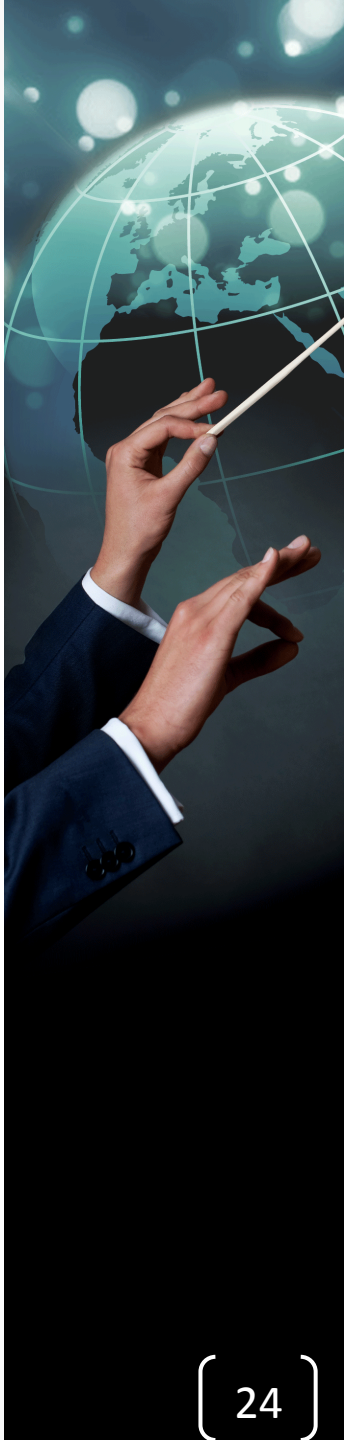
Sommaire

- Concepts
- Mise en œuvre d'un PCA
- **Maintien en condition opérationnelle**



Le Système de Management de la Continuité d'Activité (SMCA)

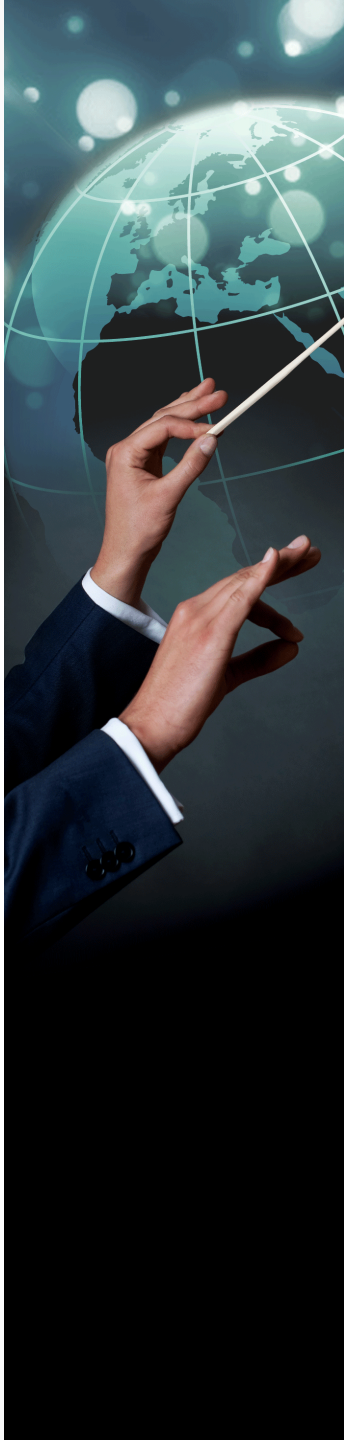
- Le SMCA est une partie du système de management global qui établit, met en œuvre, opère, contrôle, révise, maintient et améliore la continuité d'activité. (Norme ISO 22301 traduction CCA).
- Le SMCA préconise, entre autres, de mettre en place selon la roue de DEMING :
  - Une politique de continuité d'activité
  - Des rôles et des responsabilités :
    - Un Responsable des Plans de Continuité d'Activité
    - Des Correspondants des Plans de Continuité d'Activité par activité / département
  - Des tests et exercices de validation
  - Des audits
  - …



Le Maintien en Condition Opérationnelle du PCA

- Le Maintien en Condition Opérationnelle du PCA comprend :
  - Des révisions périodiques (arrêté PCA trimestriel)
  - Des tests et des exercices de validation
  - Des mises à jour ponctuelles, suite à des évolutions impératives

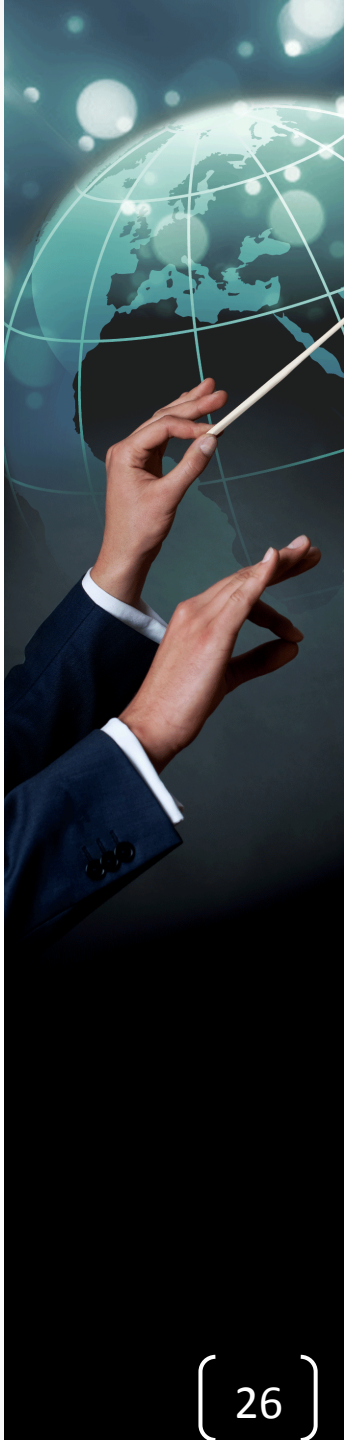
- Il est souhaitable d'anticiper l'évolution du PCA en intégrant la continuité d'activité dans la conception et la mise en place des nouveaux projets.



Les types de validation d'un PCA

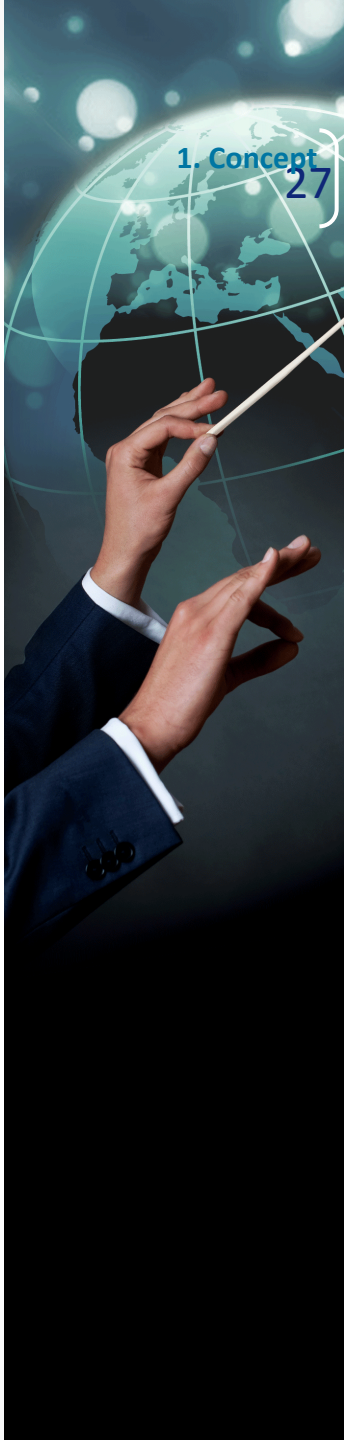
- Exercice préparé, date connue de tous les participants :
  - Simulé : peu d'impact sur l'activité
  - Réel : fonctionnement réel partiel ou total en secours

- Exercice inopiné, très peu ou pas de préparation :
  - Simulé
  - Réel



Des critères d' évaluation d'un exercice probant (1/2)

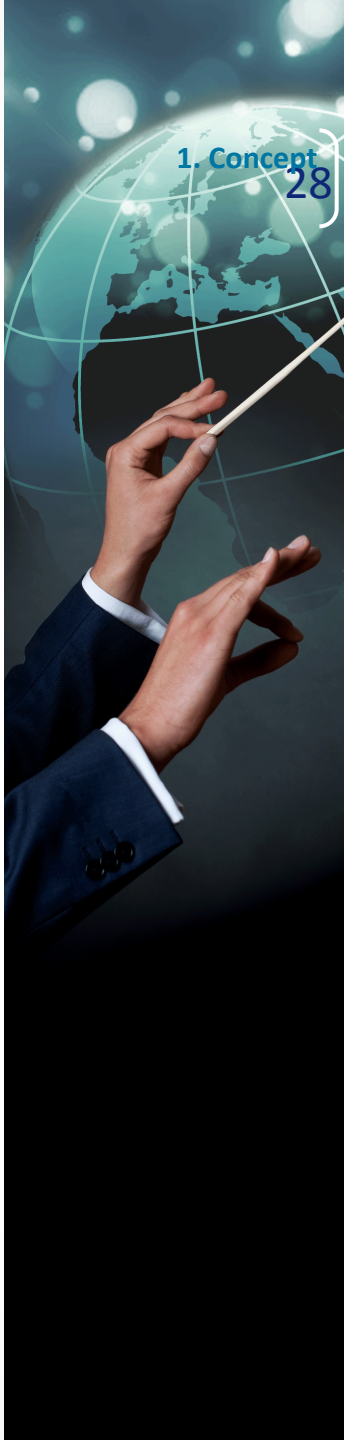
- Le périmètre du PCA s'est-il avéré adéquat aux besoins négociés avec les métiers à partir de leurs exigences ?
- Le scénario de sinistre pris en compte était-il réaliste et validé par la direction des risques ou son équivalent ?
- Les conditions de reprise d'activités observées (RTO, RPO) ont-elles été conformes aux conditions attendues par les métiers (DMIA, PMDT) ?
- L'entrainement des décideurs et des opérationnels est il suffisant ?
- Les dernières mises à jour ont-elles été testées ?
- Les exercices ont-ils été rejoués par une autre équipe ?



CCA

Des critères d' évaluation d'un exercice probant (1/2)

- Les conditions de stress des participants étaient-elles suffisantes ?
- Les exercices ont-ils révélé des erreurs ?
- Les conditions d'arrêt simulant le sinistre comportaient-elles assez d'éléments aléatoires pour éviter que l'exercice ne se déroule dans des conditions trop 'propres' et donc peu réalistes ?
- Des exercices inopinés avec une préparation limitée ont-ils été réalisés ?
- Le test/exercice a-t-il été contrôlé par des observateurs internes ou externes indépendants ?
- La durée de l'exercice a-t-elle été suffisante pour caractériser un scénario de sinistre réaliste ? Un jour ne suffit peut être pas.



CCA

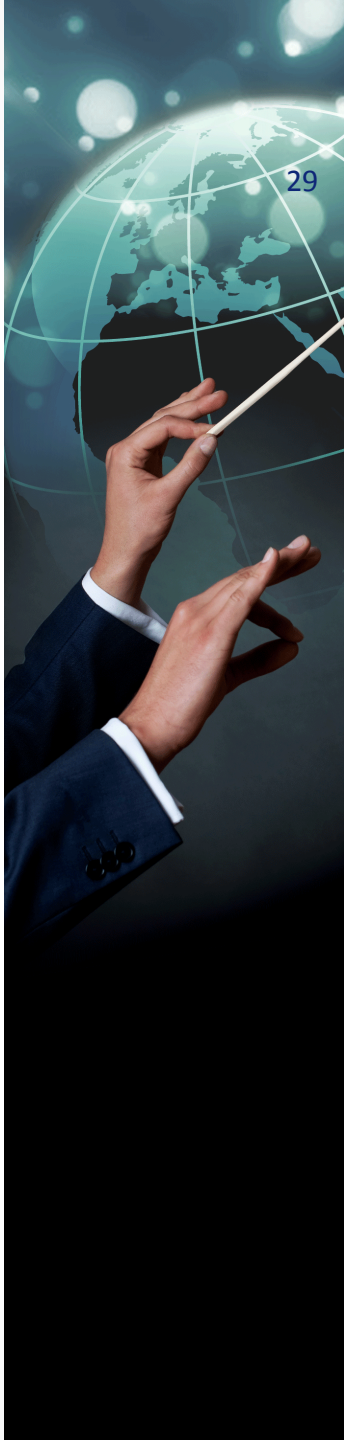
Pour conclure, deux proverbes

- "La veille d'un incident, le Return Of Investissement (ROI) d'un système de sécurité est nul, le lendemain il est infini …"

  Dennis Hoffman de RSA

- Les tuiles qui protègent de la pluie ont toutes été posées par beau temps.

  Proverbe chinois



Merci de votre attention

www.clubpca.eu

contact@clubpca.eu