6 LE RSSI

LE RSSI

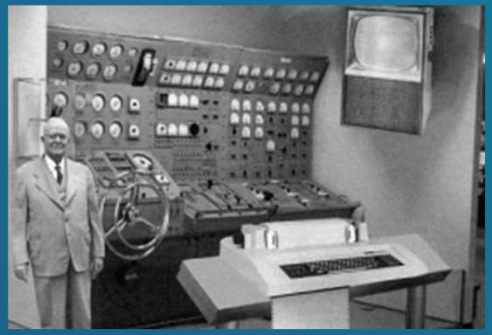
6

- Le rôle du RSSI
- Panorama de quelques missions
- La gestion de projet
- Les besoins en continuité, le PCA/PRA.
- Les Audits.
- La gestion des incidents

6 Le rôle du RSSI

Selon le CIGREF, le RSSI assure un rôle de **conseil, d'assistance, d'information, de formation** et **d'alerte :**

- veille technologique et réglementaire ;
- identification et gestion des risques ;
- conseil pour les évolutions qu'il juge nécessaires pour garantir la sécurité **logique** et **physique** du système d'information dans son ensemble.
- Il doit considérer le système de sécurité dans sa **globalité**
- Il doit pouvoir s'appuyer sur des **experts** dans les différents domaines (réseaux, systèmes, applicatifs, juridiques, communication...).
- ● Les spécificités de l'intervention du RSSI l'obligent à porter un regard critique à la fois sur **les modifications d'organisation** et les **réalisations informatiques techniques** :



6 Directeur Cybersécurité et RSSI

Directeur Cybersécurité

Equivalence en anglais :
Executive security director

Autres titres équivalents :
- **FR :** Directeur de la sécurité des systèmes d'information (DSSI)
- **EN :** *Group Chief Security Officer, Group Chief Information Security Officer, Vice-President (VP) Cyber security*

MISSION ESSENTIELLE

Au sein de grandes organisations, le Directeur Cybersécurité est un cadre dirigeant en charge de définir la stratégie de cybersécurité de manière à répondre aux enjeux de cybersécurité de l'organisation et d'être conforme aux réglementations en vigueur dans les pays où opère l'organisation. Il anime la filière cybersécurité et peut piloter un réseau de Responsables de la Sécurité des Systèmes d'Information (RSSI) permettant de couvrir l'ensemble du périmètre de l'organisation.

Il définit les indicateurs stratégiques et managériaux permettant de mesurer le niveau de maturité de l'organisation en matière de cybersécurité et rend compte à la Direction générale et au comité d'audit.

RSSI

Equivalence en anglais : *Chief Information Security Officer (CISO), Director of Information Security.*

Autres titres équivalents :
- **FR :** Officier de Sécurité des Systèmes d'Information (OSSI), Fonctionnaire de Sécurité des Systèmes d'Information (FSSI), Responsable de la Confiance Numérique (RCN)
- **EN :** *Information System Security Manager (ISSM), Information Security Manager*

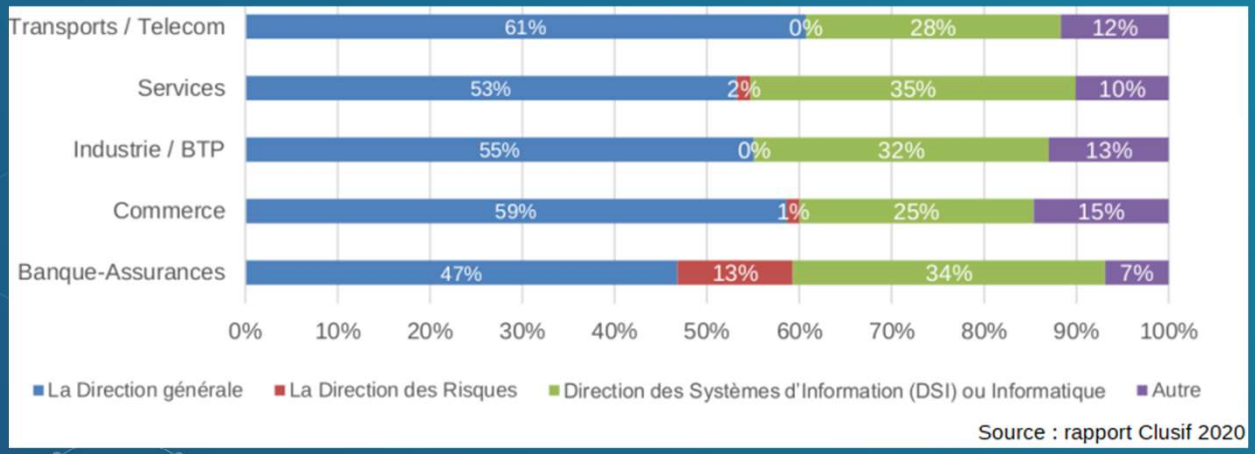
MISSION ESSENTIELLE

Le Responsable de la sécurité des systèmes d'information (RSSI) assure le pilotage de la démarche de cybersécurité sur un périmètre organisationnel et/ou géographique au sein de l'organisation. Il définit ou décline, selon la taille de l'organisation, la politique de sécurité des systèmes d'information (prévention, protection, détection, résilience, remédiation) et veille à son application. Il assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte, en particulier auprès des directeurs métiers et/ou de la direction de son périmètre.

Il s'assure de la mise en place des solutions et des processus opérationnels pour garantir la protection des données et le niveau de sécurité des systèmes d'information. Selon la taille de l'organisation, il joue un rôle opérationnel dans la mise en œuvre de la politique de sécurité des SI ou encadre une équipe.

6 Rattachement hiérarchique du RSSI

Quel est le rattachement hiérarchique du RSSI au sein de votre entreprise ?



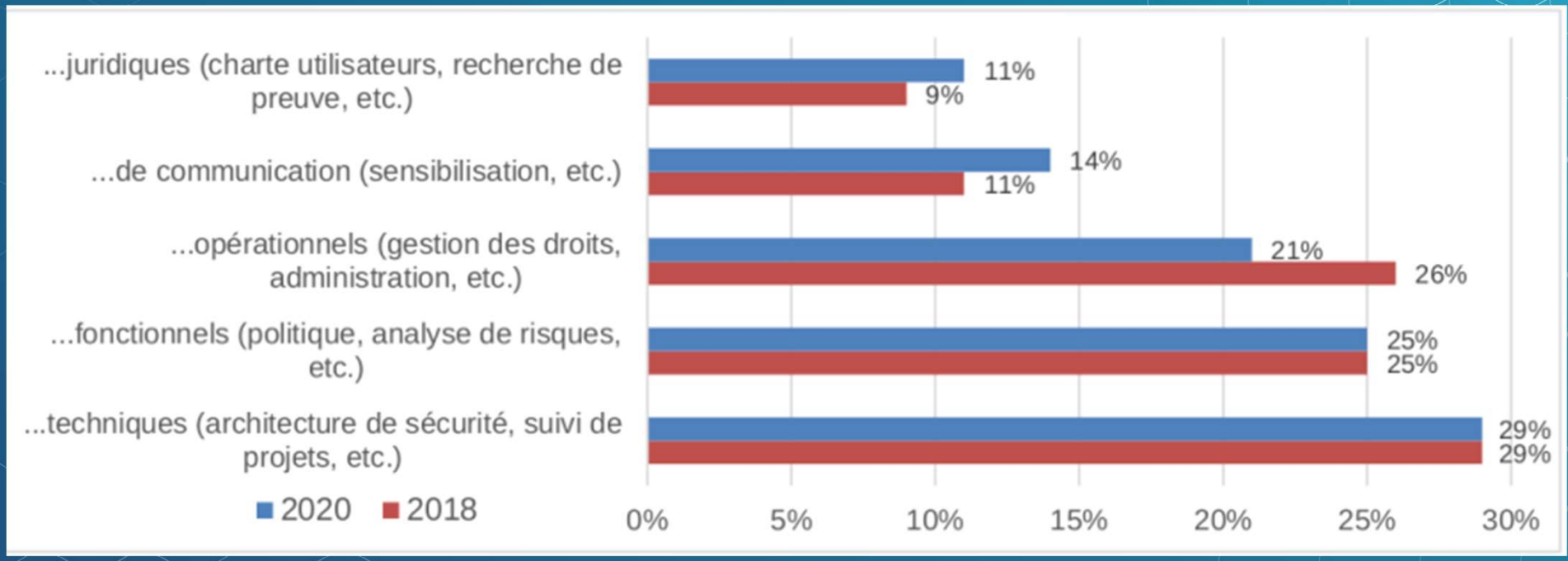
Source : rapport Clusif 2020

⇒ **3 types de recommandations** sur le rattachement hiérarchique :

- une proximité fonctionnelle avec le membre du Directoire ,
- dans une entité du même niveau que la DG dédiée à la sécurité en général,
- un rattachement fonctionnel avec la DSI

6 Les missions du RSSI

Dans le cadre des missions du RSSI, quel pourcentage représente les temps consacrés ..



Source: Rapport Clusif 2020

6 Les « vraies » missions du RSSI

Gouvernance

- Formaliser une **PSI** et mettre en œuvre le **SMSI**
- S'assurer de la **cohérence** entre les PSSI et la PSI
- **Piloter** les audits de sécurité et **manager le risque**
- **Animer** les différents intervenants tant informatiques que techniques de la sécurité des SI
- Animer et **sensibiliser tous** les différents acteurs de l'entreprise aux problématiques de la SSI
- Superviser les process de la **sécurité dans les projets** : DevSecOps, ISP, ISC

Technique

- Comprendre les **vulnérabilités** des systèmes d'information et mettre en place des actions correctives nécessaires
- **Manager** une équipe dédiée à la SSI
- **Être MOA** des projets permettant la mise en œuvre opérationnelle de la PSI :
- **IAM** dont comptes à privilèges
- Sécurisation **endpoint** : AV, EDR,
- Sécurisation **infra** : AD, BDD, PKI
- **Réseau** : NAC, FW, WAF, IDS, IPS
- **Cloud**
- Manager la **gestion des incidents** et :
- MOA des projets de détection et de réponses : SIEM, SOC, SOAR
- Superviser les tests : red team, tests d'intrusion, bug bounty, cyber range
- Coordonner la gestion des crises
- MOA des projet Reconstruction (PCA, PRA)

⇒ **un rôle de spécialiste.**

6 Les 100 premiers jours d'un RSSI

Découverte de l'écosystème « business » Faire les connexions	Modélisation des attaques d'un point de vue externe	Évaluer la maturité des mesures mises en place
Découverte du Business plan de l'entreprise Préparer un budget pour la sécurité	Modéliser la « supply chain » dans les risques redoutés	Modéliser les risques et désignation des actifs sensibles
Découverte des métiers, des compétences, capacités et gap à franchir	Cartographier les actifs internes	Créer la roadmap liée à la cyber-sécurité
Développer une vision de l'architecture d'entreprise	Développer une acculturation aux risques dans l'entreprise	Améliorer quelque chose

6 Qu’est-ce qu’un projet ?

Effort temporaire entrepris pour créer un produit, service ou résultat unique.

Caractéristiques clés

- Changement : Sans changement, pas de projets (continuité des opérations)
- Temporaire : Durée limitée
- Unique : Livrables et résultats spécifiques
- Inter-fonctionnel : collaboration d’acteurs d’horizons différents
- Progressif : Développé par étapes et continué par incréments
- L’incertitude : tout projet présente des risques (menaces vs opportunités)

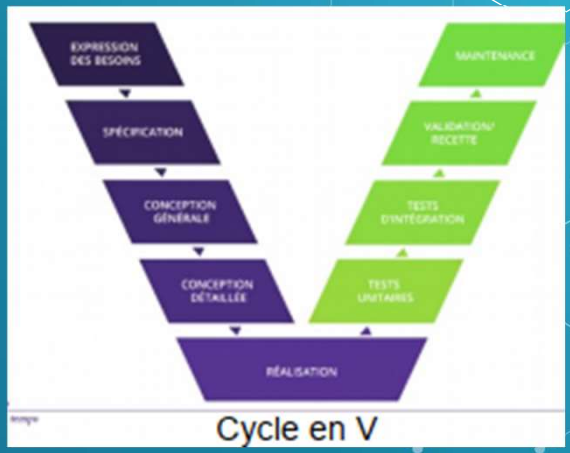
Pourquoi une méthodologie ?

⇒ Garantir le **succès d’un projet**, en minimisant les risques et les coûts, en :

– Structurant (Contraintes, viabilité)
– Planifiant (Préparation)
– Contrôlant les projets (Rendre des comptes)

« L’avenir ne se prévoit pas, il se prépare »

6 Qu’est-ce qu’un projet ?



Cycle en V

Méthodes traditionnelles (Waterfall, Cycle en V) :
suivent une séquence linéaire et ordonnée

Méthodes agiles (Scrum, Kaban, Lean, Six Sigma) :
adaptative, itérative, et flexible

PRINCE2 :
très structuré, axé sur la division des projets en phases gérables.

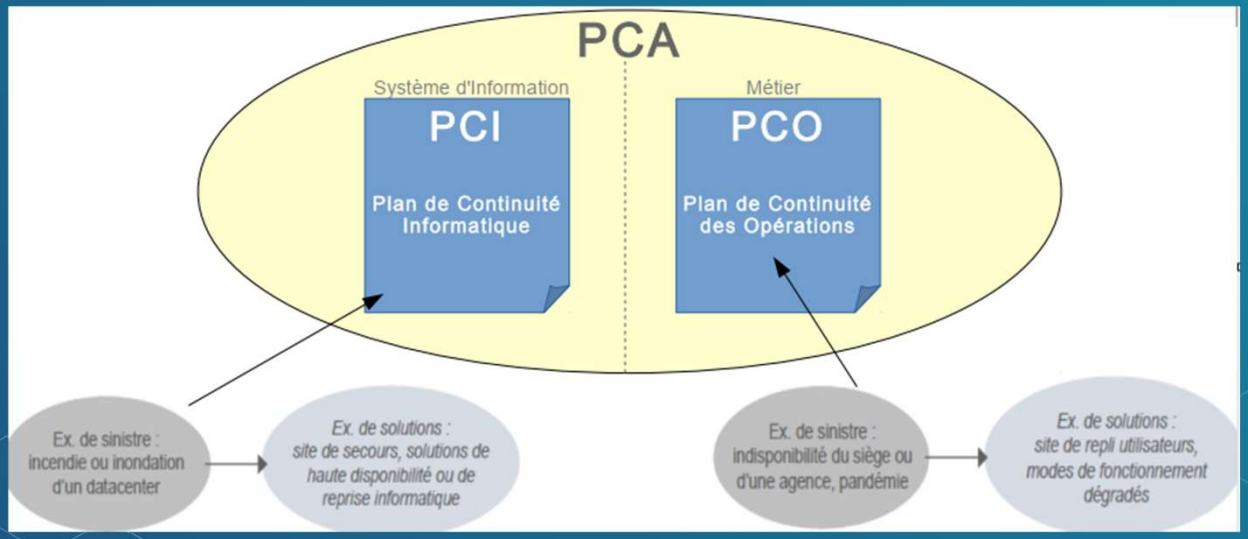
PMP :
basé sur le PMBOK (Guide du PMI), couvre cinq groupes de processus et dix domaines de connaissance

6 PCA, PCI, PCO

Toute PSSI comporte un volet Plan de Continuité d'Activité qui :

● Décline la stratégie et l'ensemble des dispositions qui sont prévues pour garantir à une organisation la reprise et la continuité de ses activités à la suite d'un sinistre ou d'un événement perturbant gravement son fonctionnement normal.

● Permet à l'organisation de répondre à ses obligations externes (législatives ou réglementaires, contractuelles) ou internes (risque de perte de marché, survie de l'entreprise, image…) et de tenir ses objectifs.

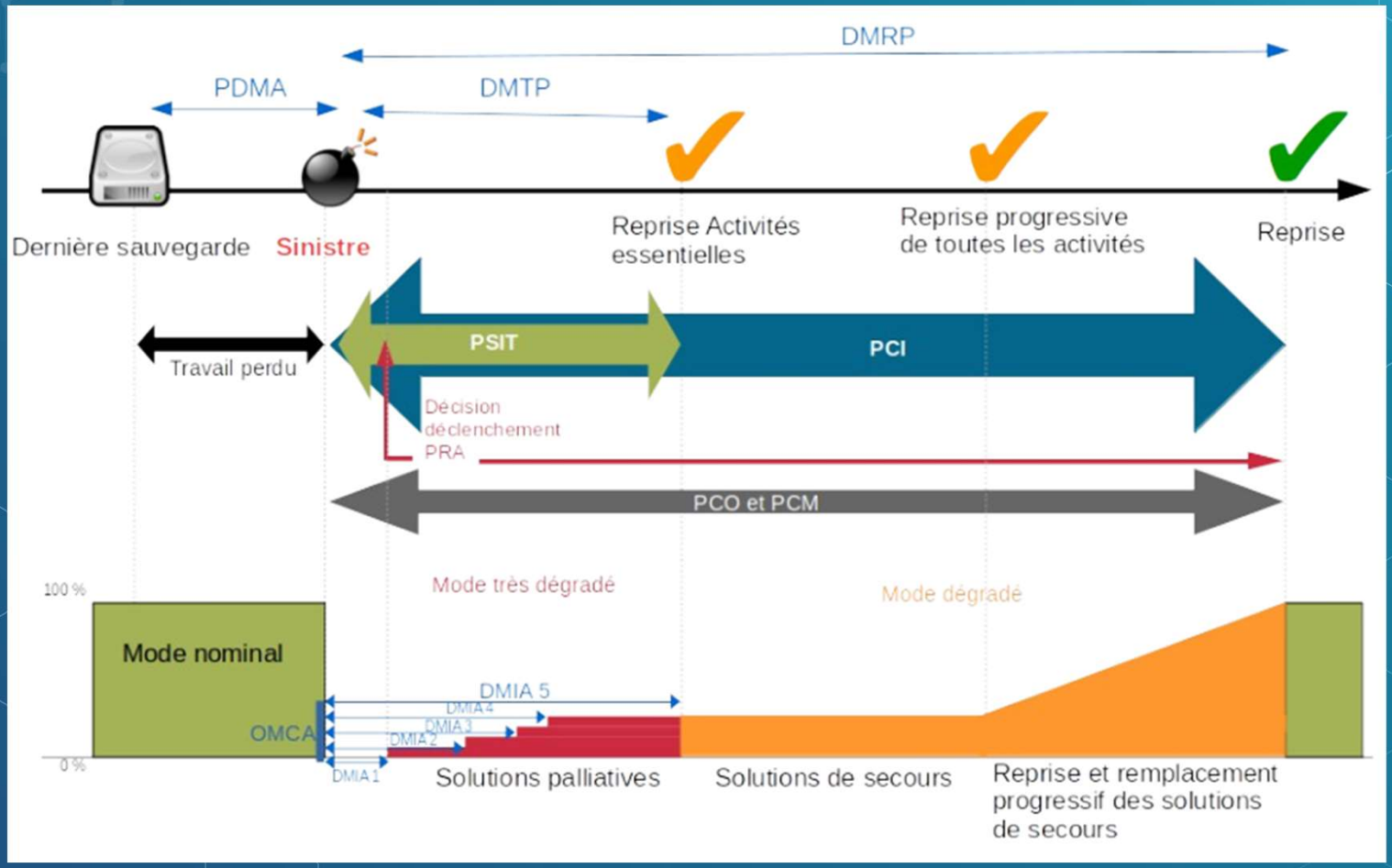


6 ISO 22301 - PCA, PSI et PGC

Organisation du PCA :

- à partir de de **stratégies** business (activité(s) / plans stratégiques business)
- à partir **d'objectifs** de récupération de la situation en cas de perturbation (PDMA/ DIMA)
- en imposant **des plans** concrets adaptés à deux situations distinctes :
- **Scénarios anticipés**
  - Plan de Continuité d'Activité (PCA)
  - Plan de Secours Informatique (PSI)
- **Situations surprenantes** (non anticipables et déstabilisantes)
  - Plan de Gestion de Crise (PGC)

6 Vocabulaire et métrique PCA



6 Différence entre PCA et PRA

PCA :

● permet en cas de **sinistre** de continuer **l'activité sans perte de service** ou avec une légère dégradation acceptable *(exemple : télétravail en cas de grève, tempête ou pandémie)*

PRA :

● permet en cas de **crise majeure ou sinistre**, de pouvoir reconstruire ou de **basculer sur un système** de relève sur une durée déterminée qui fournira les services nécessaires à la survie de l'entreprise. Il est souvent lié à un risque définir de perte de données (RPO) et durée d'interruption acceptable (RTO) *(exemple : basculement d'un datacenter sur un site de secours en cas d'incendie)*

6 Vocabulaire et métrique PCA

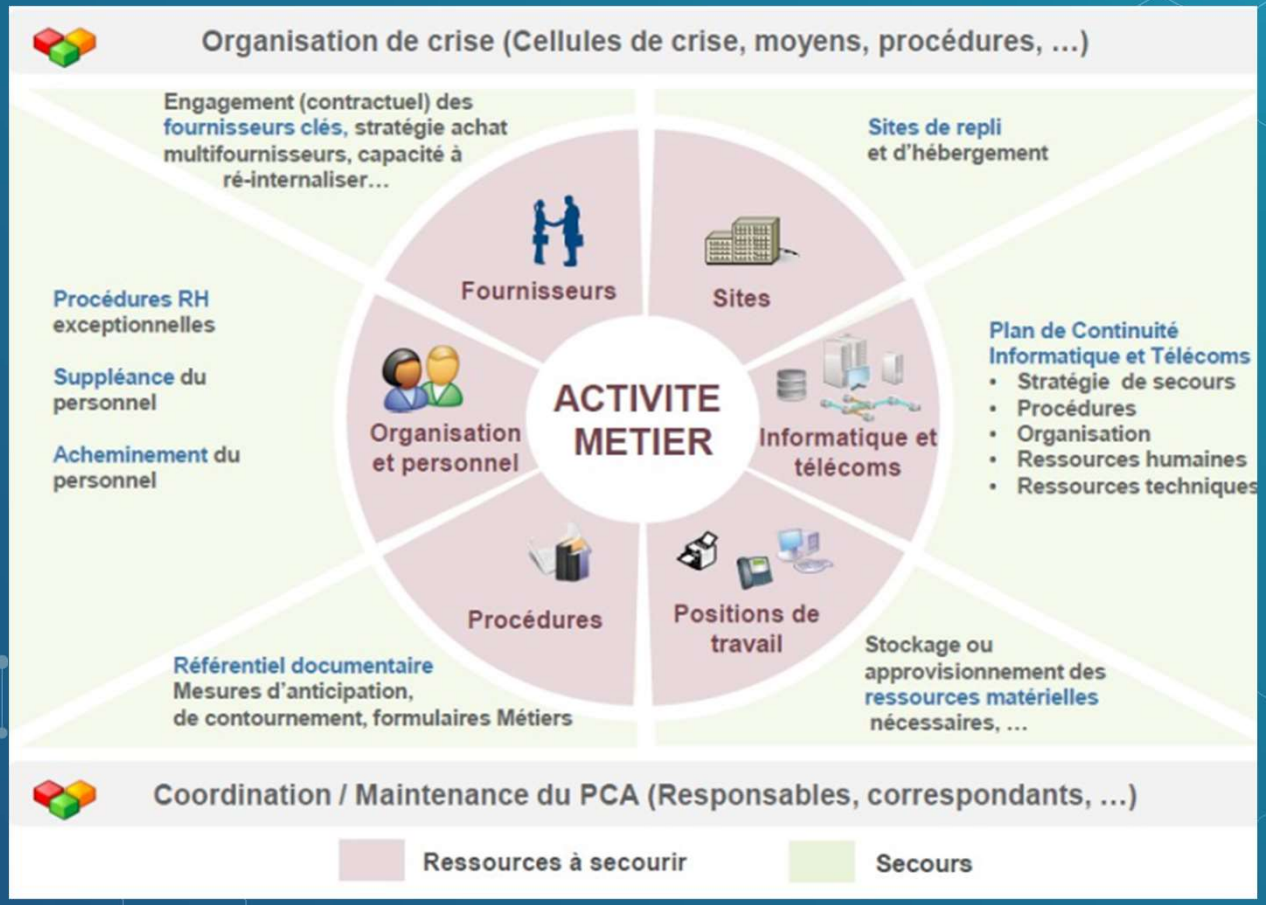
Cadre réglementaire du PCA

- Obligations réglementaires **Banque/Finance**
- Bâle II (décret CRBF en France)
- CRBF 1997-02 : plans de continuité informatique
- CRBF 2004-02 : plan de continuité d'activité documenté, cohérent et testé

applicable depuis le 1er juillet 2004 :

- pourra faire partie intégrante du plan d'audit en cas d'inspection de la Commission Bancaire
- le comité d'audit doit être informé au moins une fois depuis le 1er juillet 2005
- rapport de contrôle interne informant sur le sujet depuis avril 2005
- Instruction générale relative à la **sécurité des activités d'importance vitale** (opérateurs vitaux et sous-traitants)
- Gouvernance et obligations nouvelles (Sarbanes-Oxley, …)
- Responsabilités pénales et civiles
- Assurance

6 Des mesures préventives



8 Solutions informatiques et techniques

- Les **sites de secours** (distants ou non) :
- salle blanche : une salle machine protégée par des procédures d'accès particulières, généralement secourue électriquement
- site chaud : site de secours où l'ensemble des serveurs et autres systèmes sont allumés, à jour, interconnectés, paramétrés, alimentés à partir des données sauvegardées et prêt à fonctionner
- site froid : site de secours qui peut avoir une autre utilisation en temps normal
- site tiède : site de secours intermédiaire
- Externalisation de **sauvegardes**
- Matériel de secours
- Accord contractuel avec un partenaire ou un concurrent
- Redondance informatique (réseau / système / application)
- Externalisation provisoire d'activité
- La redondance (réseau / système / application)
- La prévention passe aussi par la sensibilisation des utilisateurs

6 Solutions informatiques et techniques : des solutions adaptées