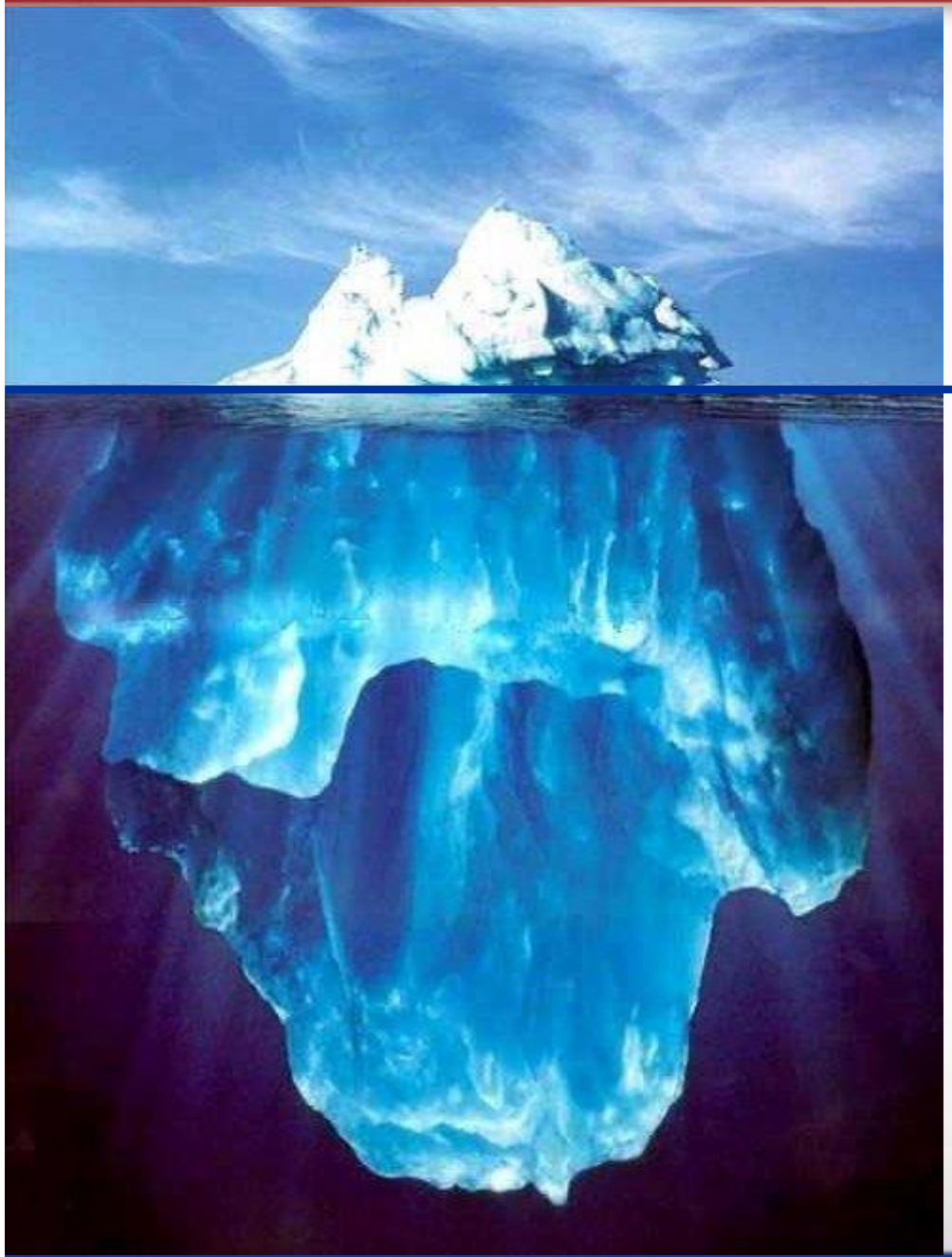

# Continuité d'Activité

## Une méthodologie pour conduire la réalisation et la mise en oeuvre de son PCA

Jean-Louis MARTIN

SSi-Conseil.com

# Plan de Continuité d'Activité : Conduire la réalisation de son PCA



CLUSIR Rhône Alpes

SSI Conseil

Sécurité des Systèmes d'Information

Jean-Louis MARTIN

« parce que la sécurité n'est pas une technologie mais un processus »*

www.ssi-conseil.com

* Bruce Schneier

# Continuité d'Activité

CLUSIR Rhône Alpes

# Construire des Plans de Continuité d'Activité

## Méthodologie & Solution

Les Enjeux : Anticiper la crise

Le Plan de Continuité d'activité :
- Solution de sécurité inscrite dans le SMSI
- Objectifs
- De quoi s'agit-il ?

Méthodologie :
- Principes de Management
- Conception
- Construire & conduire des Plans de Continuité d'Activité

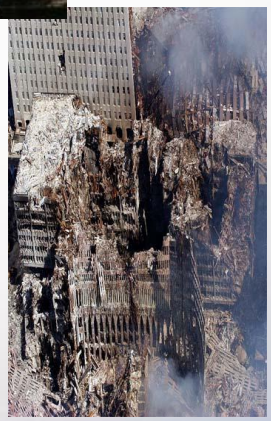
# les Enjeux

- Tempête ou inondation
- Incendie complet ou partiel
- Destruction / Inaccessibilité d'un site critique
- Grèves
- Incidents techniques de grande ampleur
  - Rupture des moyens électriques ou de communication
  - Pannes lourdes....
- Attaque « terroriste »
- Grippe aviaire







# les Enjeux

Tempête ou inondation

Incendie complet ou partiel

Destruction / Inaccessibilité d'un site critique

Grèves

Incidents techniques de grande ampleur

- Rupture des moyens électriques ou de communication
- Pannes lourdes....

Attaque « terroriste »

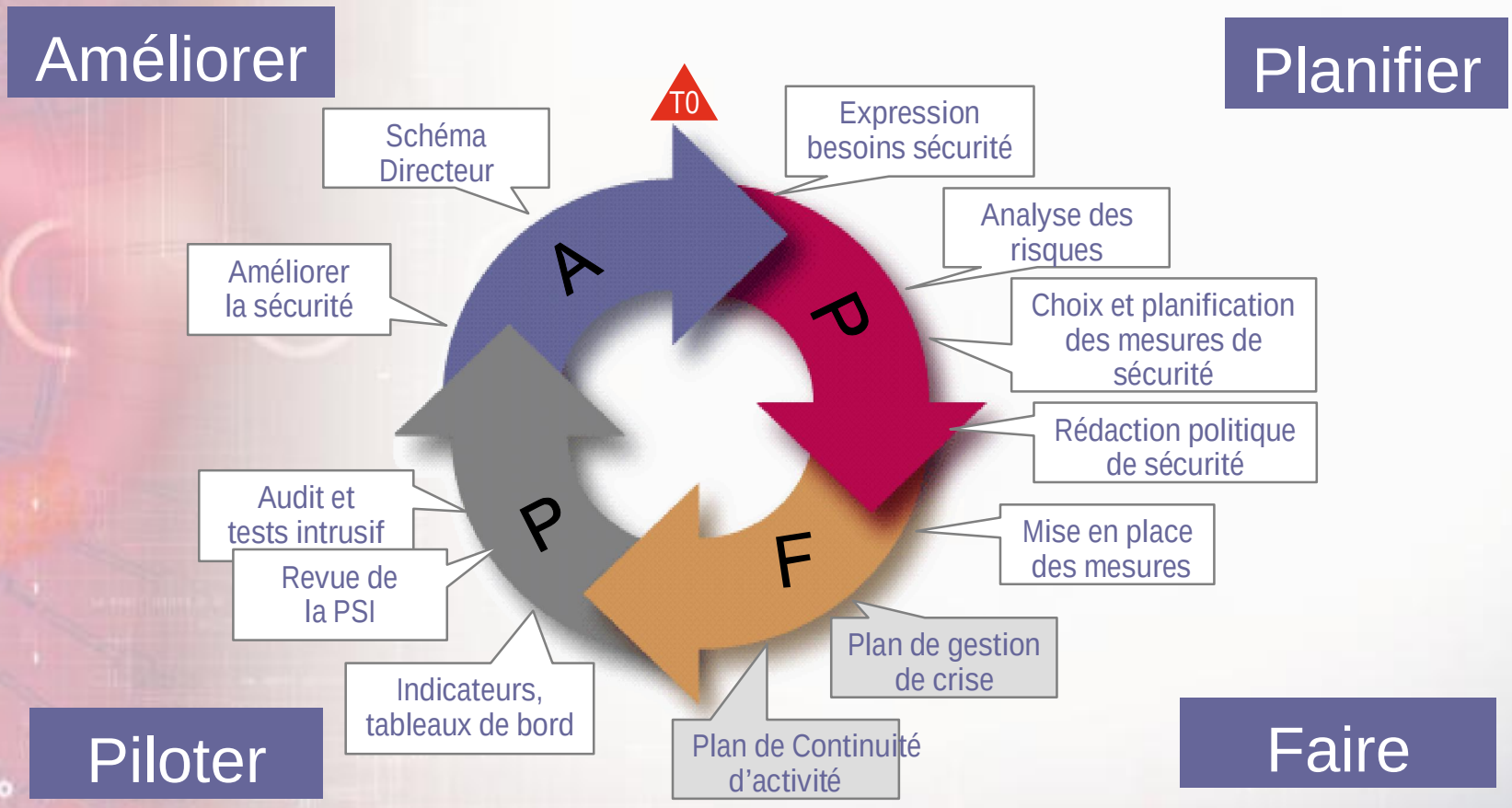
Grippe aviaire

Comment faire face ?

- Réagir dans des délais compatibles avec les besoins de l'entreprise,
- Mettre en place à la fois coordination, prise de décision et moyens opérationnels appropriés,
- Disposer de solutions de repli, pour les personnels, pour les moyens informatiques,
- Combien de temps cela peut-il durer ?
- Comment revenir à la normal

*"Les crises de demain sont souvent le refus des questions d'aujourd'hui »*

# PCA : Solutions de sécurité inscrite dans le SMSI




Source :YSOSECURE

# PCA : Objectifs (rappel)

« Un plan de continuité des activités est une réponse à l'arrêt inattendu de certaines activités d'une entreprise ou organisme. »

- mis en œuvre par une équipe de crise.
- réduit à un niveau acceptable les conséquences d'un arrêt des activités.

Objectifs :

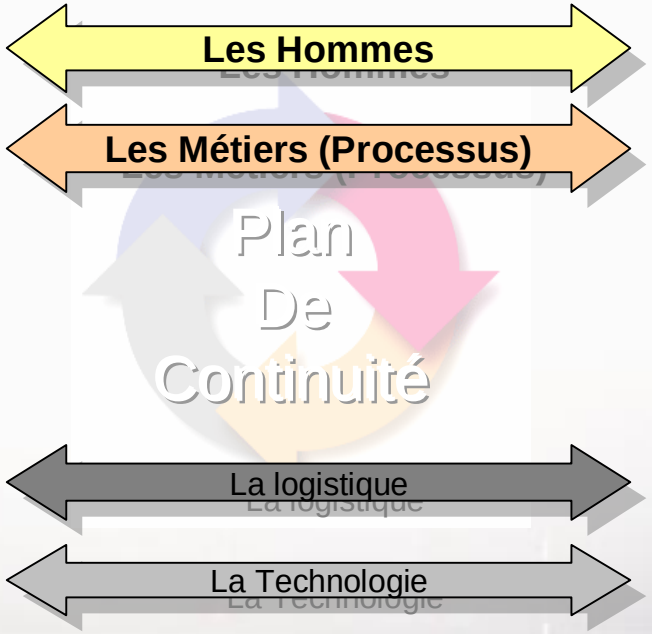
- Redémarrer
- Restaurer
- Revenir à la normale

Concerne :

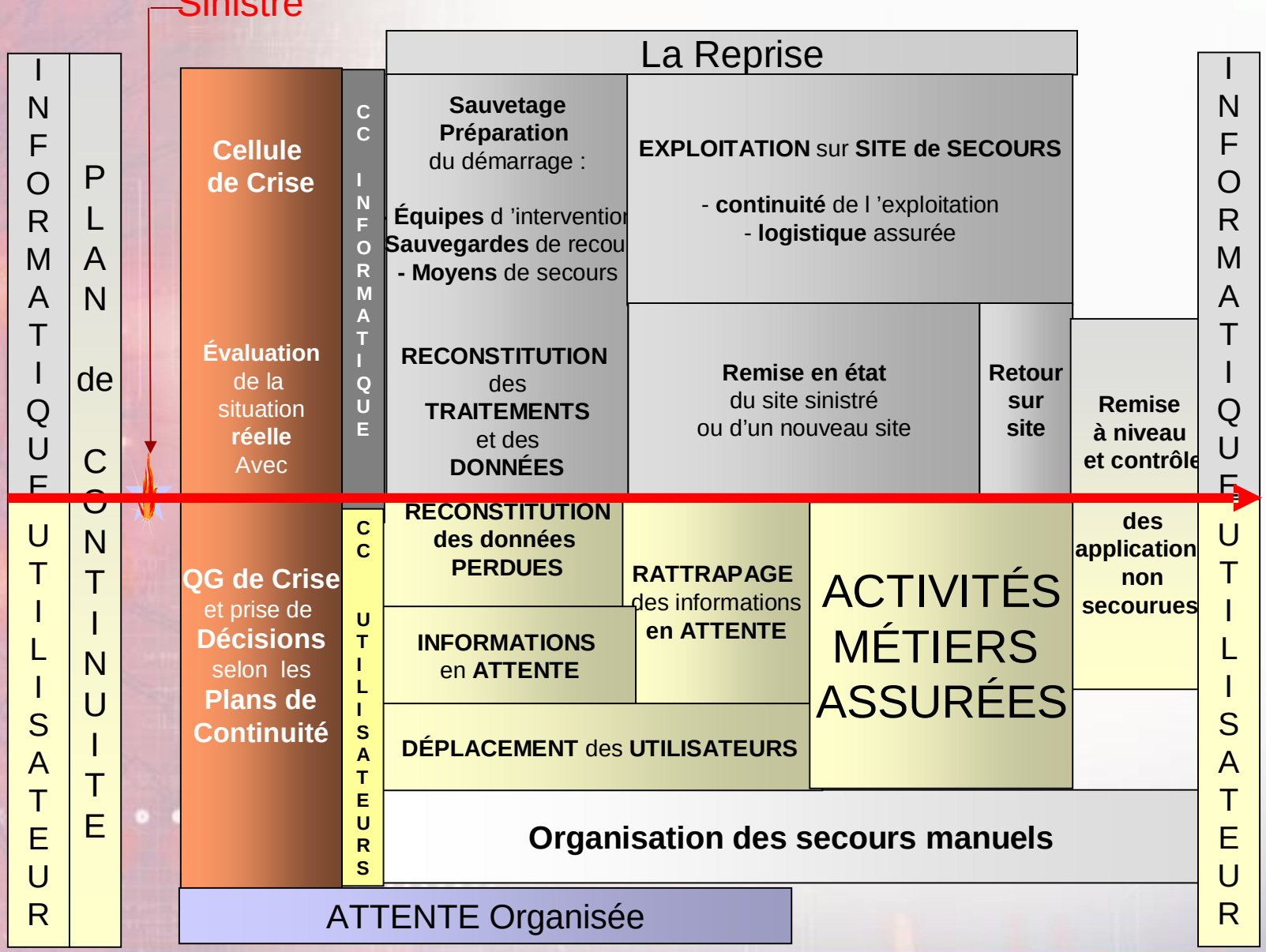
- Le personnel
- Les métiers
- La logistique
- La technologie

Nécessite :

- Anticipation
- Communication
- Évaluation permanente



# De Quoi s'agit-il ?



# Méthodologie de Conception

4 Phases :

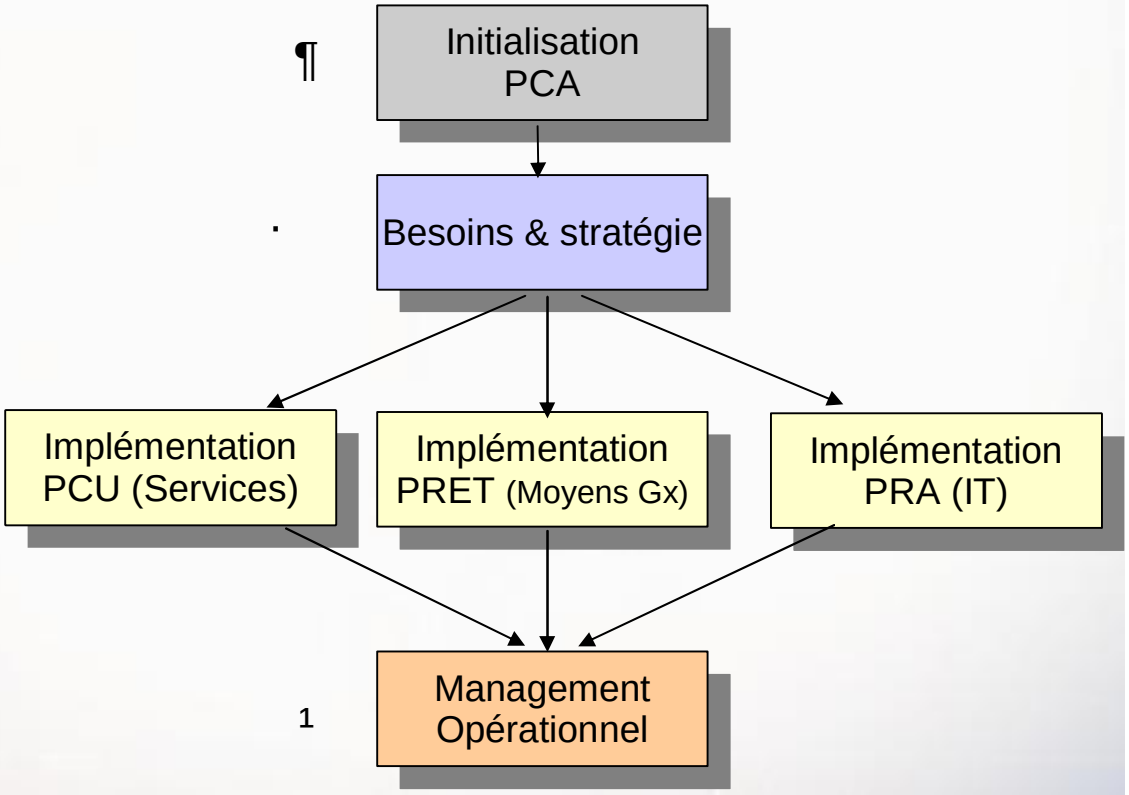
- ¶ Initialisation et Organisation
- Ë Analyse des besoins et stratégies ou BIA
- ¸ Implémentation
- 1 Management Opérationnel

3 Aspects :

**PCU** (plan de continuité utilisateurs) : La continuité de l'activité humaine et relationnelle

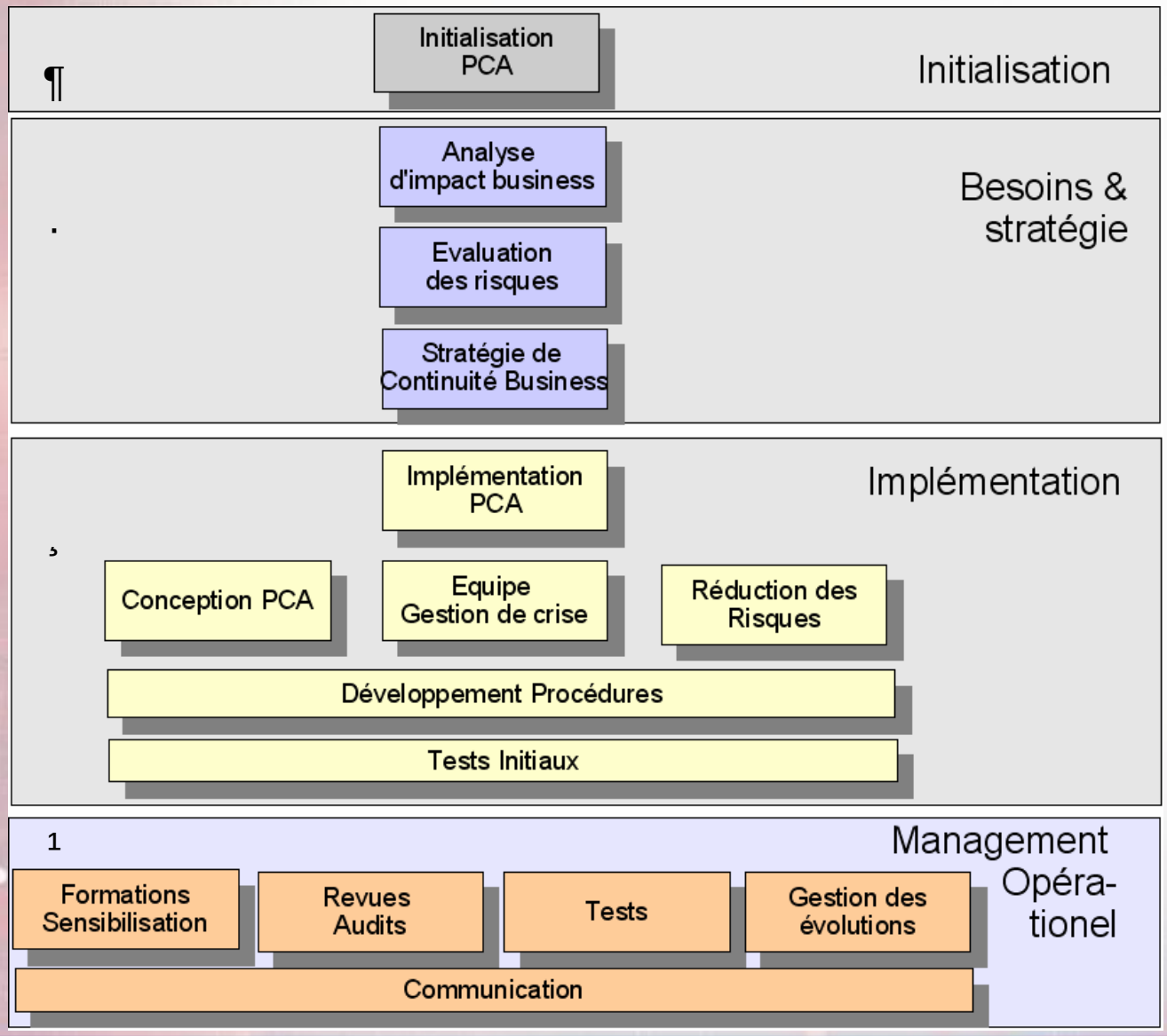
**PRET** (Plan de reconstitution de l'environnement de travail)

**PRA** (Plan de reprise d'activité IT) : La continuité des moyens technologiques notamment IT



CLUSIR Rhône Alpes

# Management de la continuité: Initialisation



# Principes de management

C'est un programme d'entreprise : il devra être managé comme projet continu, avec l'engagement de la direction générale, et l'information et la participation de tous les métiers,

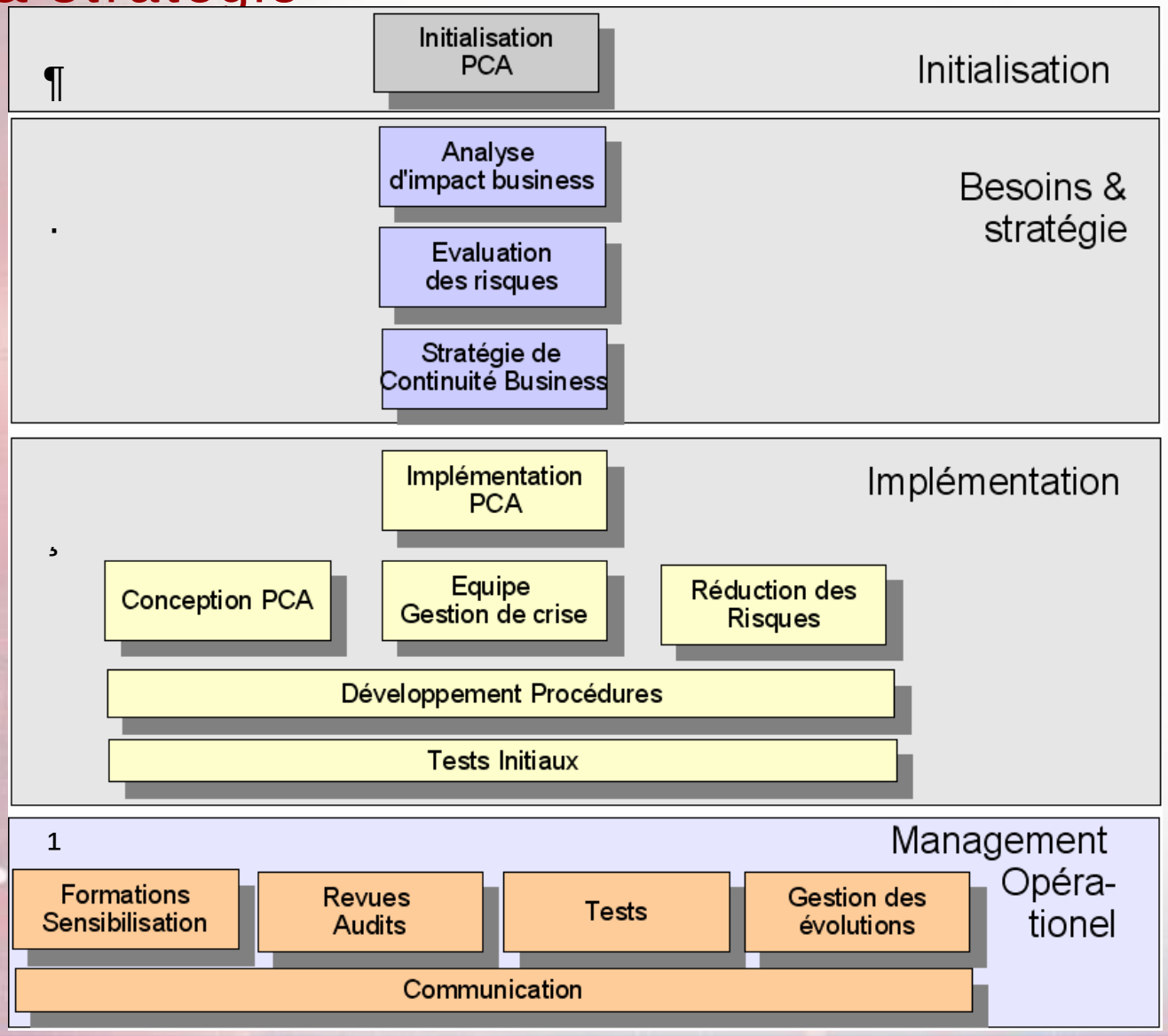
Un comité de pilotage et une structure de crise doivent être mis en place avec une définition claire des responsabilités et des processus d'escalade.

Il doit répondre à des objectifs d'entreprise : Ils seront généralement tournés vers la continuité de service aux clients et le respect des engagements pris auprès des actionnaires,

Les moyens (y compris informatiques) découleront des objectifs et non l'inverse,

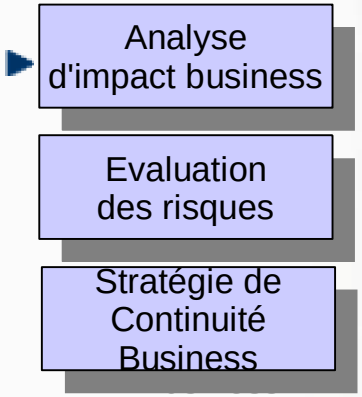
Il doit aboutir à des procédures opérationnelles claires, des modes opératoires connus, partagés par tous, et validés par des essais fréquents,

# Management de la continuité:
## Besoins & stratégie



# Besoins et Stratégie

## Analyse d'Impact



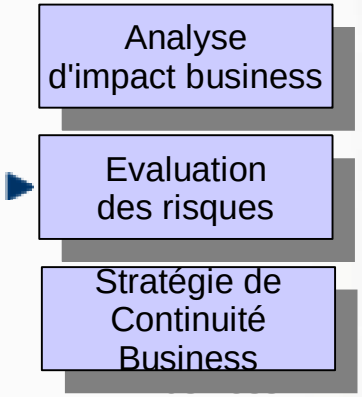

Obtenir une cartographie des activités et des processus associés, leur criticité pour le bon fonctionnement de l'entreprise, les priorités relatives face à une indisponibilité soudaine.

Recueillir auprès des responsables métiers les informations relatives aux temps maximum d'indisponibilité tolérables,

Recueillir toutes informations permettant de faire des choix quant aux meilleures stratégies pour assurer la continuité de ces fonctions ou processus,

Déterminer les facteurs internes ou externes susceptibles de concourir à l'atteinte des objectifs de reprise dans les meilleurs conditions de délais et de prix.

# Besoins et Stratégie
## Évaluation des risques




- Analyse des risques et des impacts business
- Analyse des contraintes légales liées à la reprise d'activité de certain secteur (finance par exemple),
- Analyse comparative des diverses alternatives de stratégie de continuité de service,
- Analyse coûts/bénéfices et choix de la stratégie
- Mise en place d'un contrôle budgétaire propre au plan de reprise.

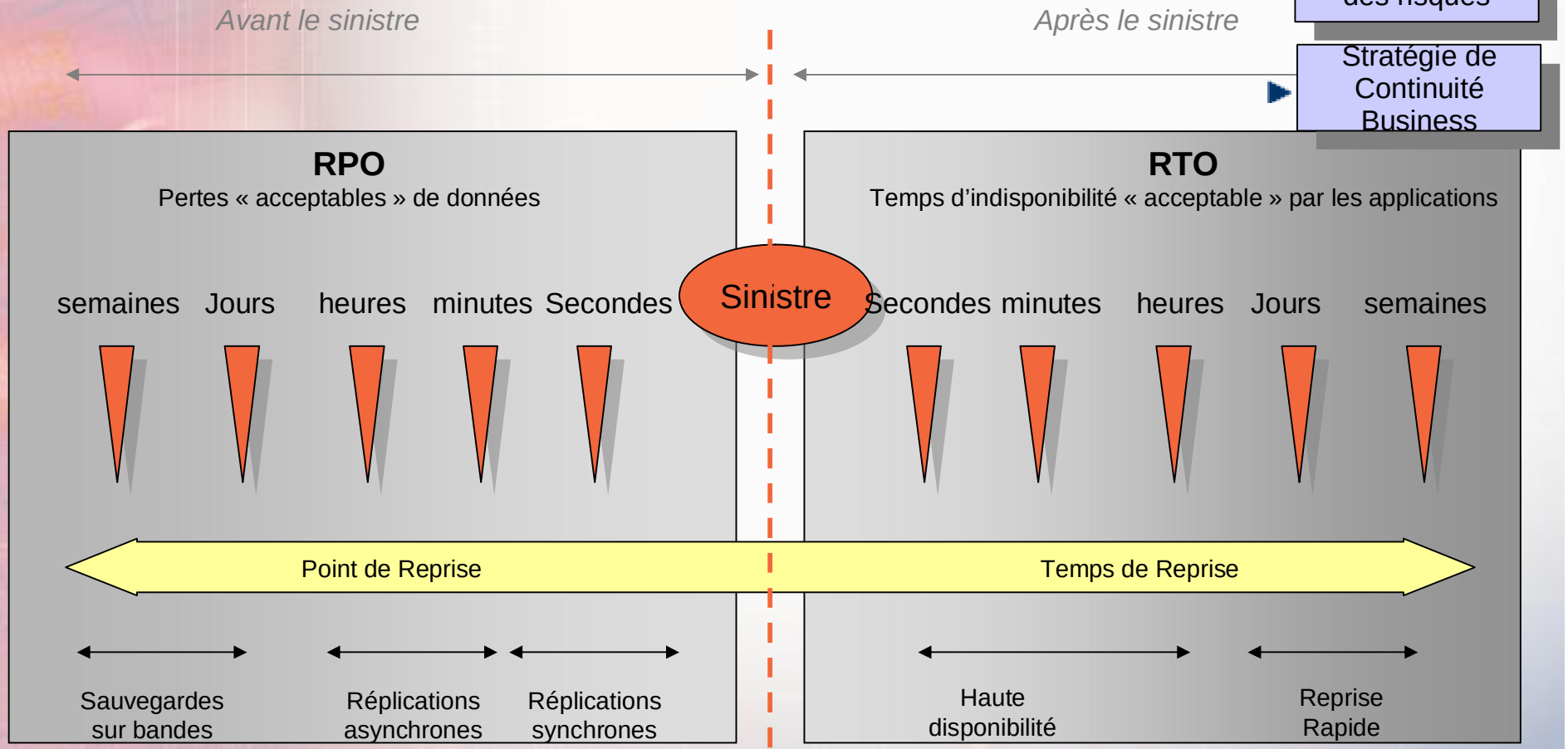
CLUSIR Rhône Alpes

# Définition du RPO et RTO « acceptables » pour chacune des applications concernées

Analyse d'impact business

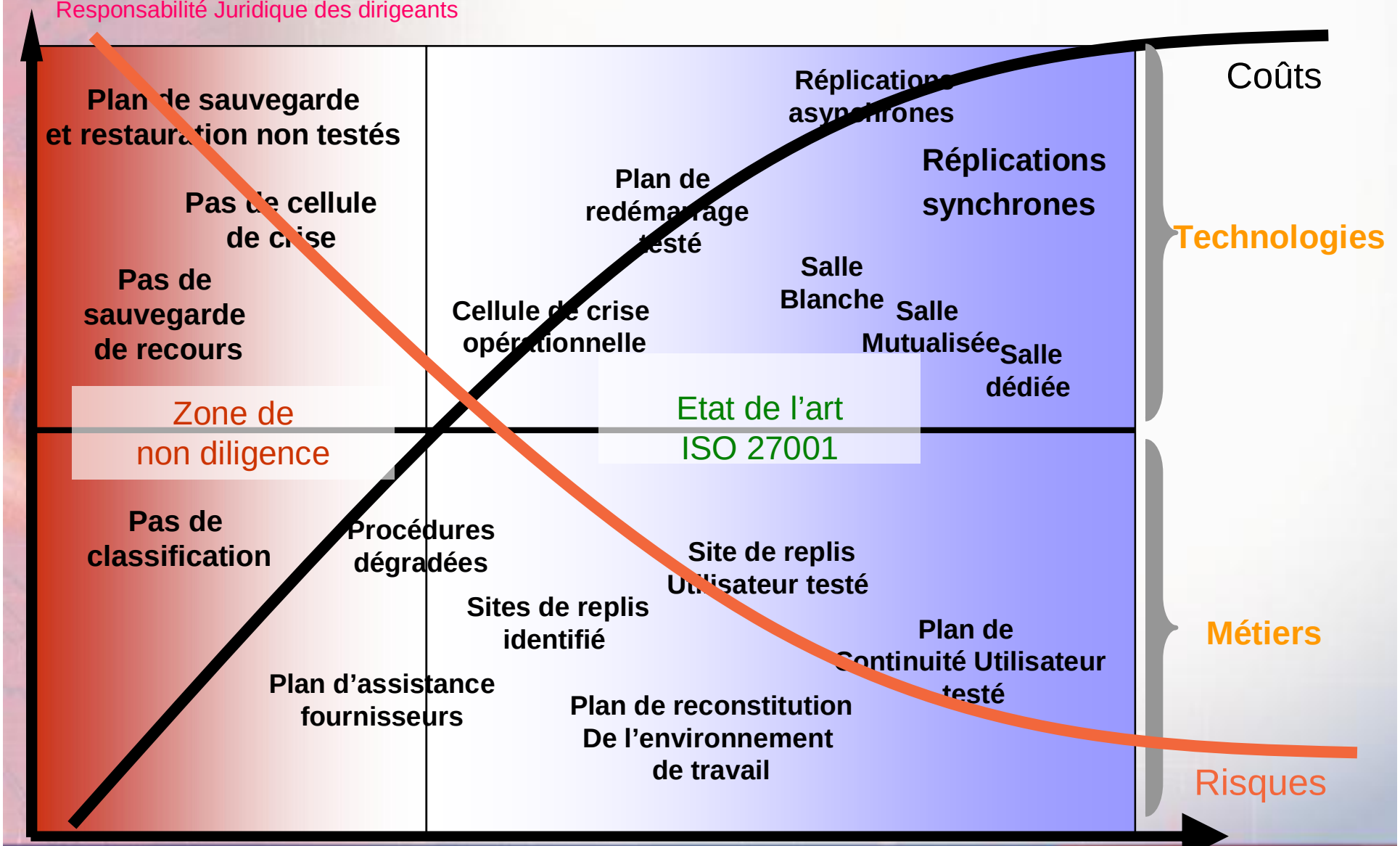
Evaluation des risques

Stratégie de Continuité Business

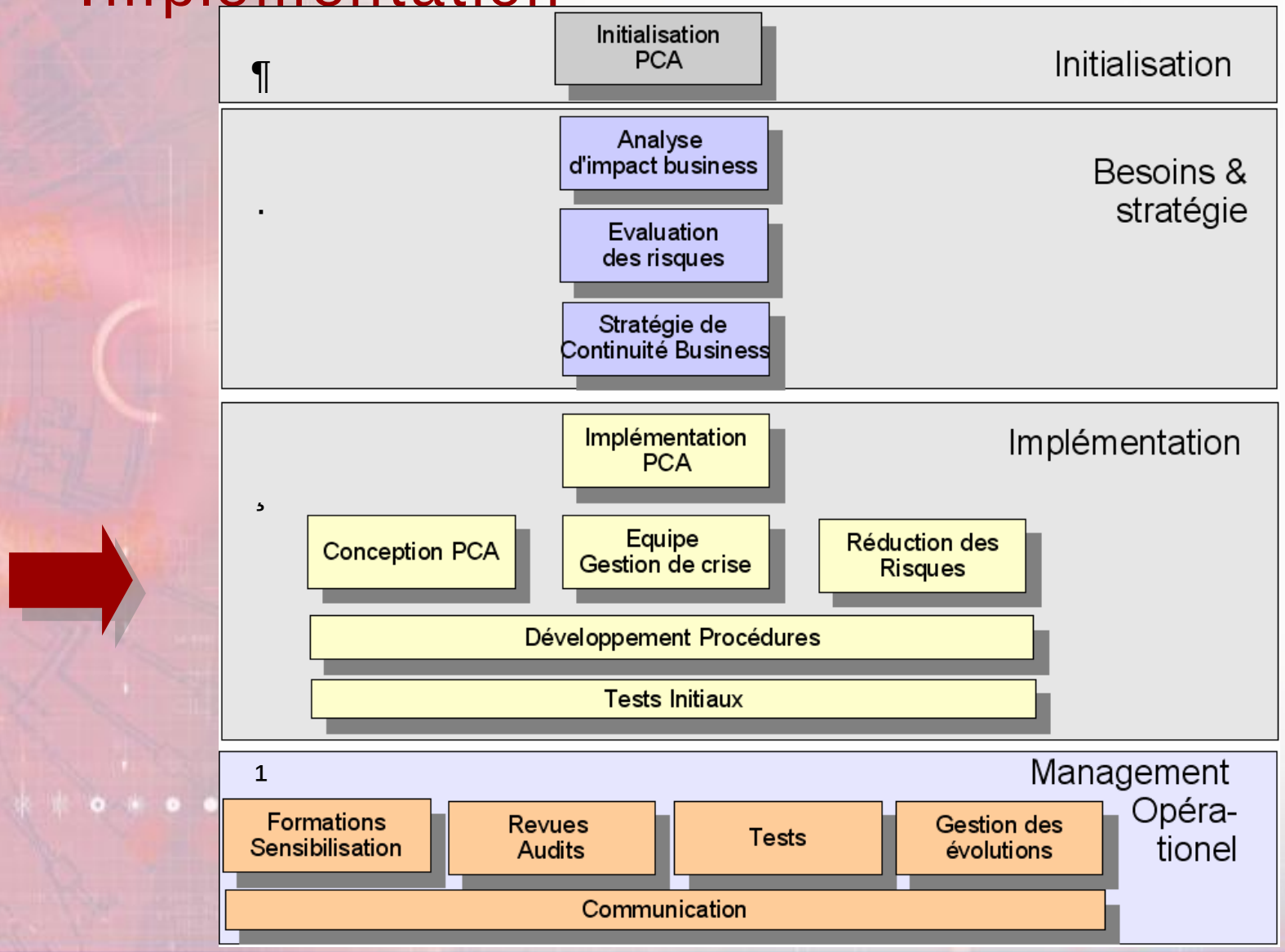


# Continuité d'activité :à quel prix ?

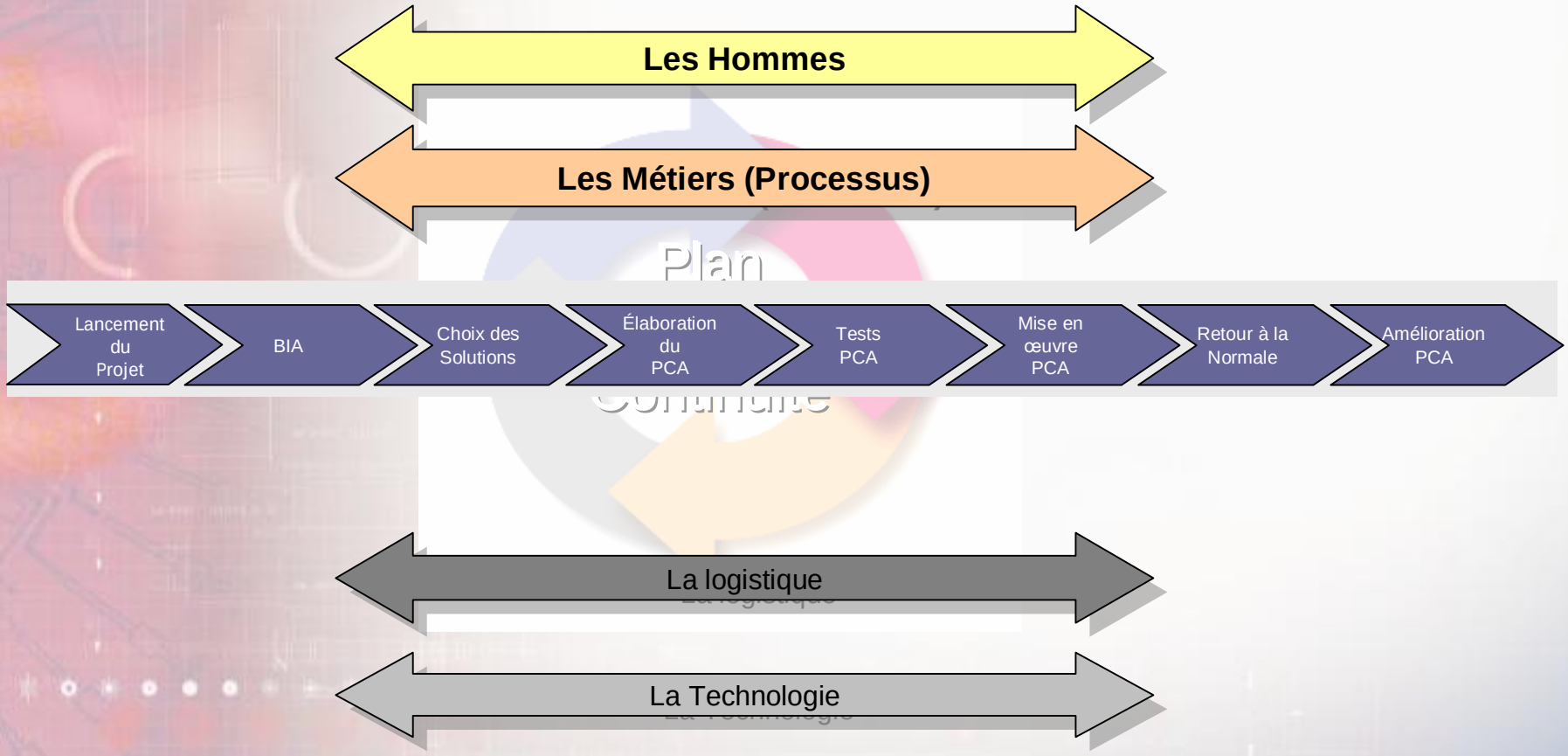
CLUSIR Rhône Alpes



# Management de la continuité: Implémentation

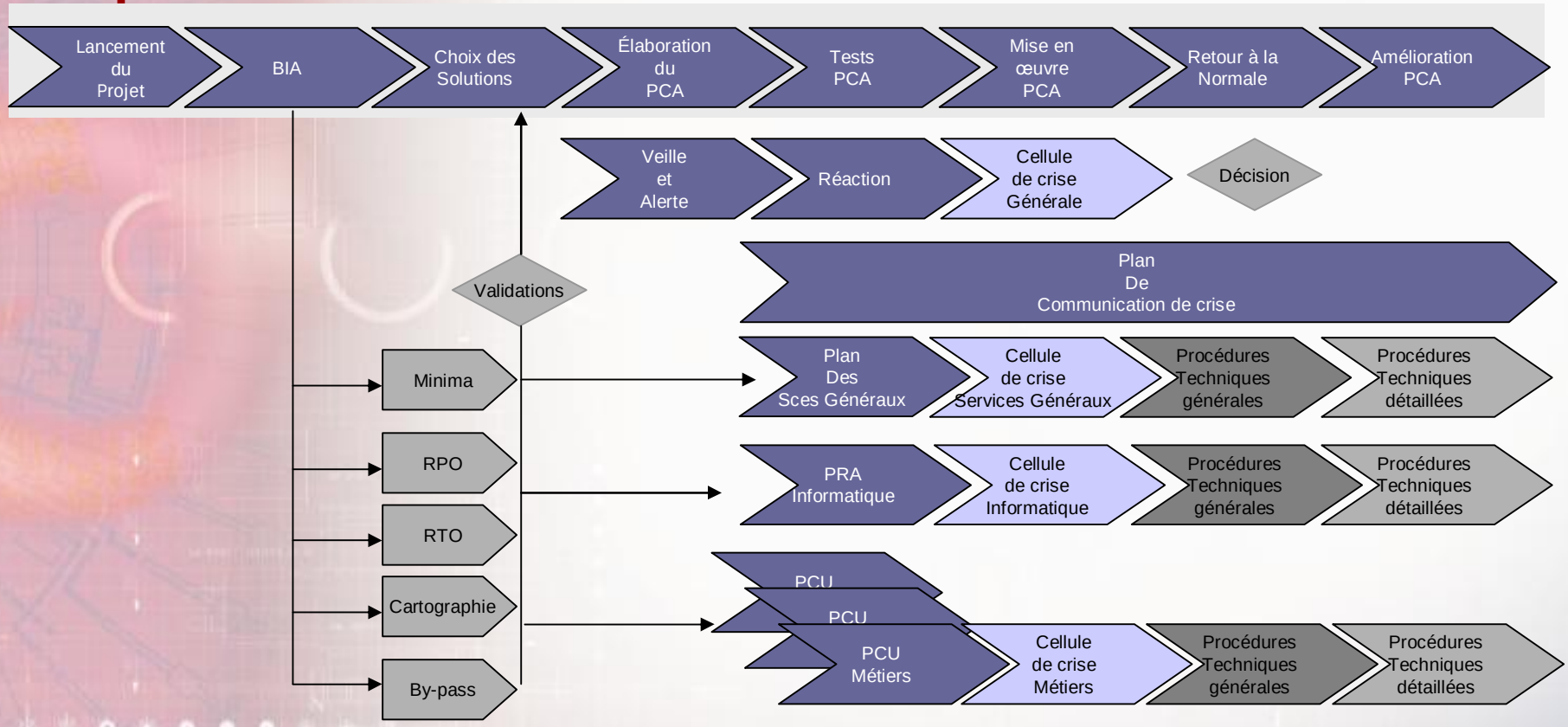


# Une Méthodologie d'Implémentation



CLUSIR Rhône Alpes

# Un assemblage ordonnancé de procédures



CLUSIR Rhône Alpes

# Développement du PRA


Le PRA est élaboré comme un projet dont l'ambition est de respecter lors des tests les contraintes RTO.

La réussite du PRA dépend de l'anticipation

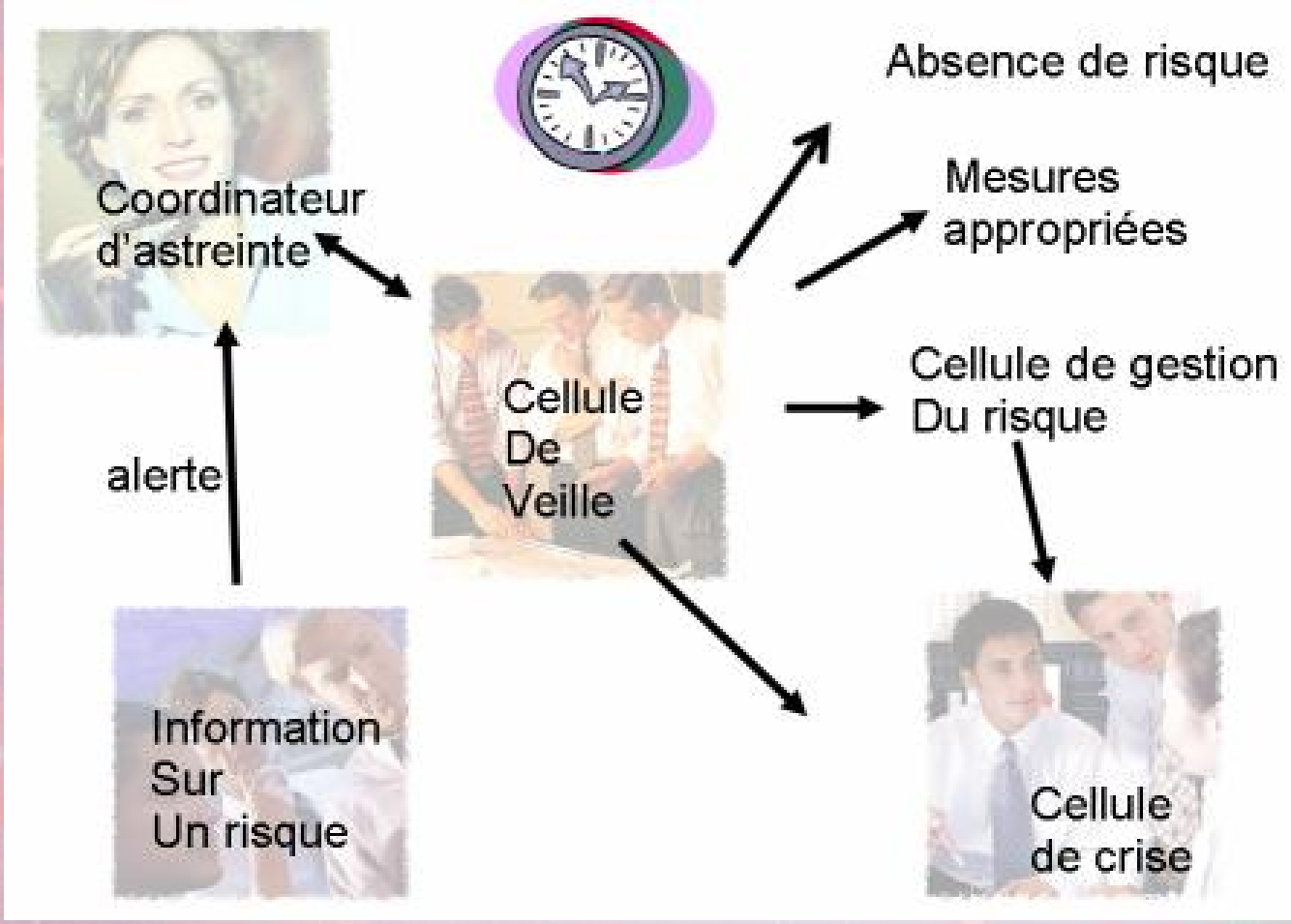
L'anticipation est traduite par des procédures écrites et ordonnancées

# Management Opérationnel

- Structure de veille
- Cellules de crise
- Communication de crise
  - Interne
  - Externe

CLUSIR Rhône Alpes

# De la Veille à la Crise
# rôle des cellules de crise



# Cellules de crise

Importance du coordinateur d'astreinte

La cellule de veille permets la détection et l'escalade

La cellule de crise Générale va permettre l'analyse des premières informations et prendre la décision de partir (ou non) en secours

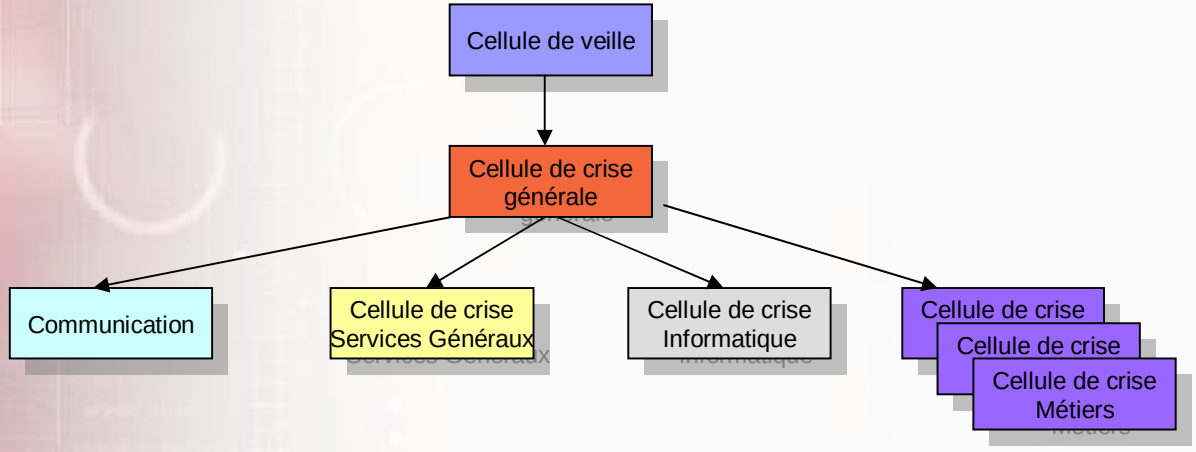
Les autres cellules de crise :

- CCMG : Moyens généraux
- CCI : Informatique
- CCM : Métiers
- CCC: Communication

Seront activées en fonction du diagnostique de la cellule de veille et de la typologie de la crise.

CLUSIR Rhône Alpes

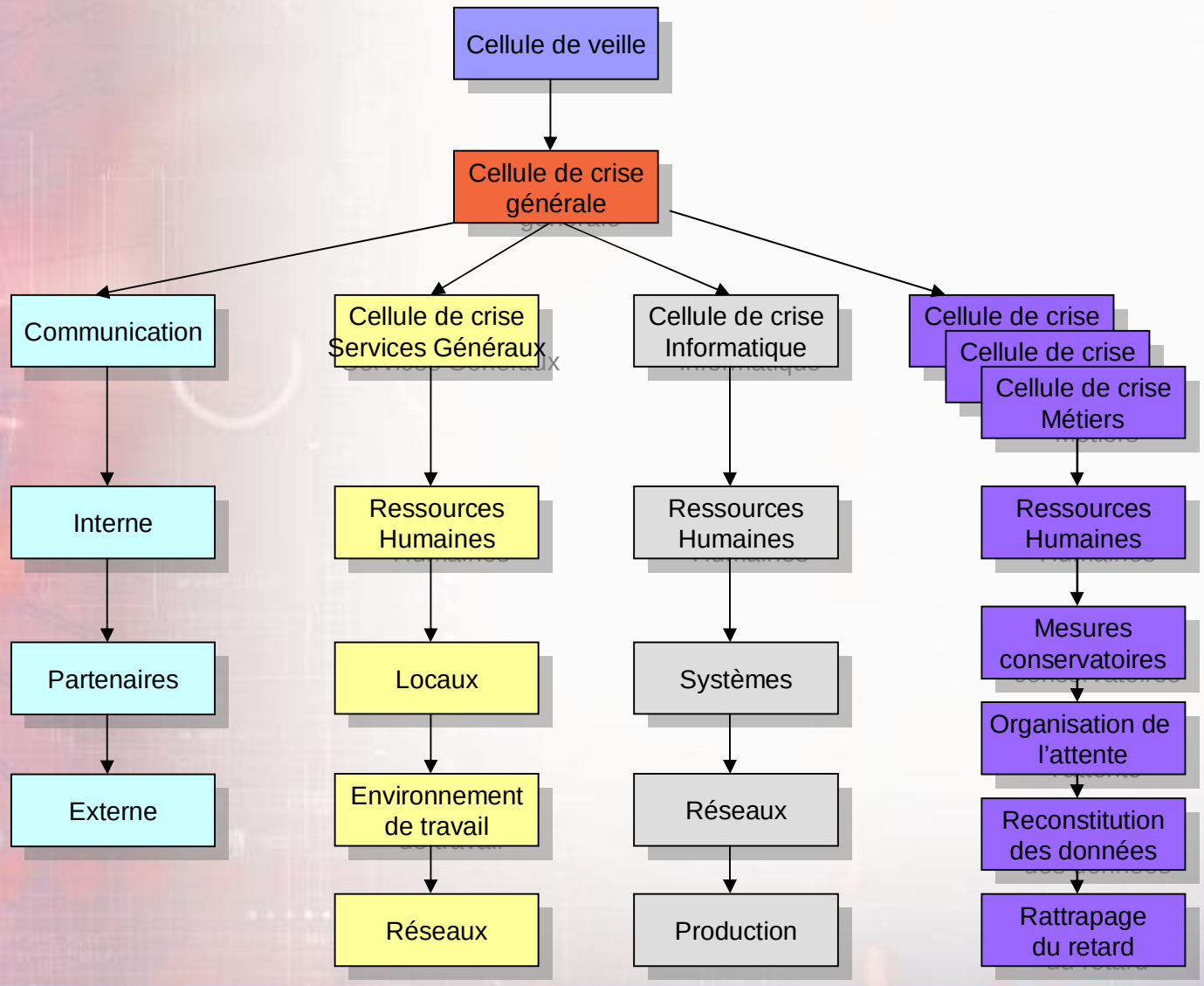
# Organisation de crise



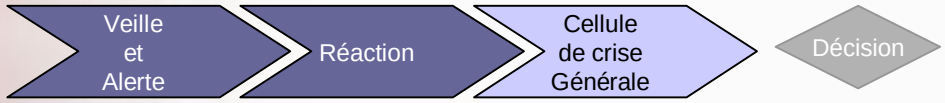
# Organisation de la cellule de crise

Directeur : il décide et conserve du recul
Directeur Adjoint : il dirige les opérations
Historien : il note les opérations
Secrétariat : Coordonne/filtre Standard & Fax
Logistique de la cellule : fournit les moyens
Responsable technique/ sécurité : L'expertise technique
Coordination interne :liaison filiale groupe)
Communication (Interne/externe)
Experts support

# Organisation de crise



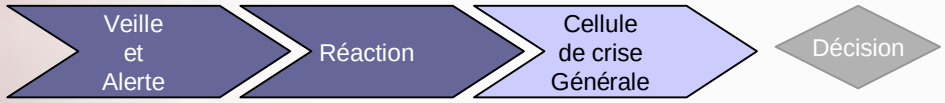
# Veille & alerte




Liste des Procédures :

- Organisation de la veille
- Détection du sinistre
  - De jour
  - De nuit Week-end et jours fériés
- Constat du sinistre

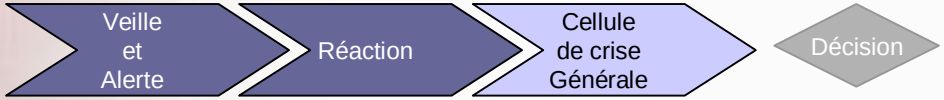
# Réaction




Liste des procédures :

- Appel des autorités extérieures,
- De jour
  - Évacuation des locaux,
  - Regroupement des personnels,
- Attente de l'intervention des autorités externes,
- Réception des comptes-rendus des autorités externes,
- Pré communication cellule de crise,
- Pré communication Directions Métiers,
- Estimation des dégâts liés aux systèmes d'information,
- Estimation de l'indisponibilité.

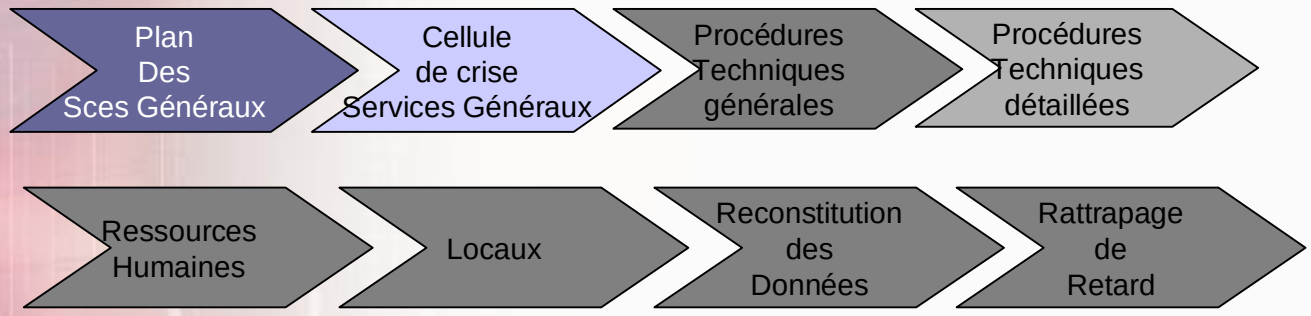
# Réaction & Cellule de Crise générale




Liste des procédures :

- Désignation du lieu de RV de la Cellule de Crise Générale,
- Appel des membres de la Cellule de Crise Générale,
- Préparation de l'ordre du jour,
- Attente réunion de crise,
- Envoi des fax de lancement du replis,
- Convocation des cellules de crise Métiers,
- Convocation de la cellule de crise Services Généraux,
- Convocation de la cellule de crise Informatique,
- Avis aux partenaires (hébergeurs, sous-traitants, ...)

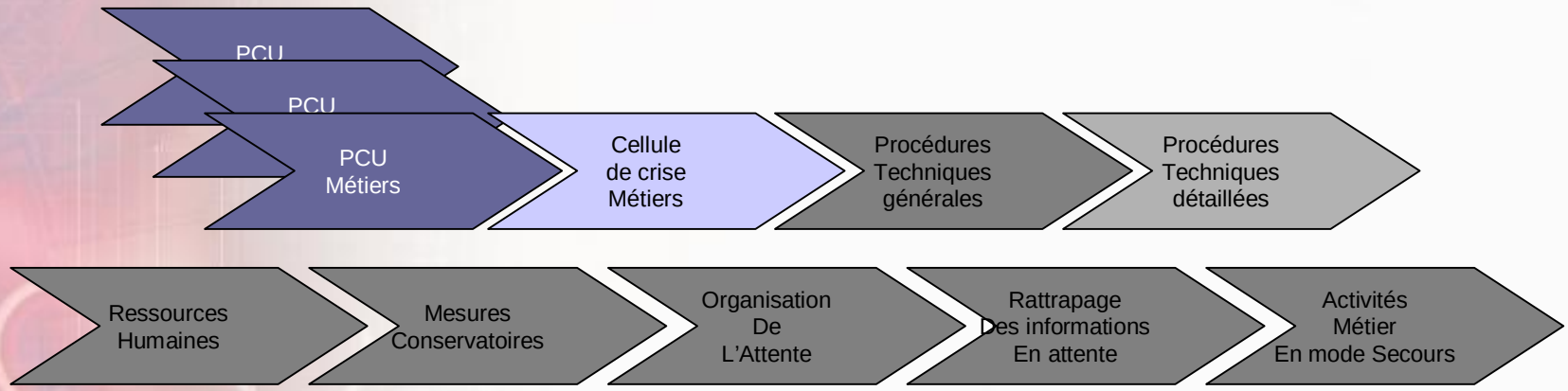
# Plan de Reconstitution de l'Environnement de Travail




Liste des procédures du P.R.E.T.:

- Réquisition des moyens et locaux,
- Réquisition des moyens de reconstitution de l'environnement de travail,
- Organisation des conditions d'exploitation,
- Organisation de nouveaux moyens généraux :
  - Communication,
  - Courrier,
  - Éditique,
  - Etc....
- Organisation du retour à une situation normale des moyens généraux.

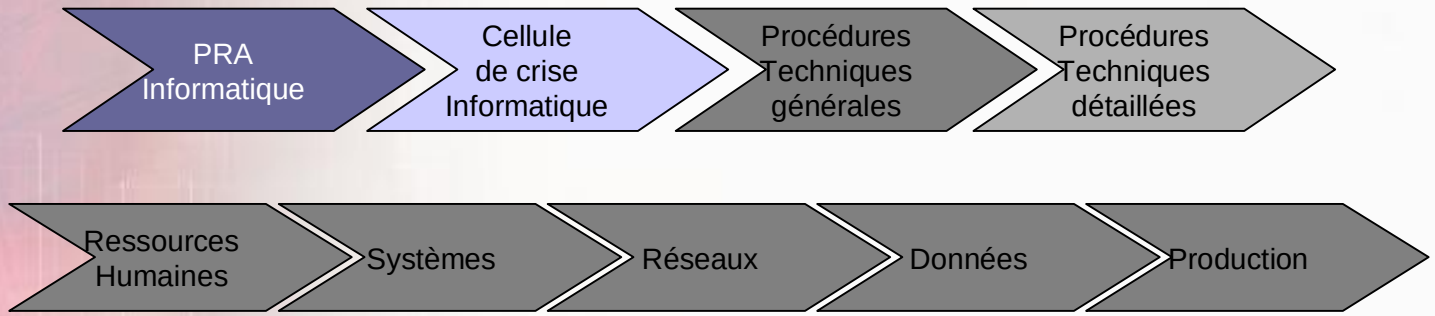
# Plan de Continuité Utilisateurs




Liste des procédures du PCU :

- Procédures d'organisation générale et logistique en liaison avec le PRET,
- Procédures de déplacement des utilisateurs,
- Procédures exceptionnelles concernant les mesures conservatoires et d'organisation « intelligente » de l'attente,
- Procédures de rattrapage des retards,
- Procédures de travail en mode dégradé,
- Procédures de retour à une situation normale.

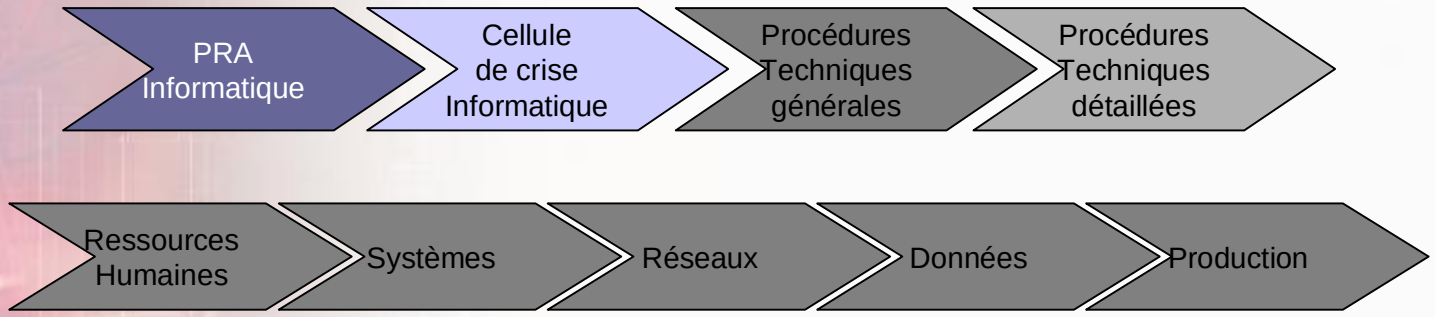
# PRA Informatique 1/2




Liste des procédures du PRA Informatique :

- Activation du plan de reprise d'activité informatique,
- Récupération de la documentation de secours
- Transfert des personnels sur site de secours,
- Si Secours sans réplication :
  - Récupération des sauvegardes de recours,
  - Mise à disposition de la configuration de secours,
  - Restauration des environnements Systèmes et Paramètres Réseau,
  - Restauration des Données.
- Si Secours avec réplication :
  - Procédures de bascule (systèmes, données)

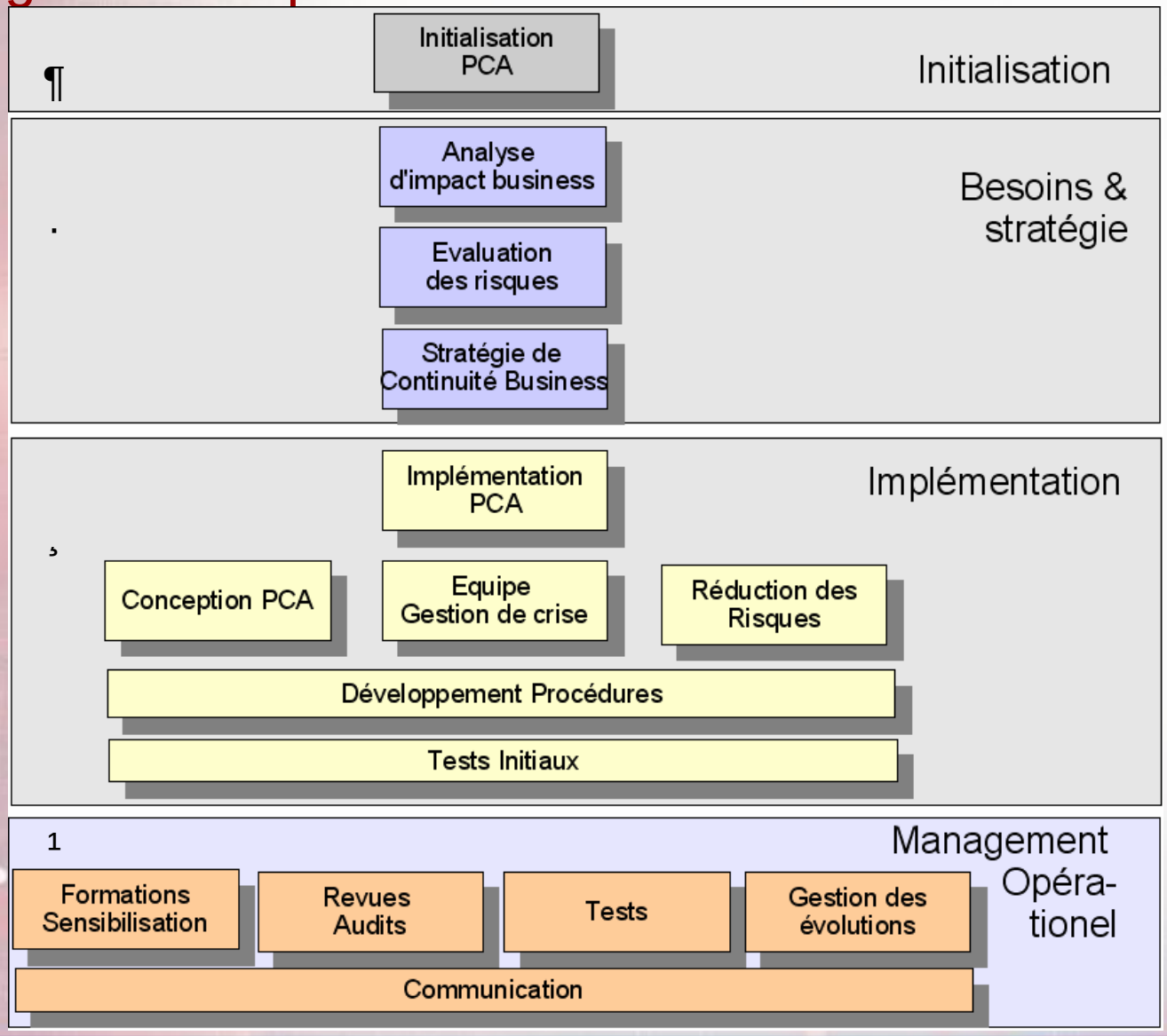
# PRA Informatique 2/2




Liste des procédures du PRA Informatique (suite):

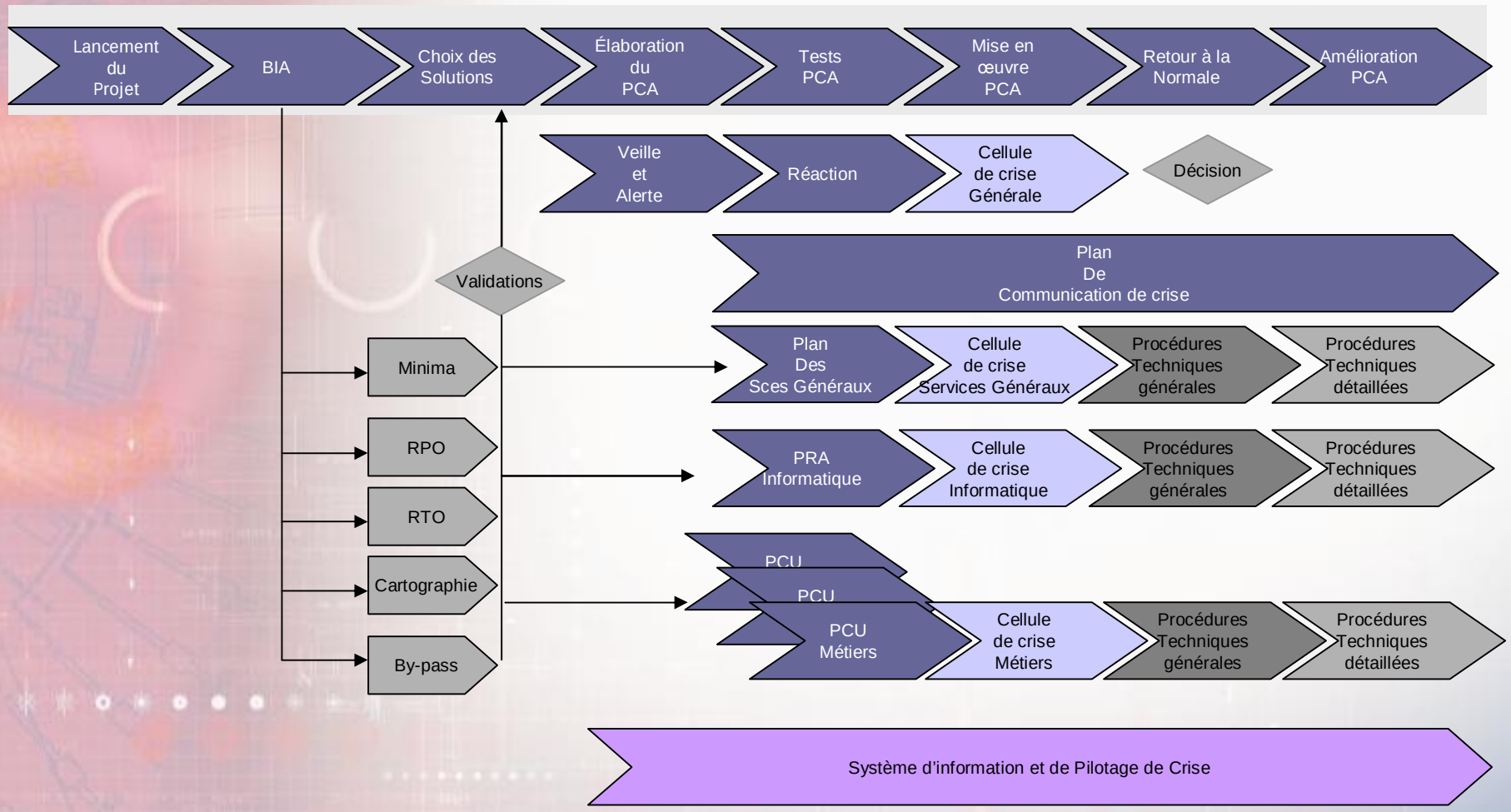
- Ajustements concernant les données (Cohérence),
- Tests et validations utilisateurs,
- Ouverture du réseau,
- Lancement de la production en secours,
- Tâches liées au retour à un environnement de production normal.

# Management de la continuité: Management Opérationnel



CLUSIR Rhône Alpes

# Conduite Opérationnelle « Clé(USB) en main »

# Conduite des plans de continuité :

## Le système d'information d'aide au management de crise :

Suivi opérationnel de l'enchaînement des tâches





Système Documentaire des procédures Avec Hyperliens

# Typologie de la documentation

Annuaires, Listes,
- Documents de type Excel

Plans d'accès, copies de contrats, schémas, cartographie,...
- Documents de type multimédia (Mappy ou Via Michelin)
- Documents de type Visio

Documents pré formatés
- Fax, Mails, Messages de communication, ordres du jour...

Outil de pilotage et de suivi des tâches et du timing
- Gantt de type MS Project

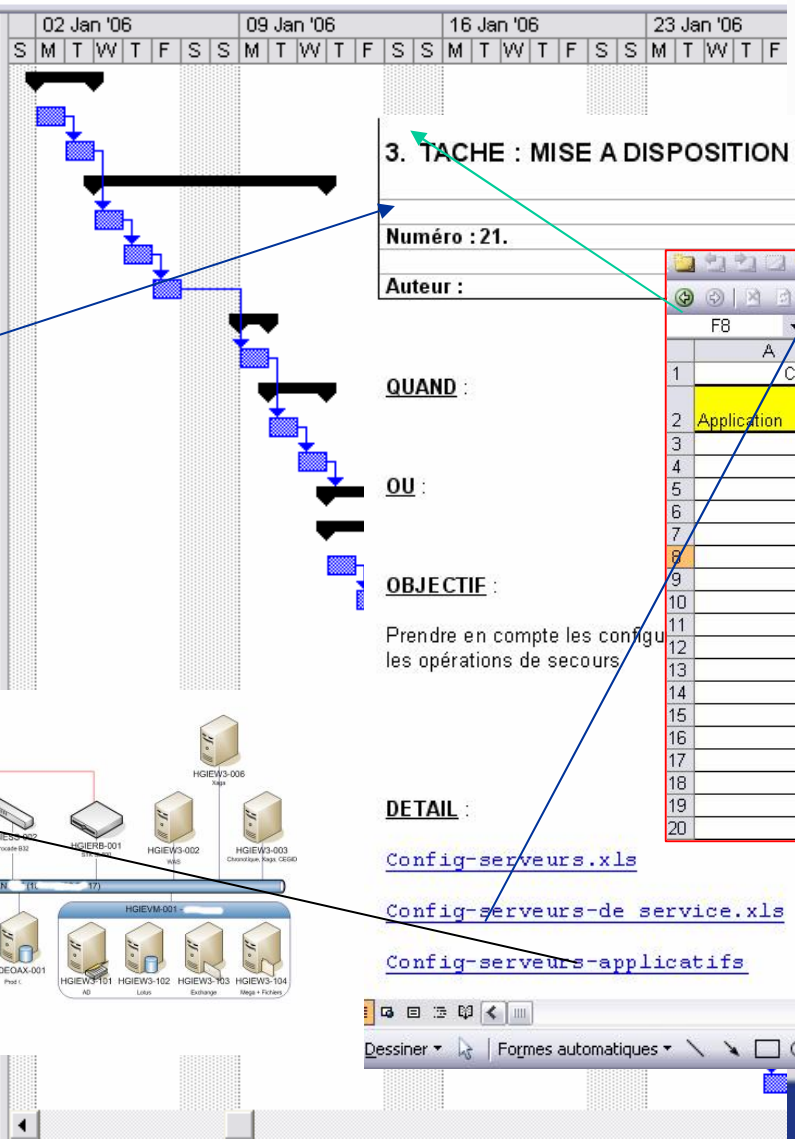
Procédures
- Procédures générales documents de type Word ou Txt
- Procédures détaillées: celles habituellement mises à jour dans les dossiers d'exploitation

Documents de gestion et de contrôle du plan de secours

CLUSIR Rhône Alpes

# Exemple

| | Task Name |
|---|---|
| 1 | – **Décision de back-up** |
| 2 | Récupération du back-up book |
| 3 | Appel équipe de back-up |
| 4 | – **Arrivée équipe de back-up** |
| 5 | Confirmation du besoin ausite secours |
| 6 | Arrêt trait.si possible |
| 7 | Messages aux utilisateurs |
| 8 | – **Organisation equipes back-up** |
| 9 | Constituion équipes |
| 10 | – **Récupération des sauvegardes** |
| 11 | Envoi du fax de convoyage |
| 12 | Convoyage des supports |
| 13 | – **Mise à Disposition de la configuration** |
| 14 | – **Avis d'arrivée sur site secours** |
| 15 | Liste du personnel déplacé |
| 16 | Envoi du fax des personnels dép |
| 17 | Préparation n° F.Télécom |
| 18 | Avis aux sociétés de service |
| 30 | Information 1 CC |




**3. TACHE : MISE A DISPOSITION DE LA CONFIGURATION**

**Numéro : 21.** **RESPONSABLE : Centre de BUP**

**Auteur :**

**QUAND** :

**OU** :

**OBJECTIF** :

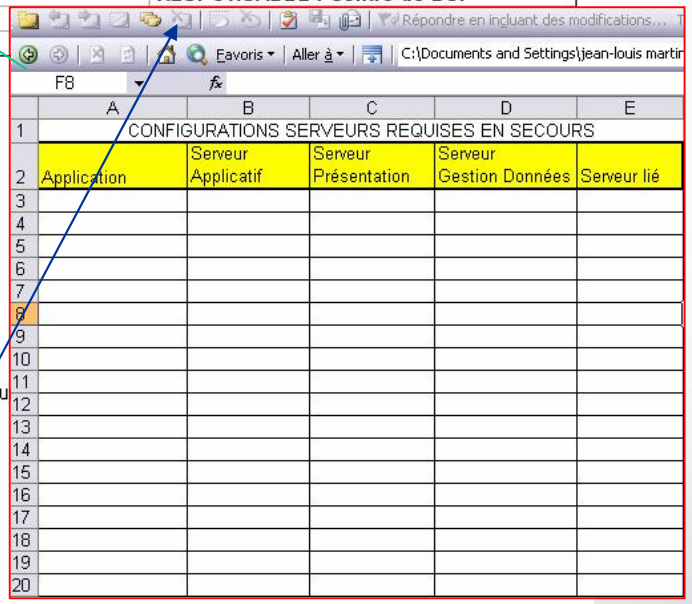
Prendre en compte les configu
les opérations de secours

**DETAIL** :

Config-serveurs.xls

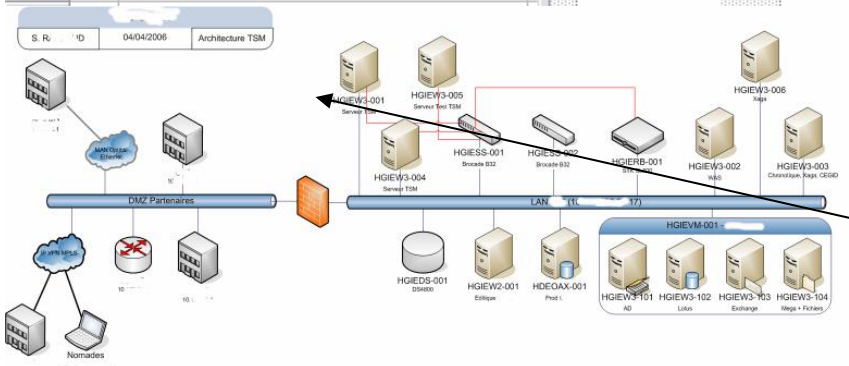
Config-serveurs-de service.xls

Config-serveurs-applicatifs



CONFIGURATIONS SERVEURS REQUISES EN SECOURS

| Application | Serveur Applicatif | Serveur Présentation | Serveur Gestion Données | Serveur lié |
|---|---|---|---|---|




CLUSIR Rhône Alpes

# Liens utiles

CLUSIF Plan de Continuité d'Activité : https://www.clusif.asso.fr/fr/production/ouvrages/pdf/PlanContinuiteActivite.pdf

BCI (business continuity Institute) et son Good Practice Guideline : http://www.thebci.org/goodpracticeguidetoBCM.pdf

E&Y Continuité d'activité : http://www.ey.com/global/Content.nsf/France/issues_perspectives_SI_continuite_activite

PAS 56 un Quasi-Standard du BSI : http://www.bsi-global.com/Risk/BusinessContinuity/PAS56.xalter

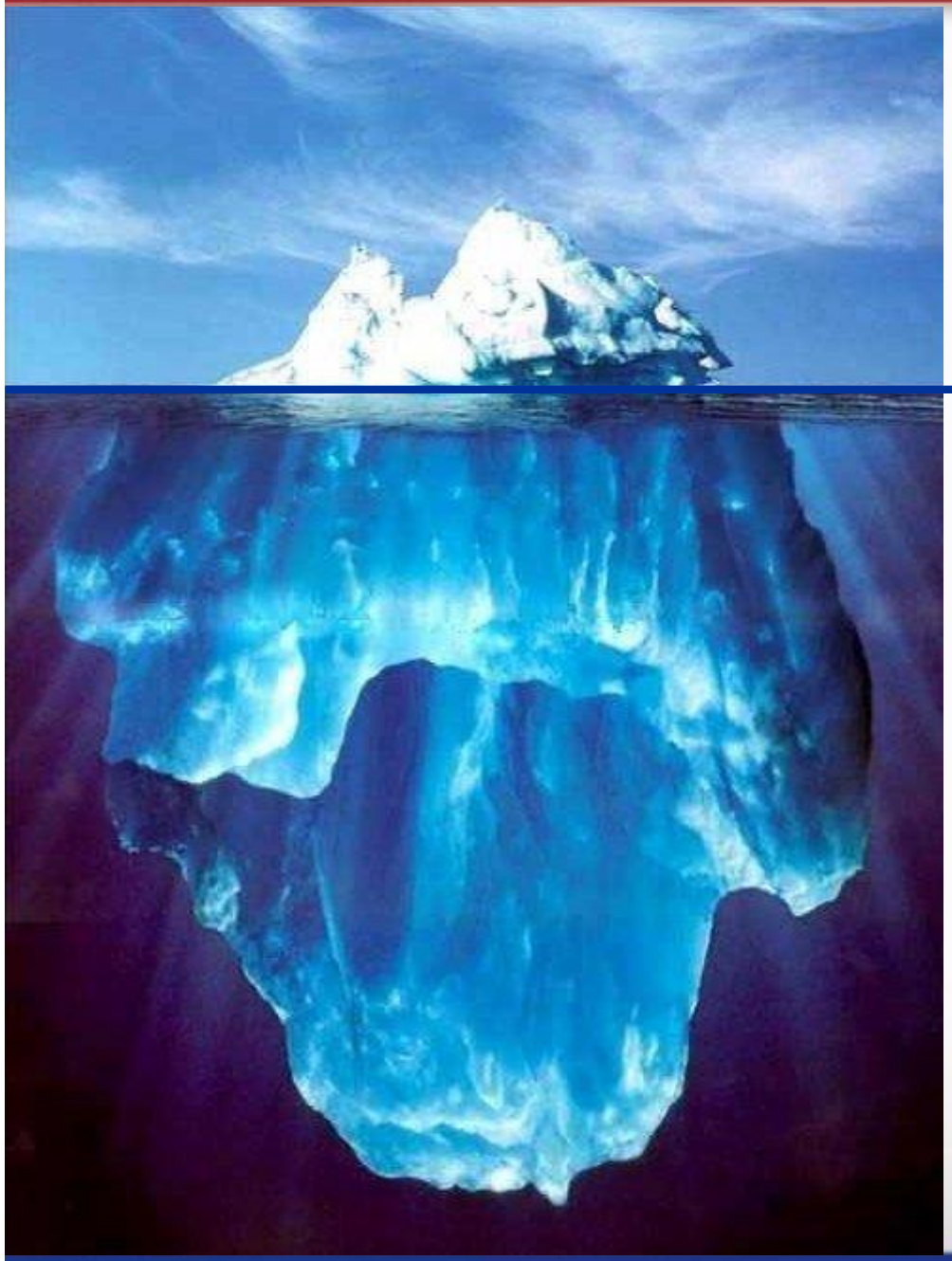
EMC² Today's Choice for buiness continuity : http://www.emc.com/ilm/pdf/H1307_BusContinuity_web.pdf

VMware : Solutions pour Continuité d'activité : http://www.vmware.com/fr/solutions/continuity/

Gestion de crise : http://www.patricklagadec.net/fr/

Gestion de crise : (Dr JM Guillery) :http://www.gestiondecrise.com

Communication de crise & sensible : http://www.communication-sensible.com



CLUSIR Rhône Alpes

SSI Conseil

Sécurité des Systèmes d'Information

Jean-Louis MARTIN

« parce que la sécurité n'est pas une technologie mais un processus »*

www.ssi-conseil.com

# Merci de votre attention

* Bruce Schneier

# Pourquoi un PCA ?

Satisfaire aux obligations légales et réglementaires,

Réduire le délai nécessaire à la restauration des tâches essentielles,

Garder son positionnement concurrentiel en diminuant l'impact d'un incident majeur,

Rassurer les clients, les fournisseurs,

Utiliser le plan comme un argument commercial pour les clients,

Améliorer la sécurité et l'engagement des salariés,

Limiter le coût d'un sinistre, maîtriser les coûts de reprise,

Permettre un retour «à la normale » plus rapidement possible,

Obtenir des remises sur les contrats d'assurance.

# Les facteurs clés de succès d'un projet PCA

- Implication forte de la Direction générale,
- Le Responsable Sécurité, rattaché à la DG est responsable du projet,
- Reporting régulier en relation avec les Directions Opérationnelles,
- DG + DO + RS arbitrent et valident le plan,
- Maintenance permanente,
- Tests réguliers,
- Communication élaborée.