HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

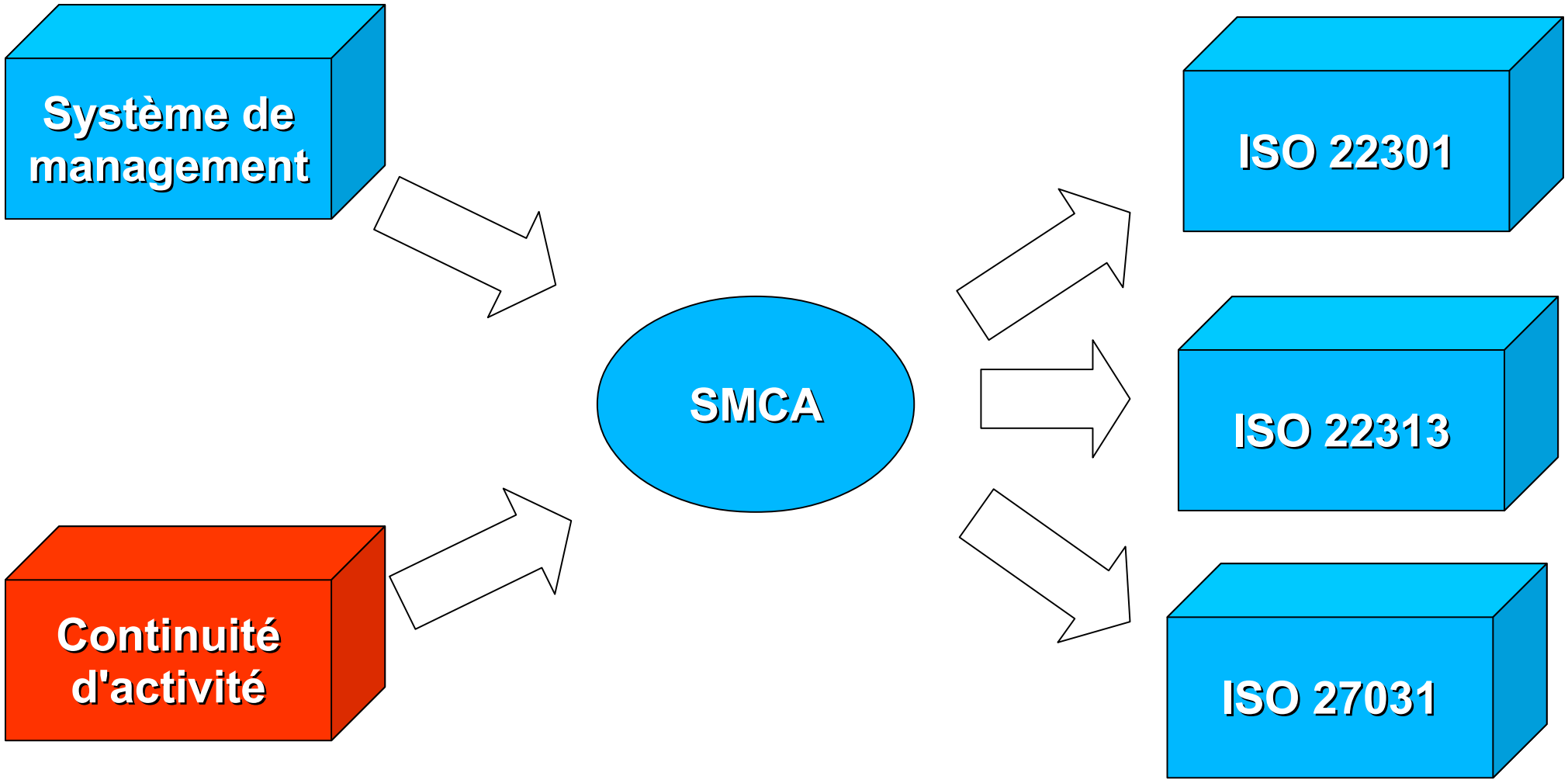
Norme ISO 22301

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

ADIM - Associations des directeurs informatiques de Monaco
Vendredi 22 mars 2013

Thomas Le Poetvin
Hervé Schauer

Introduction



Continuité d'Activité : définitions

- Plan de Continuité d'Activité (PCA)
  - Ensemble de **mesures** visant à assurer, selon divers **scénarios de crises**, y compris face à des chocs extrêmes, le maintien, le cas échéant de façon **temporaire** selon un **mode dégradé**, des **prestations** de services **essentielles** de l'entreprise, puis la **reprise** planifiée des activités (CRBF 2004/02)

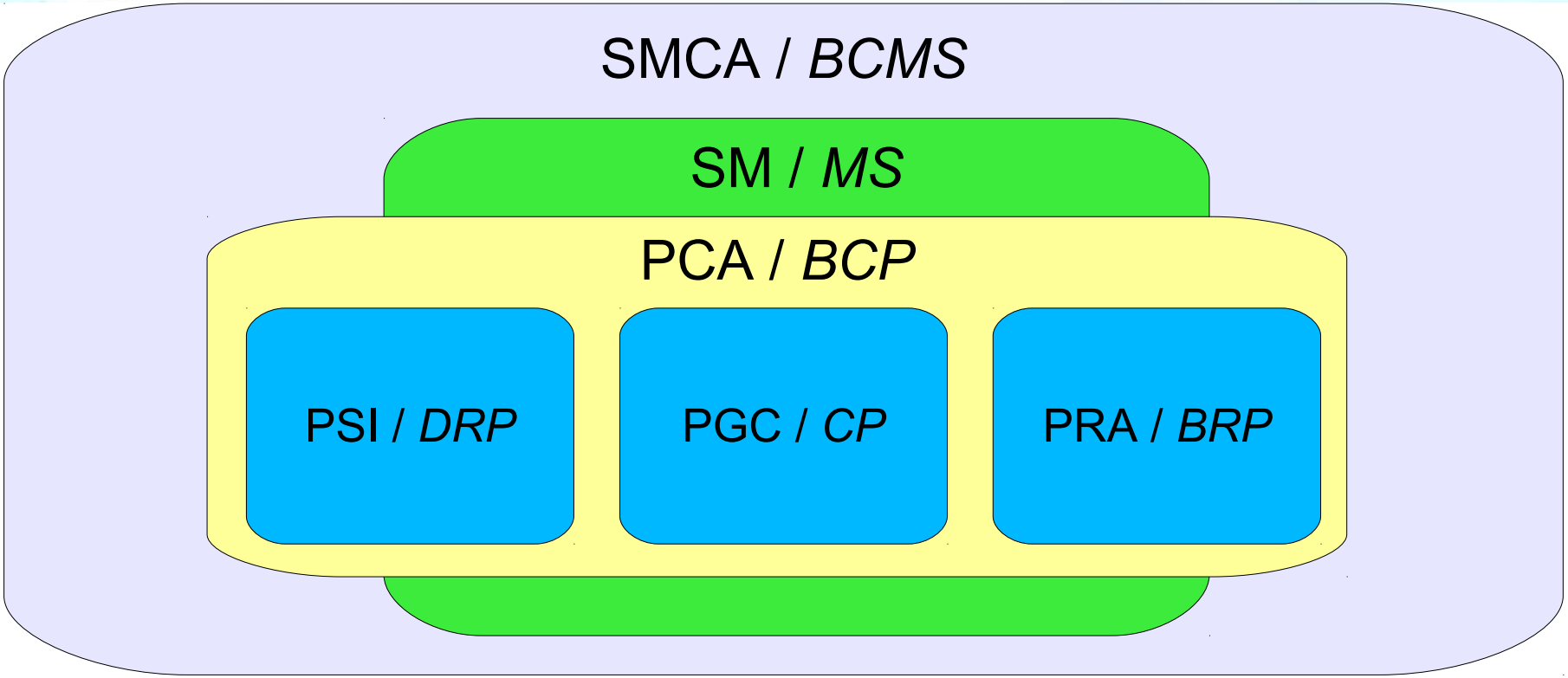
  - Procédures documentées servant de guide aux organisations pour répondre, rétablir, reprendre et retrouver un niveau de fonctionnement prédéfini à la suite d'une interruption (ISO 22301 3.6)

Continuité d'Activité : définitions

- Plan de Secours Informatique (PSI)
  - Ensemble des procédures et dispositions pour garantir à l'entreprise la reprise de son système informatique en cas de sinistre. Sous-ensemble du PCA qui couvre les moyens informatiques et télécoms (AFNOR)

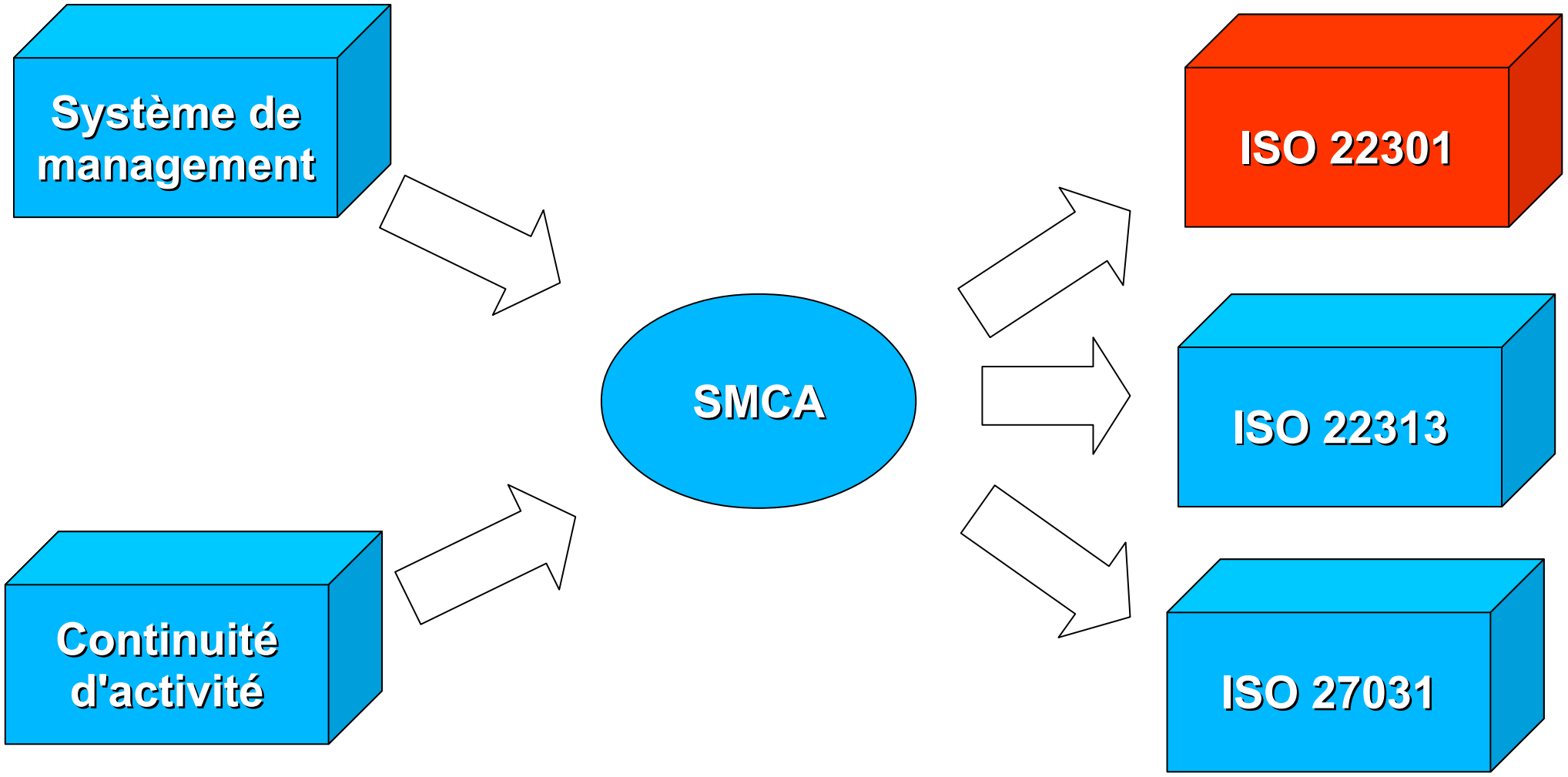
- Plan de Reprise d'Activité (PRA)
  - Ensemble de procédures qui permettent de repartir à partir d'un point d'interruption donné (CCA)
    - « reprise » suppose qu'il y eut interruption […].
  - Identifiée comme la partie purement métier du PCA.

Continuité d'Activité : vocabulaire courant



- PCA : Plan de Continuité d'Activité / *Business Continuity Plan*
- PSI : Plan de Secours Informatique / *Disaster Recovery Plan*
- PRA : Plan de Reprise d'Activité / *Business Recovery Plan*
- PGC : Plan de Gestion de Crise / *Contingency Plan*

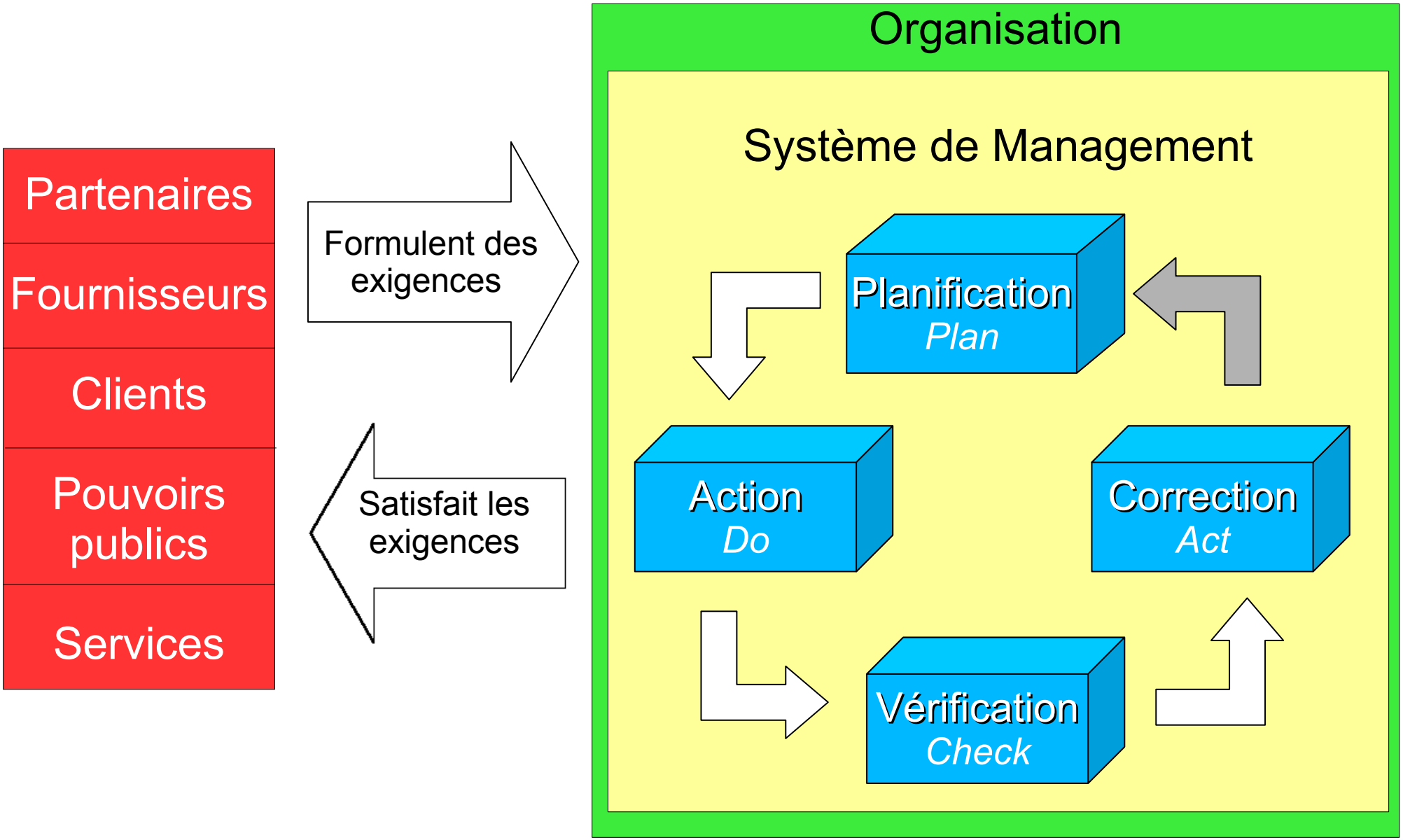
Introduction



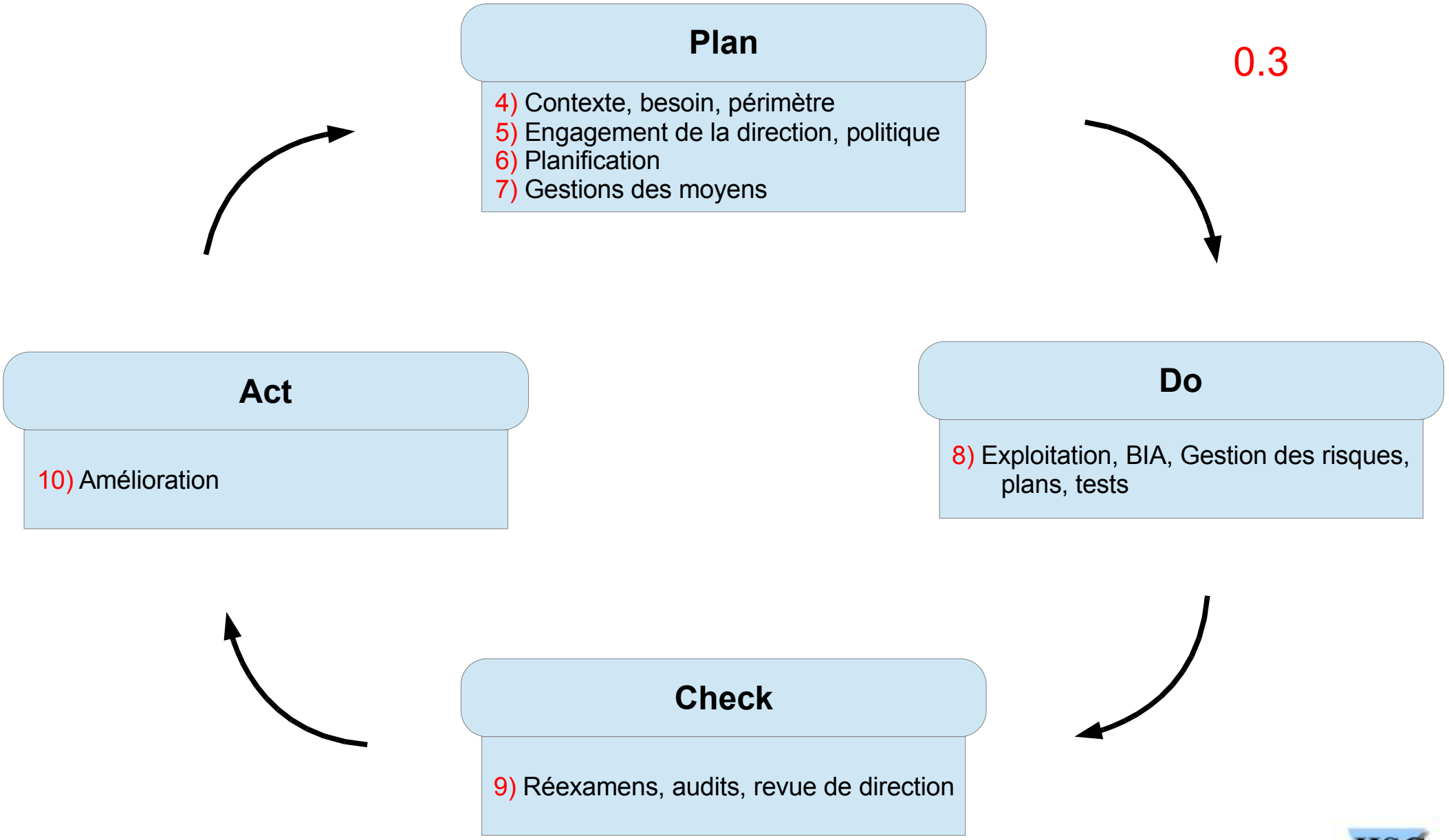
ISO 22301

- Norme utile pour (1)
  - Établir, mettre en œuvre, maintenir et améliorer un SMCA
  - Assurer la conformité avec la politique de continuité d'activité
  - Démontrer cette conformité à des tiers
  - Certifier son SMCA par un organisme de certification accrédité
  - Auto-évaluer et auto-déclarer sa conformité

Système de management



ISO 22301 : PDCA (0.3)



CA : Vision opérationnelle

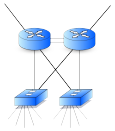
Sites

Travail manuel

Personnel

Données

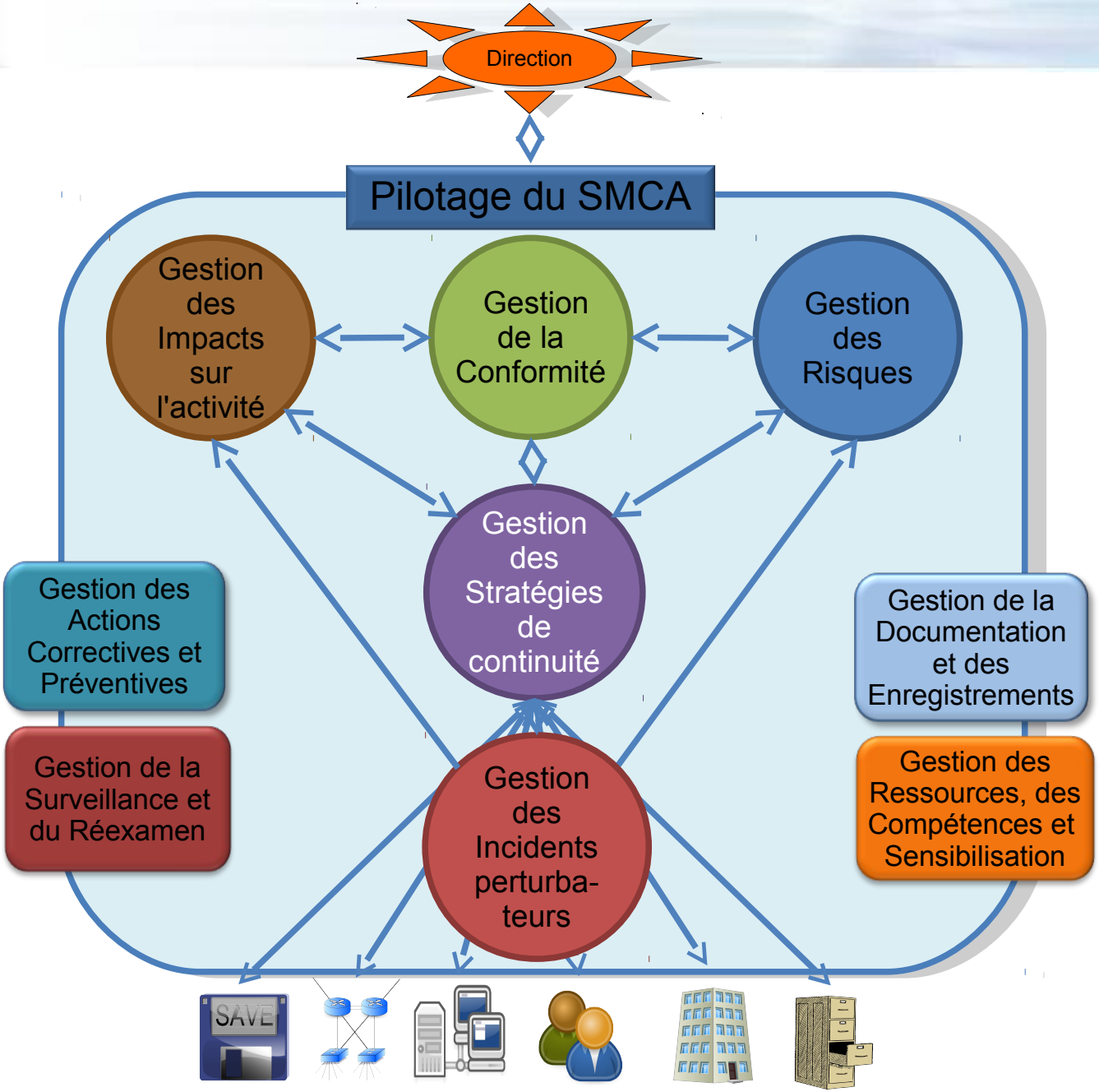
Matériels & logiciels



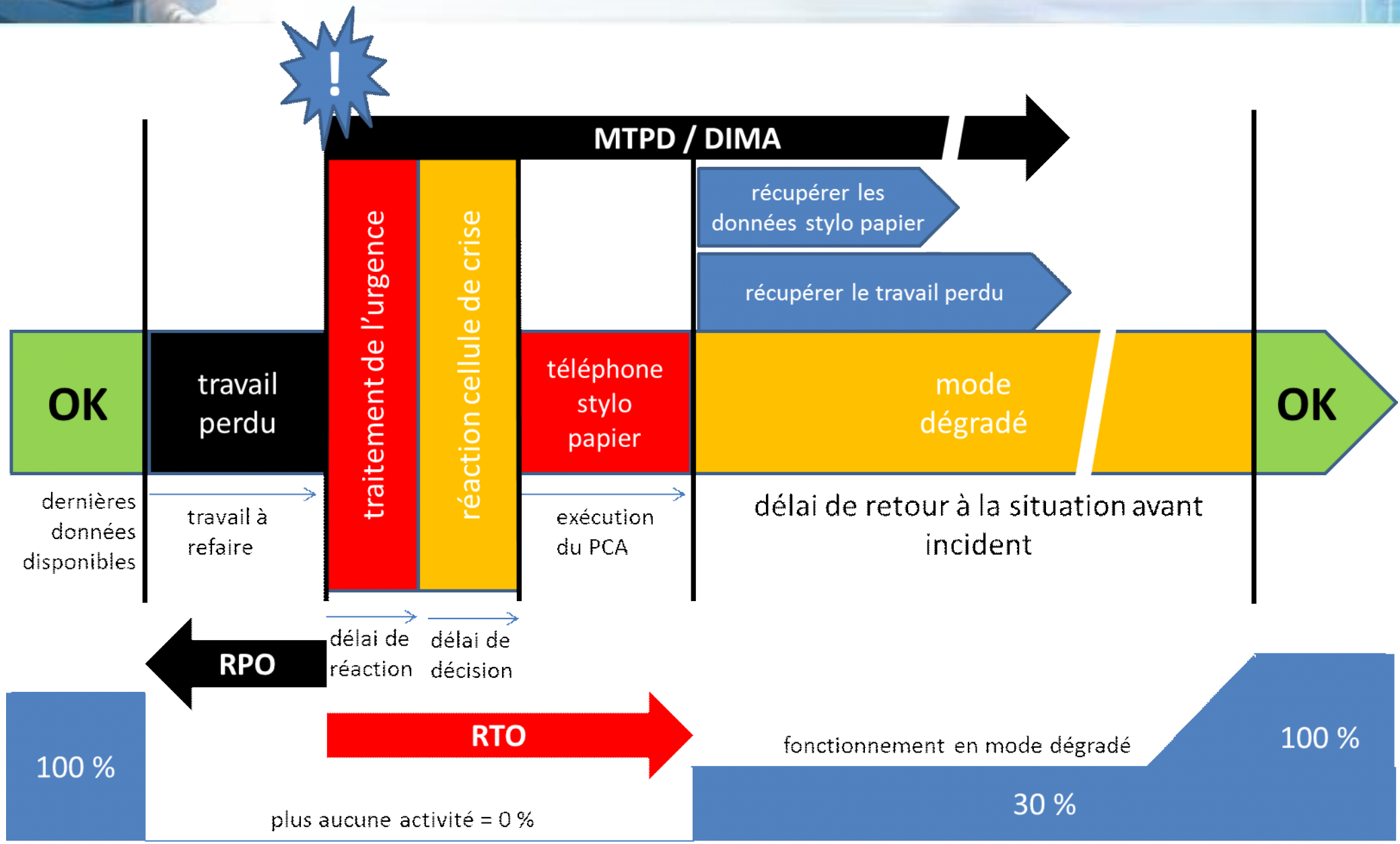
Réseaux

- Dispositif organisationnel ou technique permettant de
  - réduire les risques (proactif)
    - Vraisemblance et durée de la perturbation
    - Impacts
  - assurer la continuité d'activité (réactif)
    - Gérer l'incident
    - Poursuivre les activités
- Finalité de la discipline « Continuité d'activité »

Système de management de la continuité d'activité (SMCA)

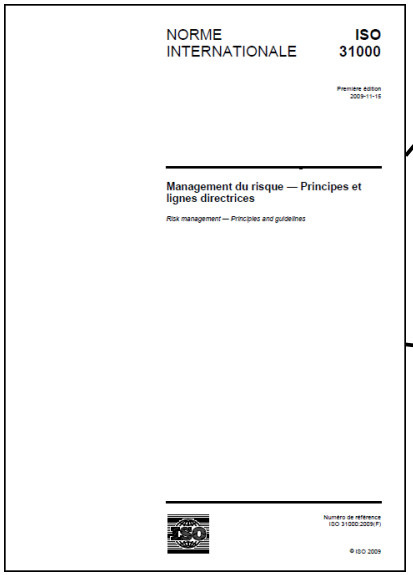


Séquencement d'un incident perturbateur



Intégration dans le SMCA

- Hiérarchie documentaire
  - Approche descendante (*top-down*)
  - Coté maîtrise d'ouvrage


NORME INTERNATIONALE

ISO 31000

Première édition 2009-11-15

Management du risque — Principes et lignes directrices

Risk management — Principles and guidelines

Numéro de référence ISO 31000:2009(F)

© ISO 2009

Périmètre et Politique du SMCA

ISO 22301 4.3
ISO 22301 5.3

ISO 22301 8.2.3 a) b) c)
ISO 31000 5.4

Appréciation du risque

ISO 22301 8.2.2

Analyse des impacts sur l'activité

Stratégie de continuité d'activité

1) Stratégies de continuité d'activité

2) Exigences sur les ressources

3) Protection et atténuation

ISO 22301 8.2.3 d)
ISO 22301 8.3.3
ISO 31000 5.5

Atouts de la norme ISO 31000

- Consensus international sur le management des risques
  - Compréhension mutuelle mondiale
  - Vise à harmoniser les processus de management du risque dans les normes existantes et à venir : sans les remplacer
  - Comparaisons plus faciles entre les secteurs d'activités et les techniques

- Gestion des risques **dans la durée**
  - pas juste une appréciation des risques à un instant "t"

Défauts de la norme ISO 31000

- Ne constitue pas une méthode utilisable
  - Lignes directrices générales
  - Ne se suffit pas à elle-même
  - Absence de base de connaissances
  - Imprécise sur les composantes d'un risque

- Accorde une **liberté** qui peut conduire à
  - Erreurs dans l'identification des composantes du risque
  - Appréciation trop superficielle ou trop détaillée

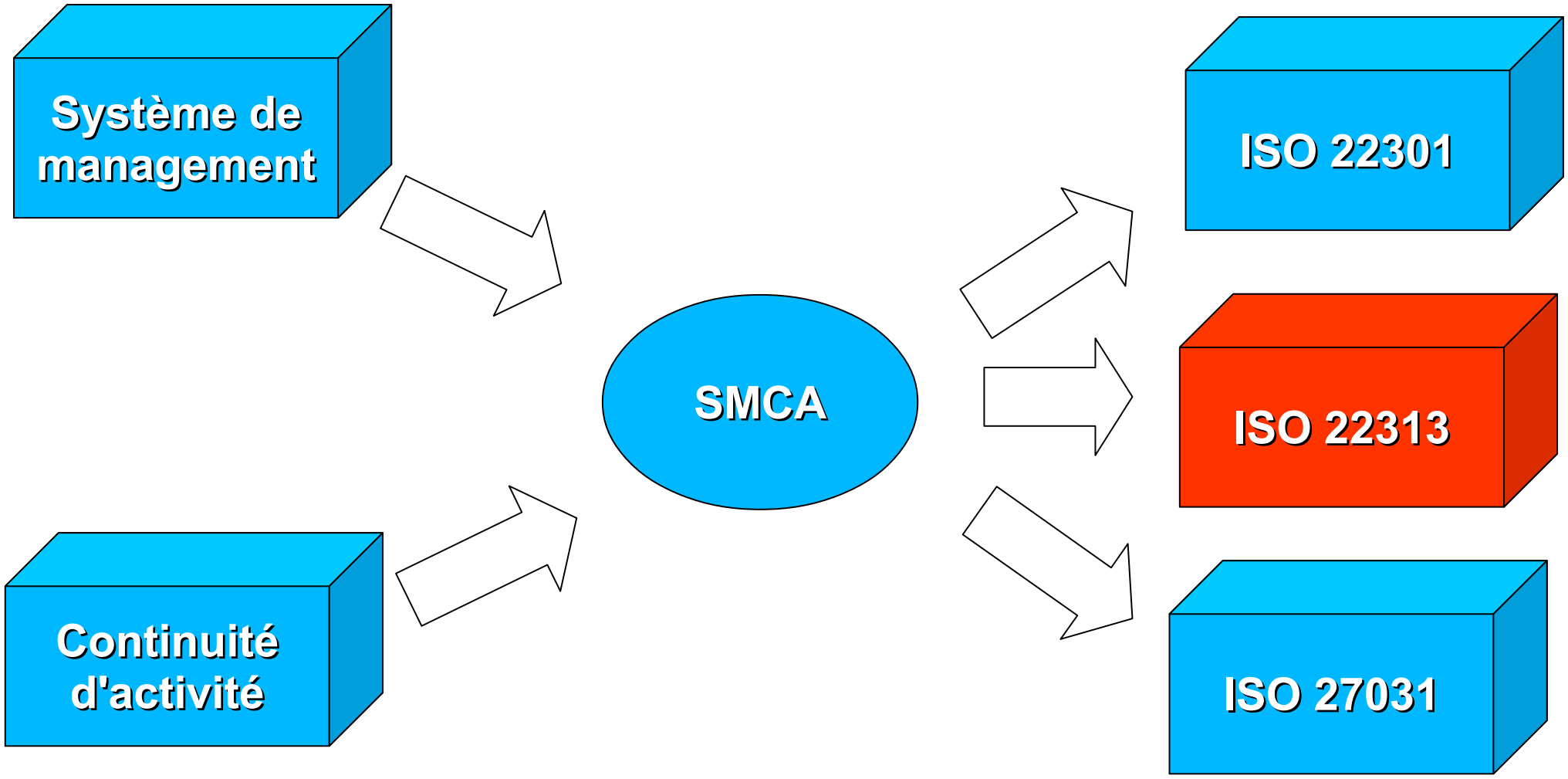
L'approche : des cultures différentes

- Américaine : DRII
  - D'abord l'AdR
    - Ressources supports pour le BIA
    - Scénarios pour le BIA
    - Pas de vision précise du périmètre métier
    - Visions DG & Métier indispensables
  - Approche par scénario d'incident perturbateur
    - Cadre l'application du plan
    - Multiplication des Plans
    - Ne favorise pas l'adaptabilité des acteurs du PCA
- Anglo-saxonne : BSI
  - D'abord le BIA
    - Conséquences pour l'AdR
    - Facilite l'identification des ressources supports
    - Pas de risques validés
  - Approche par processus
    - Imbrication logique des Plans par briques
    - Les acteurs du PCA doivent appliquer intelligemment les Plans
    - Pas simple en phase de stress
    - Cadre global

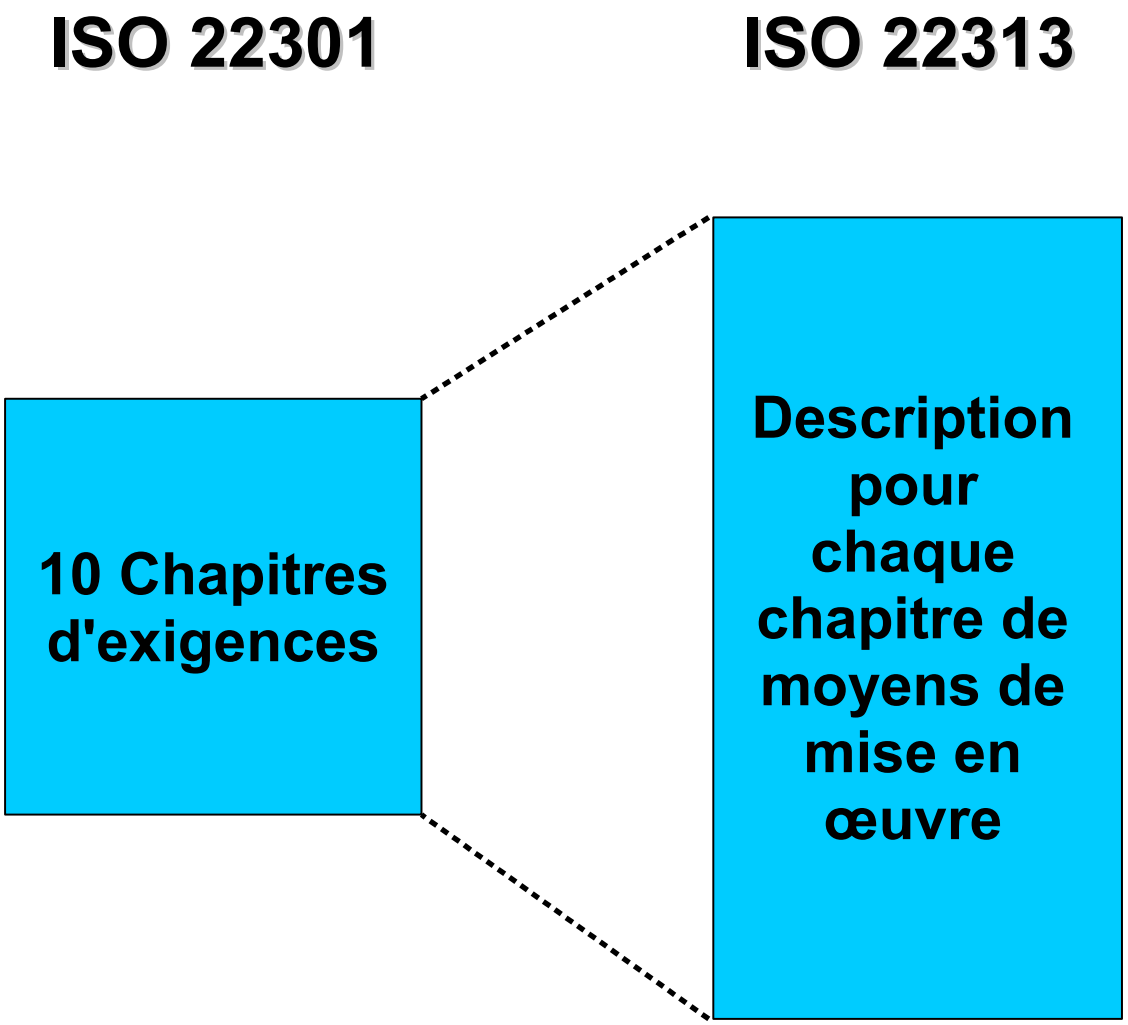
Dans la pratique...

- La Direction Générale a déjà une vision sur
  - Ses activités critiques
  - Les scénarios d'incidents perturbateurs à couvrir
- BIA et AdR réalisés en parallèle
  - Mutualisation des entretiens
  - S'alimentent l'un l'autre
- Définition des Plans de Continuité d'Activité
  - Un maximum par processus et fonctions supports
  - Des plans spécifiques pour les incidents perturbateurs transverses
    - Pandémie
    - Coupure électrique générale
    - ...

Introduction



ISO 22301 par rapport à ISO 22313

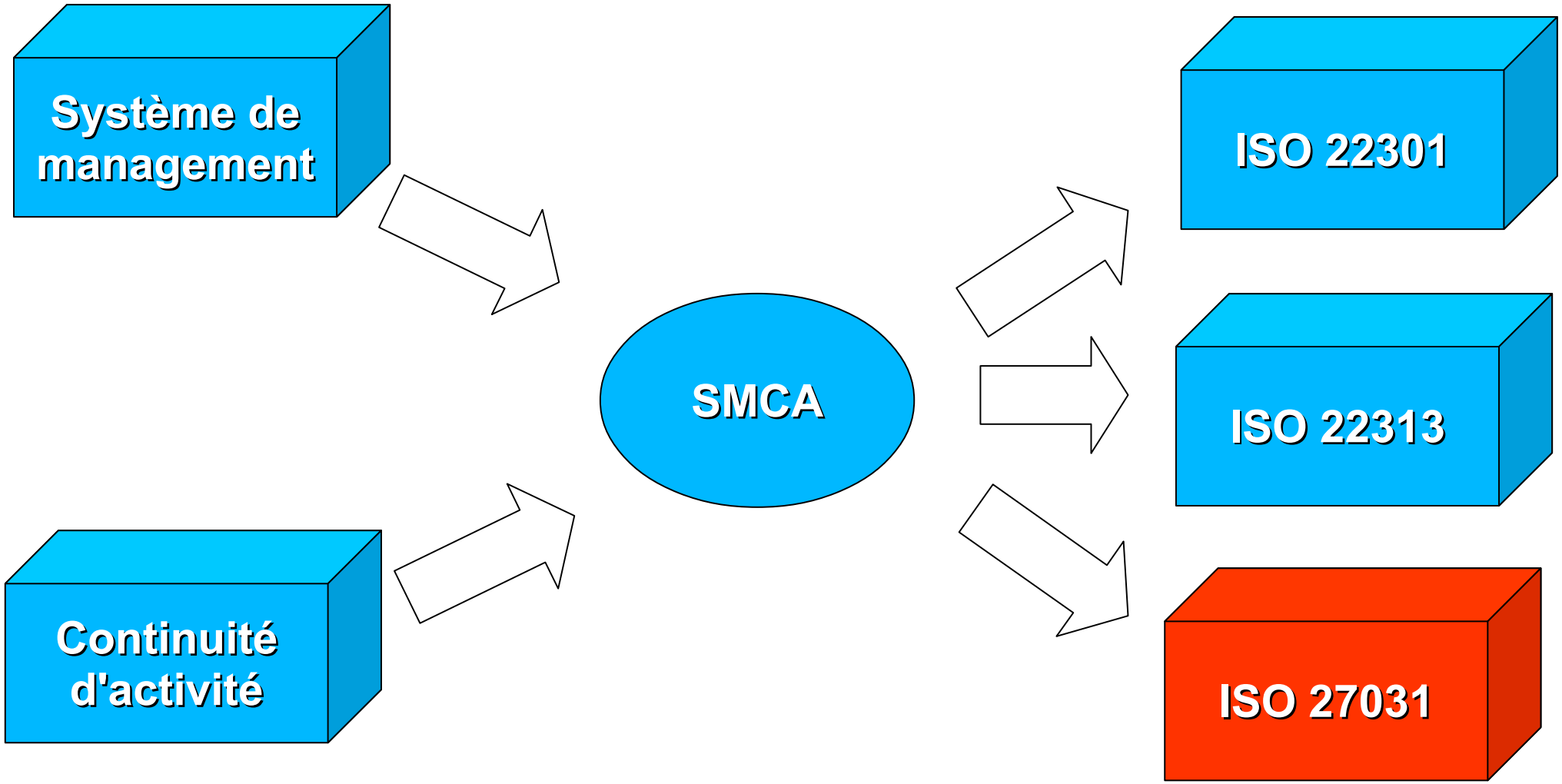


ISO 22301 par rapport à ISO 22313

- ISO 22301
  - Exigences pour le SMCA
  - Usage du verbe
    - **SHALL**
  - Volumétrie
    - Nombre total de pages
      - 32
  - Certification possible

- ISO 22313
  - Guide de mise en œuvre
  - Usage du verbe
    - **SHOULD**
  - Volumétrie
    - Nombre total de pages
      - 60
  - Pas de certification possible

Introduction à l'ISO 22301



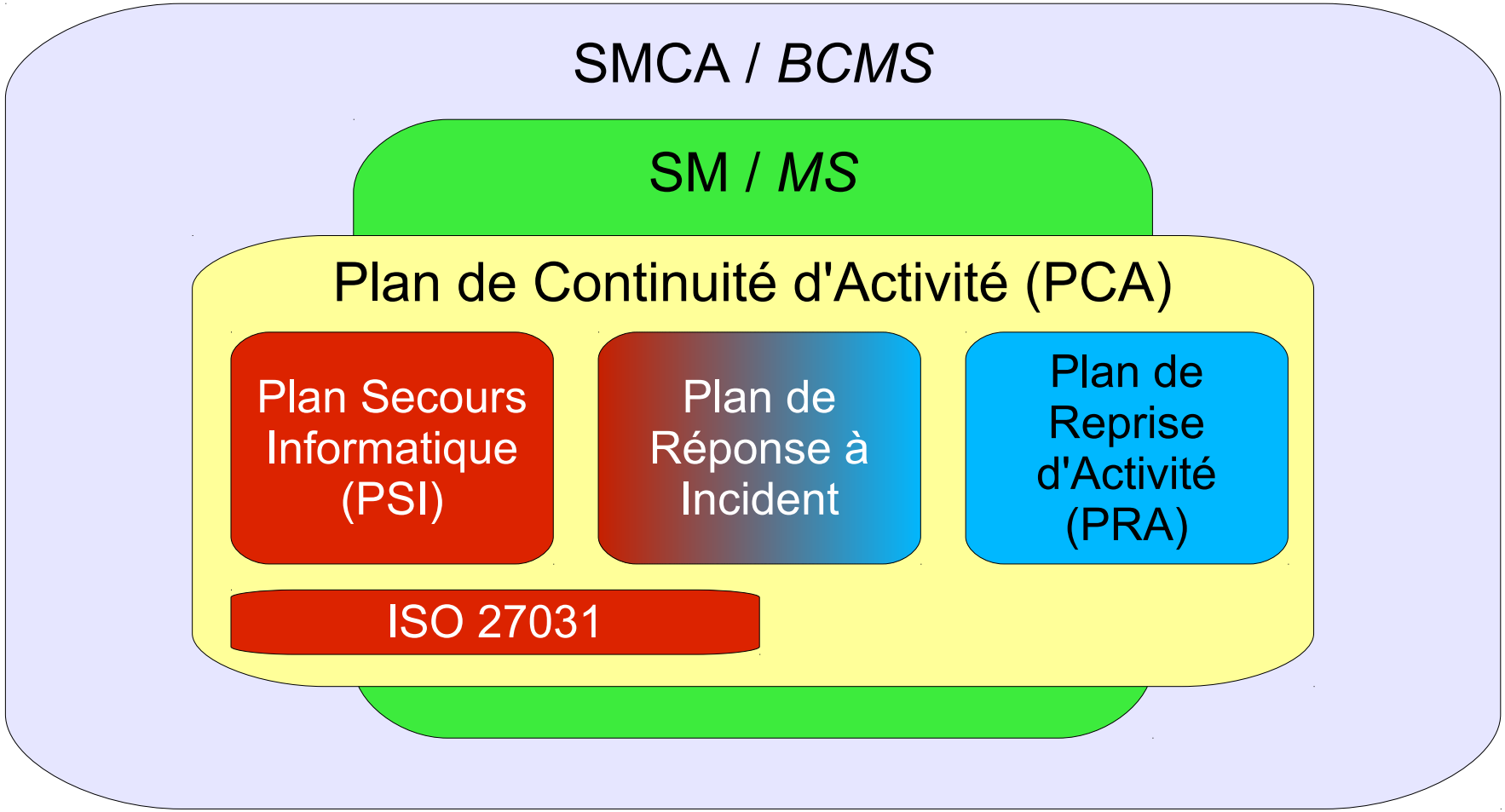
ISO 27031

- Directives liées à la continuité des activités IT alignées sur le SMCA
- Développée et publiée avant l'ISO 22301 et l'ISO 22313
- PTCA : Préparation des TIC pour la Continuité d'Activité (4)
  - *ICT readiness for Business Continuity*

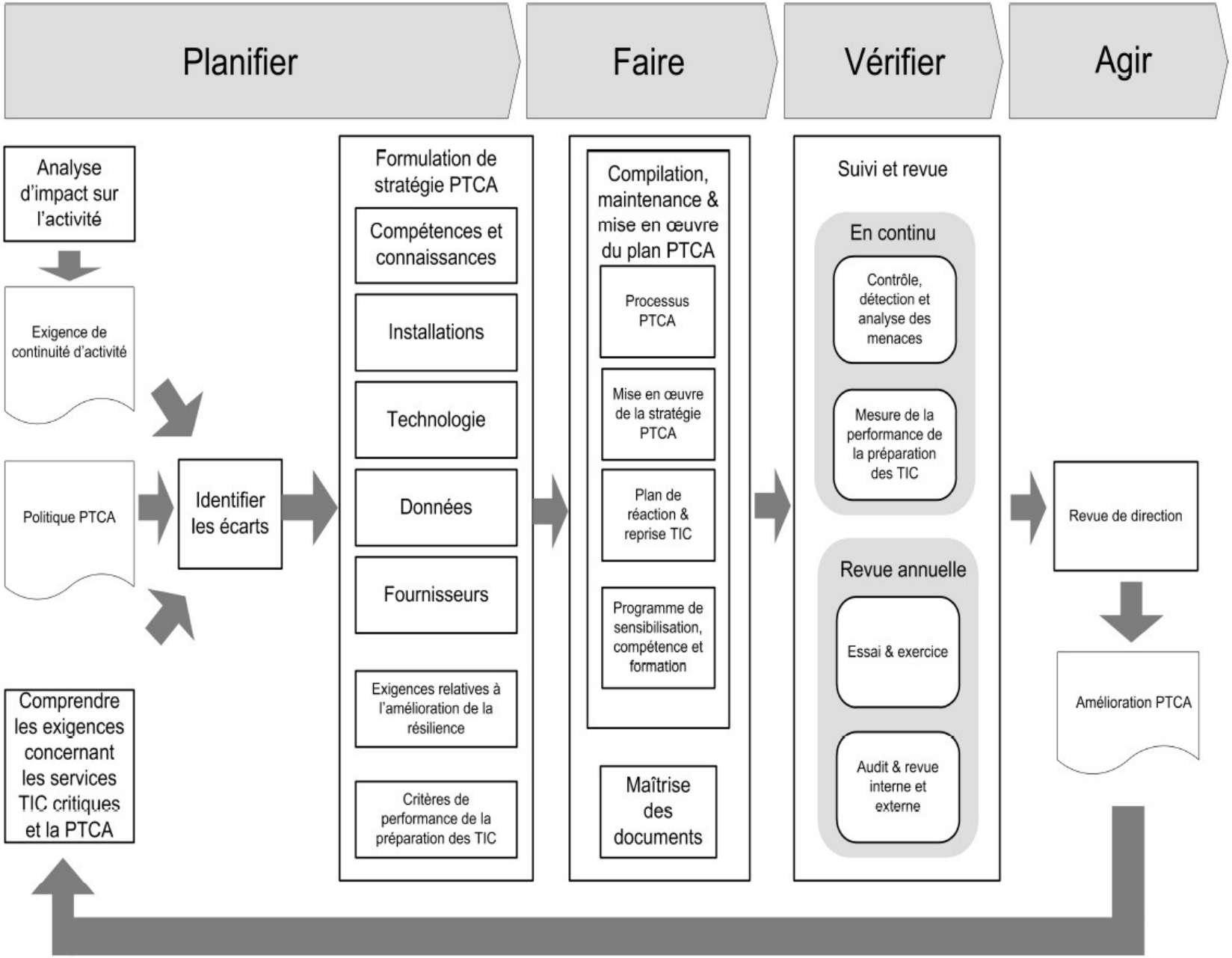
- Référence les normes :
  - ISO 27001 : Système de Management de la Sécurité de l'Information
  - ISO 27002 : Mesures de sécurité
  - ISO 27005 : Gestion des risques en sécurité de l'information
  - ISO 27035 : Gestion des incidents liés à la sécurité de l'information

ISO 27031

- PTCA : Préparation des TIC pour la Continuité d'Activité (4)
  - Fait partie intégrante du PCA et par transitivité du SMCA

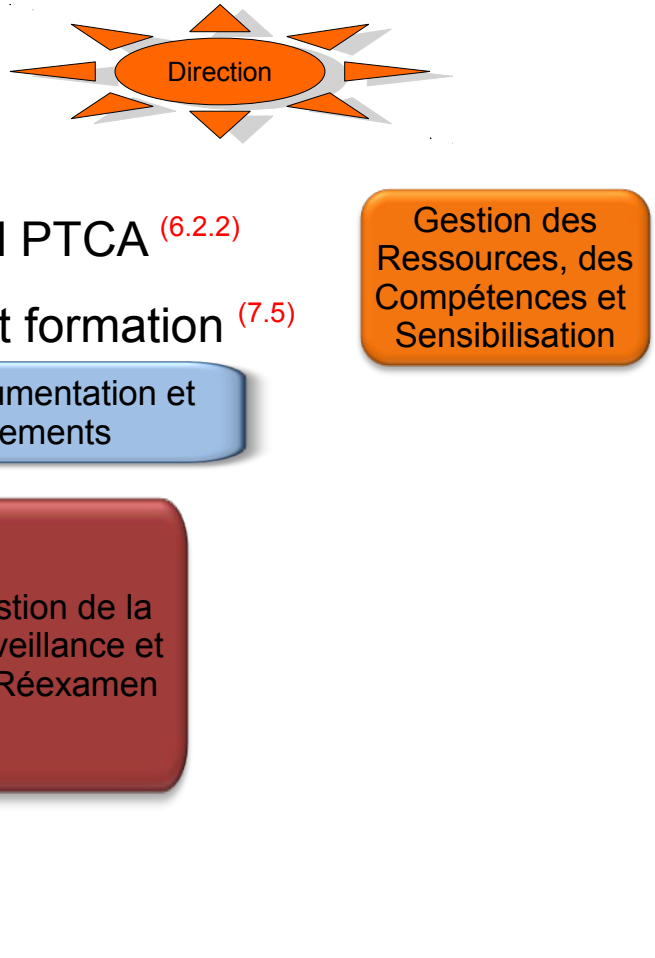


Phases PDCA de la PTCA / du PSI



Intégration de la PTCA dans le SM

- La PTCA s'intègre dans le SMCA mais peut également être gérée comme un processus holistique
  - Utilisation du cycle PDCA (5.6) : différent de la 22301
  - Engagement de la Direction (5.7.1)
  - Politique PTCA (5.7.2)
  - Ressources (6.2) et compétences du personnel PTCA (6.2.2)
  - Programme de sensibilisation, compétence et formation (7.5)
  - Maîtrise des documents (7.6)
  - Suivi et revue (7.6)
  - Mesure des critères de performance (8.4)
  - Audit interne (8.2)
  - Revue de direction (8.3)
  - Amélioration de la PTCA (9)



Intégration de la PTCA dans le PCA

- La PTCA s'intègre complètement dans le PCA
  - Fait partie intégrante du processus de management de la continuité d'activité (5.1)
    - Suppose que l'organisme **a déjà procédé** un BIA en amont (6.3.1)
      - Activités métiers priorisées en termes de continuité
      - Les exigences de continuité d'activité se traduisent en délais de reprise : RTO, RPO & OMCA (Objectif Minimal de CA : correspondance DIMA)
    - Plusieurs étapes inhérentes à une appréciation des risques (6.3.2 & 6.3.3)
      - Identifier des services IT critiques et leurs composants (ressources)
      - Apprécier les risques d'interruption ou de détérioration des services
      - Identifier les écarts entre l'IT et les exigences de continuité d'activité
    - Détermination des options de stratégie PTCA (6.4)
    - Réaction aux incidents (7.3)
    - Essai et exercice (8.1.3)

Gestion des Impacts sur l'activité

Gestion des Risques

Gestion des Incidents perturba-teurs

Gestion des Stratégies de continuité

La PTCA en amont des projets

- Concevoir et intégrée la PTCA en amont de la création des services IT (5.5)
  - Intégration de la continuité d'activité dans les projets

- Bénéfices
  - Stratégie de la PTCA globale cohérente
  - Niveaux de services IT en adéquation avec les objectifs de continuité d'activité
  - Établissement en amont la communication entre les métiers et l'IT
  - Résilience au meilleur coût