COMMON Romandie

IBM

Journée COMMON

Introduction à la résilience de l'infrastructure informatique (1 heure 30)

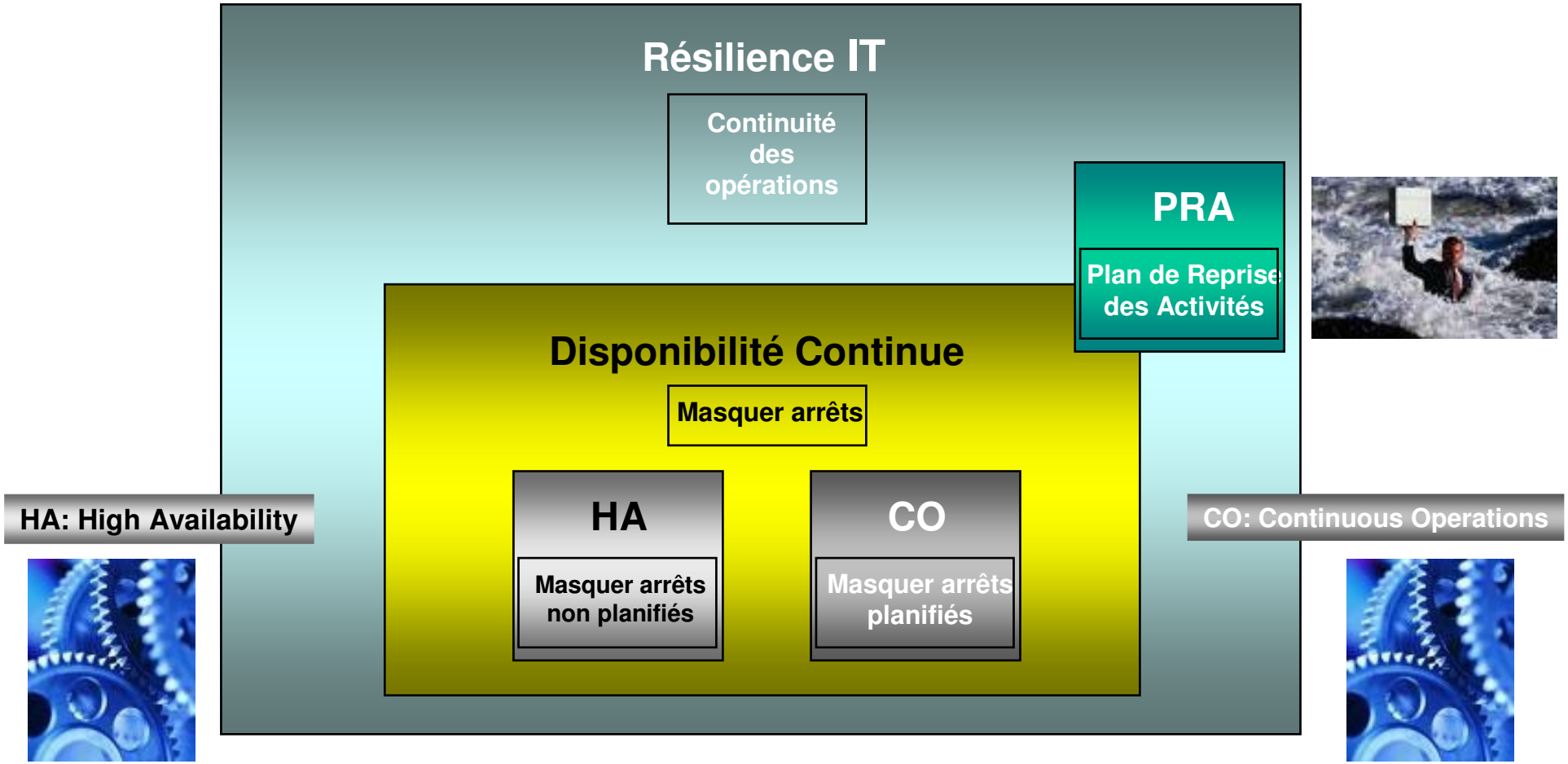
13 Mai 2014 - Genève

Jocelyn DENIS
Engagement Leader
High Availability Center of Competency (HACoC)

Agenda de l'introduction à la résilience

- **Définitions** des standards de l'industrie pour la résilience
- **Principes de base** de la résilience
- Résilience et Service Management **côté client**:
  - Tendances architecturales pour la disponibilité et le PRA
  - Comment les processus de gestion de l'informatique influencent la résilience

Définition des standards de l'industrie pour la Résilience



Source: IEEE - SHARE

Définition des standards de l'industrie pour la Résilience

Plus difficile à mesurer… Plus difficile à garantir

- **Business Resiliency (BR)** - The ability of the business to rapidly adapt and respond to opportunities, regulations and risks, in order to ***maintain secure and continuous business operations***, be a more trusted partner, and enable growth.
  Business Resilience spans business strategy, organizational structure, business and IT processes, IT infrastructure, applications and data, and facilities. It arises from the implementation and management of a plan that ensures high availability through monitoring and automatic adjustment of redundant or virtualized infrastructure components.
  Disaster Recovery (DR) is one component of an overall Business Resilience Plan.
- **Continuous Availability (CA)** - Attribute of a system to ***deliver non disruptive service*** to the end-user 7 days a week, 24 hours a day (there are no planned or unplanned outages).
- **High Availability (HA)** - Attribute of a system to ***provide service during defined periods, at acceptable or agreed upon levels and mask unplanned outages*** from end-users. It employs Fault Tolerance, Automated Failure Detection, Recovery, Bypass, Reconfiguration, Testing, Problem and Change Management.
- **Continuous Operations (CO)** - Attribute of a system to ***continuously operate and mask planned outages*** from end-users. It employs non-disruptive hardware and software changes, non-disruptive configuration, software coexistence.
- **Single-Point-of-Failure (SPoF)** - Any Configuration Item that ***can cause an incident when it fails***, and for which a countermeasure has not been implemented (ITIL).

Source: IEEE - SHARE

Quelles sont les différences entre disponibilité et PRA?

- **Disponibilité Continue (DC):**
  - Lorsqu'un composant de l'infrastructure IT (HW ou SW) tombe en panne (non planifié) ou est arrêté (planifié), **le service rendu aux utilisateurs n'est pas impacté**, ou impacté de manière très limitée (uniquement les transactions en cours de traitement ("in-flight transactions") → elles devront être "rolled-back").
    - Exemples de fonctions de DC en environnement Power Systems:
      - Pour les systèmes: PowerHA, Live Partition Mobility (arrêts planifiés)
      - Pour les données: AIX LVM mirroring, Metro Mirror (*réplication synchrone des données par les disques*), clustering Oracle RAC
  - Dans le pire des cas, cette situation conduira à un restart (*et non pas un recovery*) sans perte de données. Cela peut alors être réalisé en quelques sec ou minutes.
  - *Si l'incident affecte tous les composants IT, voire au-delà (bâtiments, hommes…), alors cela n'a plus rien à voir avec la Disponibilité Continue…*
- **Plan de Reprise d'Activité (PRA):**
  - Lorsqu'un incident impacte plusieurs composants (ou tous) dans un lieu donné (ce qui peut aller bien au-delà de l'infrastructure IT), alors on parle de **sinistre**.
  - Dans une telle situation, **tous les services de l'IT sont interrompus** et **une décision doit alors être prise par le management** de redémarrer ou pas l'ensemble des activités sur le site distant de PRA. Cela peut être réalisé en plusieurs heures ou jours, avec une perte de données plus ou moins importante.
    - Exemples de fonctions de PRA en environnement Power Systems:
      - PowerHA/EE, AIX GLVM, Global Mirror (*réplication asynchrone*), Oracle Dataguard

Quelles sont les similitudes entre disponibilité et PRA?

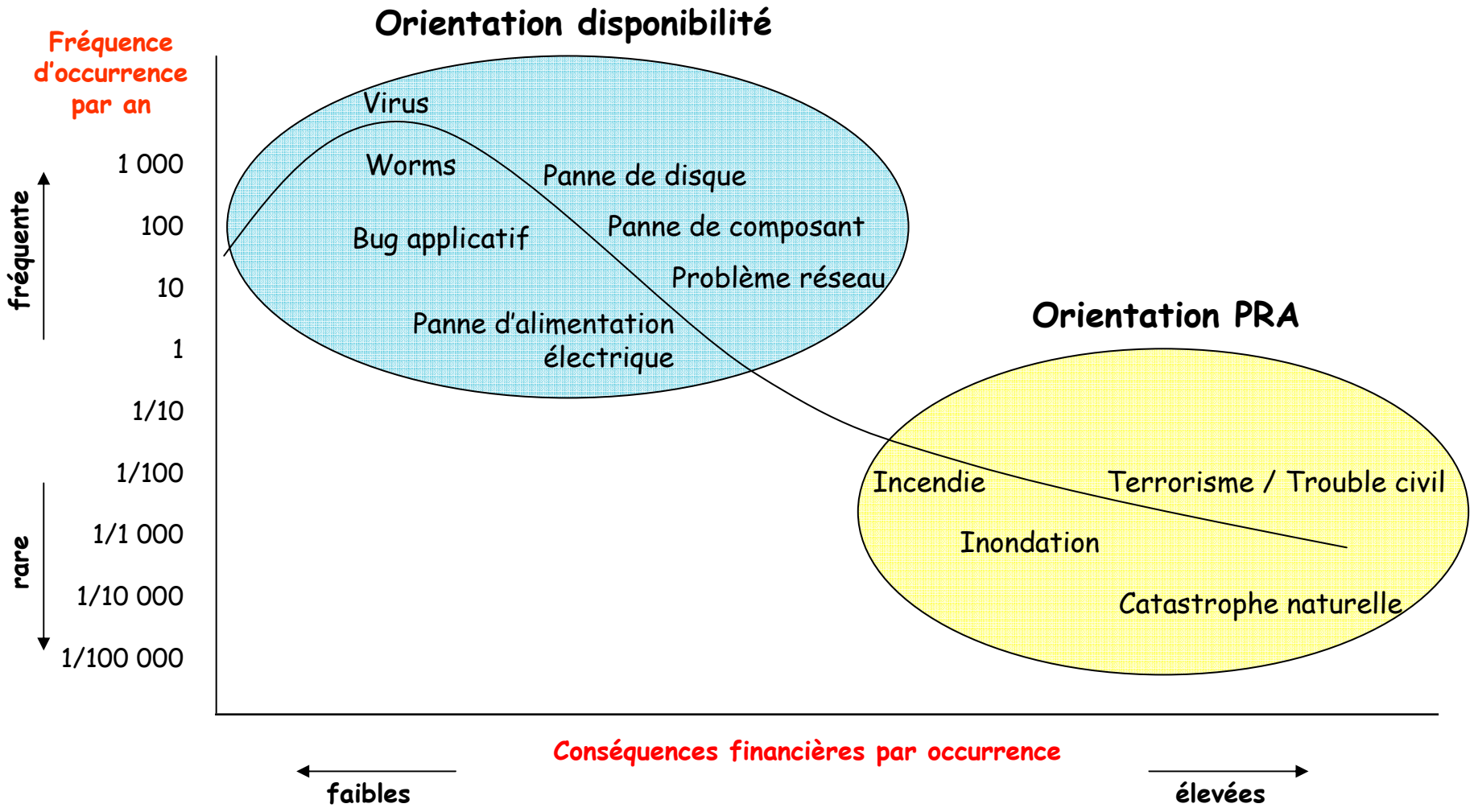
- **Ils correspondent tous les 2 aux mêmes besoins métiers:**
  - "Quoiqu'il arrive à l'informatique, je ne veux pas perdre de données et je ne veux pas impacter l'activité des métiers". Cela peut se traduire en :
    - Des objectifs de RPO = 0 et RTO = 0 pour le PRA.
  - Ce qui correspond très exactement à ce que "*la tolérance de panne par la redondance et la bascule automatique de la charge*" signifie pour la Disponibilité Continue !!!

- **Les objectifs de DC et de PRA pourraient alors être exprimés avec les mêmes indicateurs:**
  - Le RTO du PRA n'est rien d'autre qu'un objectif de MTTR appliqué à un sinistre complet sur un site.
  - L'objectif de MTTR n'est rien d'autre qu'un objectif de RTO en cas d'arrêt d'un composant.

- **Nous recommandons d'implémenter des solutions technologiques séparées pour la Disponibilité Continue et le PRA qui soient spécifiques et dédiées:**
  - L'objectif étant qu'une des solutions ne fonctionne pas au détriment de l'autre.

- **Toutefois, dans certaines circonstances particulières, les solutions technologiques de DC et de PRA peuvent être combinées:**
  - Par exemple, avec 2 sites séparés sur un campus ou avec une distance limitée mais suffisante entre eux, alors un cluster intersites et une réplication synchrone des données pourraient couvrir à la fois les fonctions de disponibilité et de PRA (mais pas pour un sinistre régional)
    → *cela signifie que les risques à couvrir doivent être **analysés** et **évalués** par le client avant de bâtir l'architecture devant assurer les besoins de disponibilité et de PRA.*

Probabilité des risques et impacts correspondant



Signification d'un pourcentage de disponibilité de service

Pourcentage annuel de disponibilité pour une application 24 x 7 :

- **99 %**
  - **87 heures (3 jours ½)** d'arrêt par an au maximum
- **99.5 %**
  - **44 heures** d'arrêt par an au maximum
    → 2 fois moins
- **99.9 %**
  - **9 heures** d'arrêt par an au maximum
    → 3 fois moins
- **99.99 %**
  - **1 heure** d'arrêt par an au maximum
    → 9 fois moins
- **99.999 %**
  - **5 minutes** d'arrêt par an au maximum
    → 12 fois moins
- *L'industrie aéronautique est réputée pour avoir une disponibilité (fiabilité du transport aérien) de 99.99999 % !*

- **Les technologies actuelles sont extrêmement fiables.**
- **Certains produits ont des MTBF de 30 à 40 ans (System z et Power Systems par exemple).**
- **Mais cela ne veut pas dire que vous pouvez espérer fonctionner pendant 30 à 40 ans sans panne.**
- **Cela signifie que vous avez 2.5 à 3 % de "probabilité" de panne cette année (1/40 à 1/30).**
- **Avec 100 machines, vous pouvez donc vous attendre à 2 à 3 pannes chaque année en moyenne.**

Principes de base de la résilience et du Service Management

Résilience métiers

Résilience IT

Systèmes

Réseau et équilibrage dynamique de la charge

Clustering

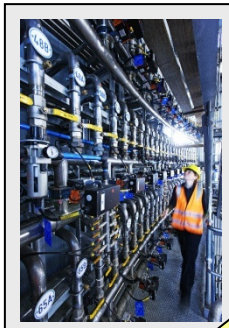
Redondance

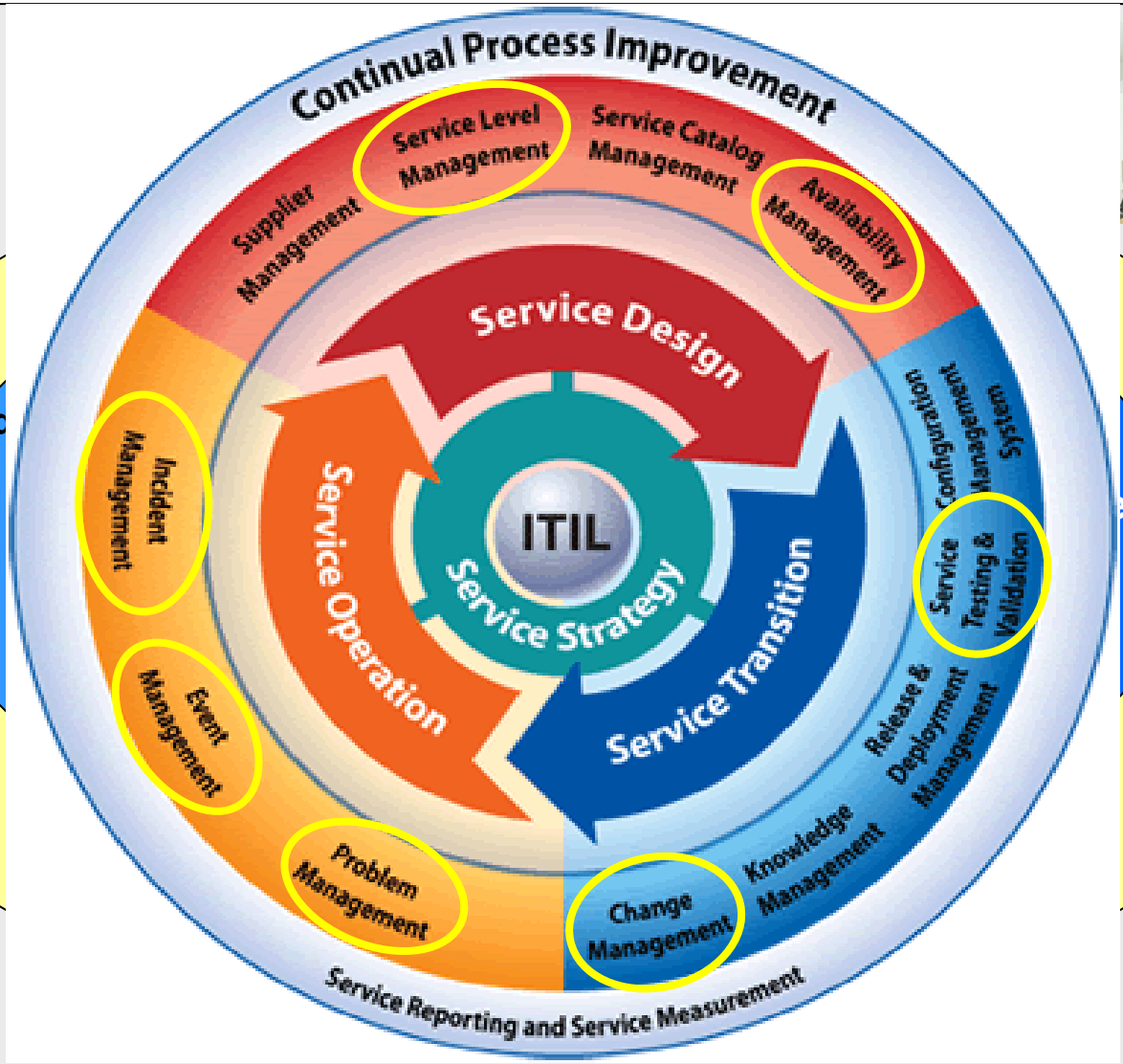
Données

Réplication des données:
- Locale → synchrone
- Distante → asynchrone

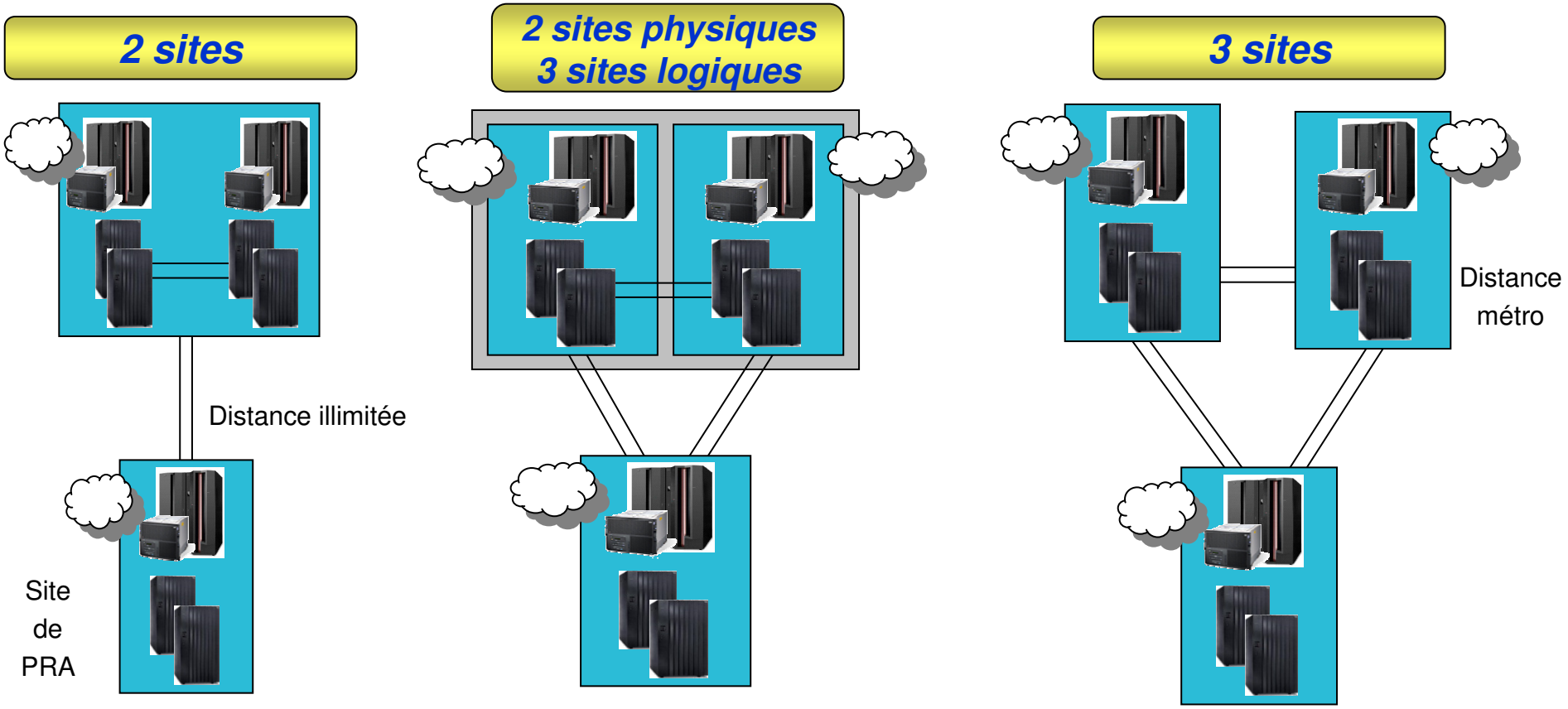
Service Management:
- Processus
(automatisation, monitoring, test, changements, incidents, problèmes…)
- Procédures
- Personnels

Principes de base de la résilience et du Service Management



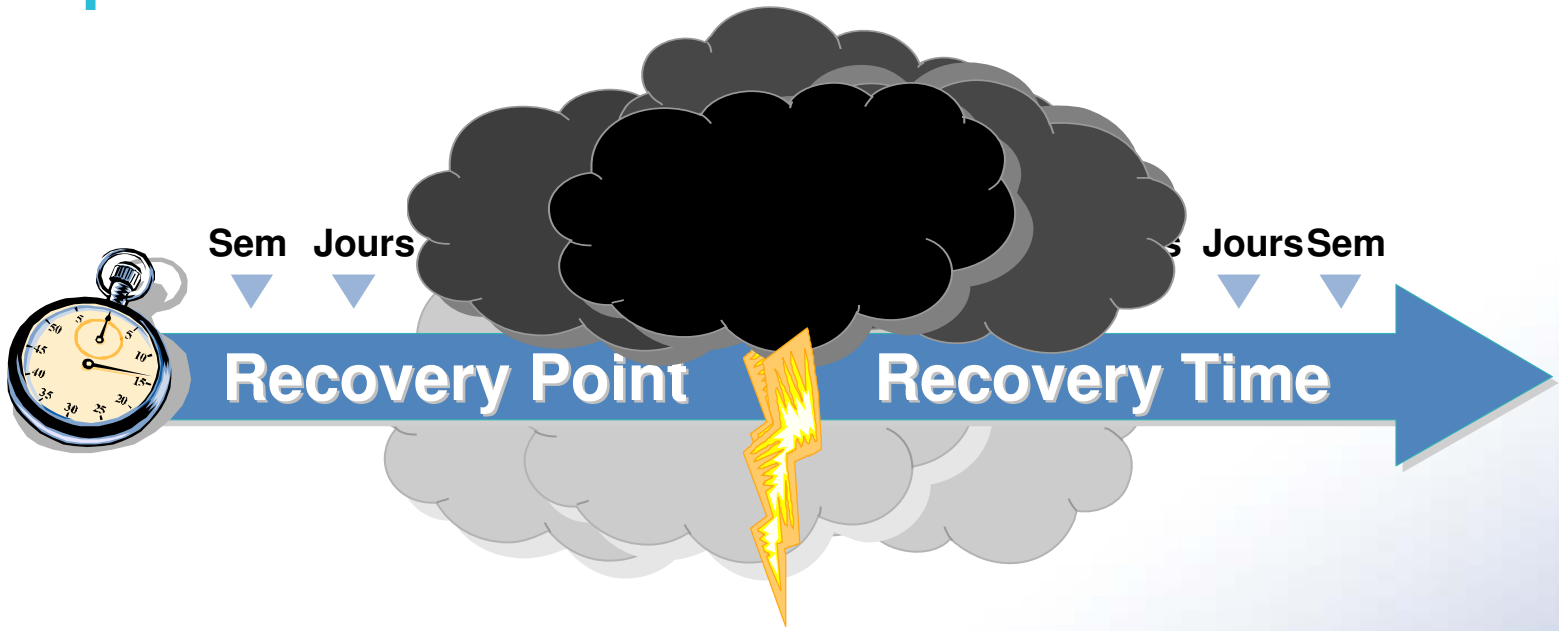


Exemples clients: tendances architecturales pour DC et PRA



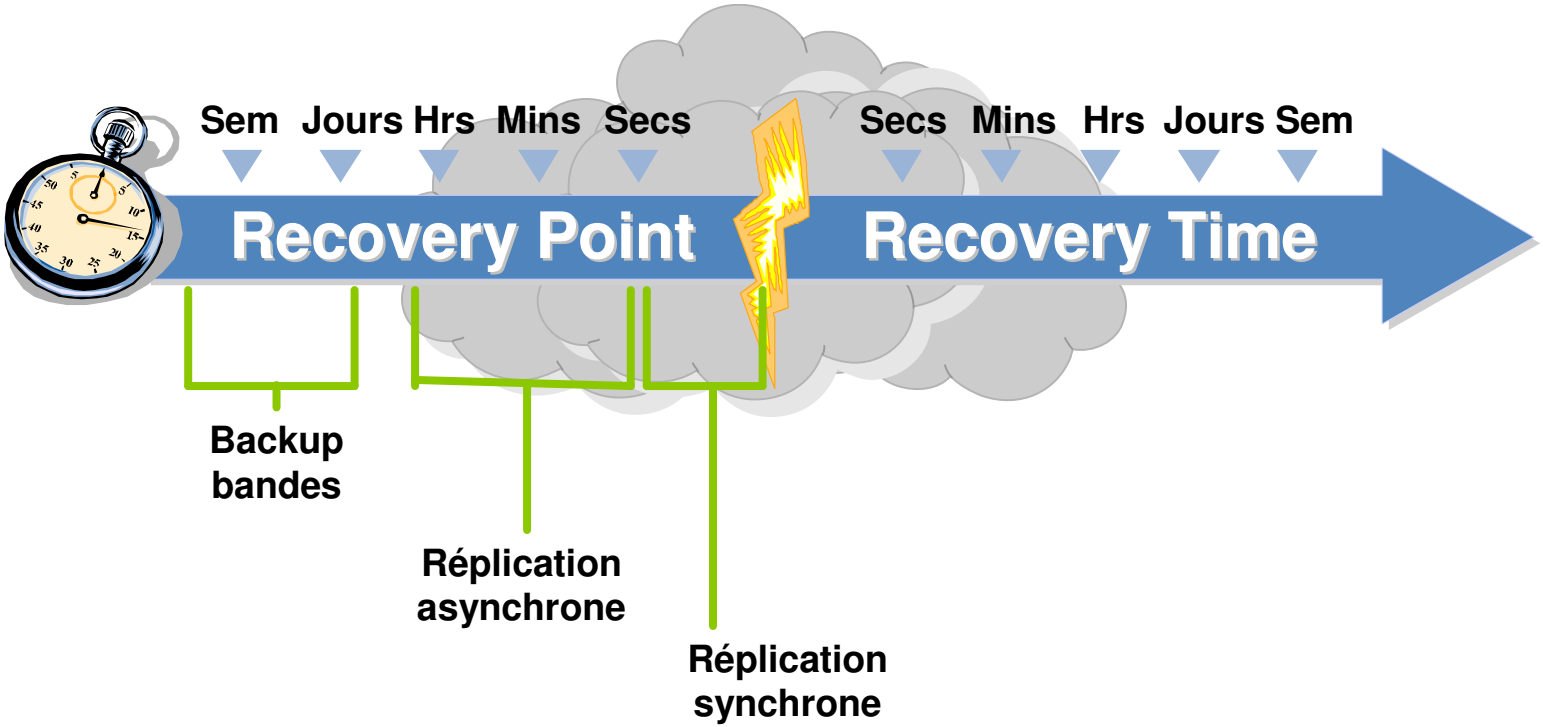
- **Pression exercée par les métiers et les règlementations :**
  - L'informatique fait désormais partie intégrante de la stratégie des sociétés. L'IT n'a plus seulement un rôle de support, les services de l'informatique sont désormais en prise directe avec les clients et contribuent à l'image de la société elle-même (*exemple typique du site web d'une société*).
    - Enquête du Gartner Group 2007: "*La plupart des compagnies qui ont subi un arrêt de leur informatique pendant au moins 8 jours ont purement et simplement disparu du marché*".
  - Diverses institutions de règlementation financière internationales exigent des solutions de PRA longue distance (Basel III, FSA, FED/SEC, Sarbanes Oxley, MiFID) et de disponibilité du service.

Concepts clés du PRA : RPO et RTO

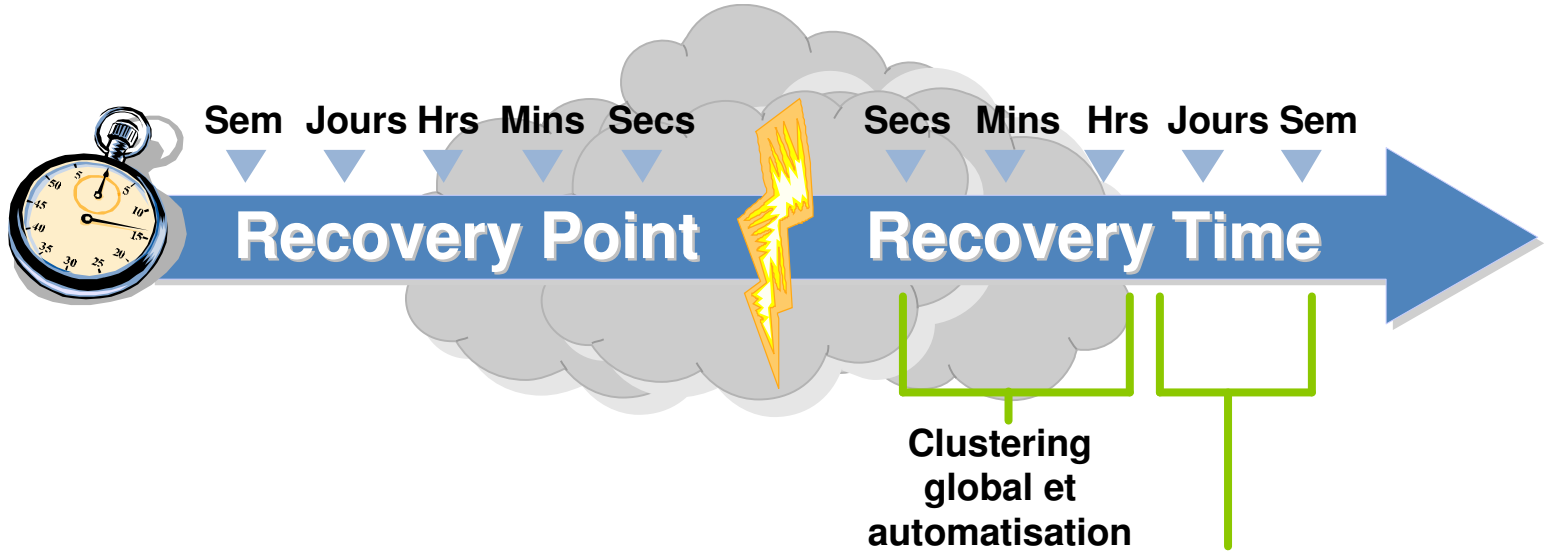


- **Recovery Point Objective (RPO)**
  - Quantité de données perdues en cas de sinistre – mesurée en unités de temps.
  - Après le redémarrage sur le site de PRA, quelle quantité de données acceptez-vous de perdre ?
- **Recovery Time Objective (RTO)**
  - Temps nécessaire pour redémarrer les services de l'informatique (systèmes, sous-systèmes, réseau, et applications).

La technologie de réplication des données oriente le RPO



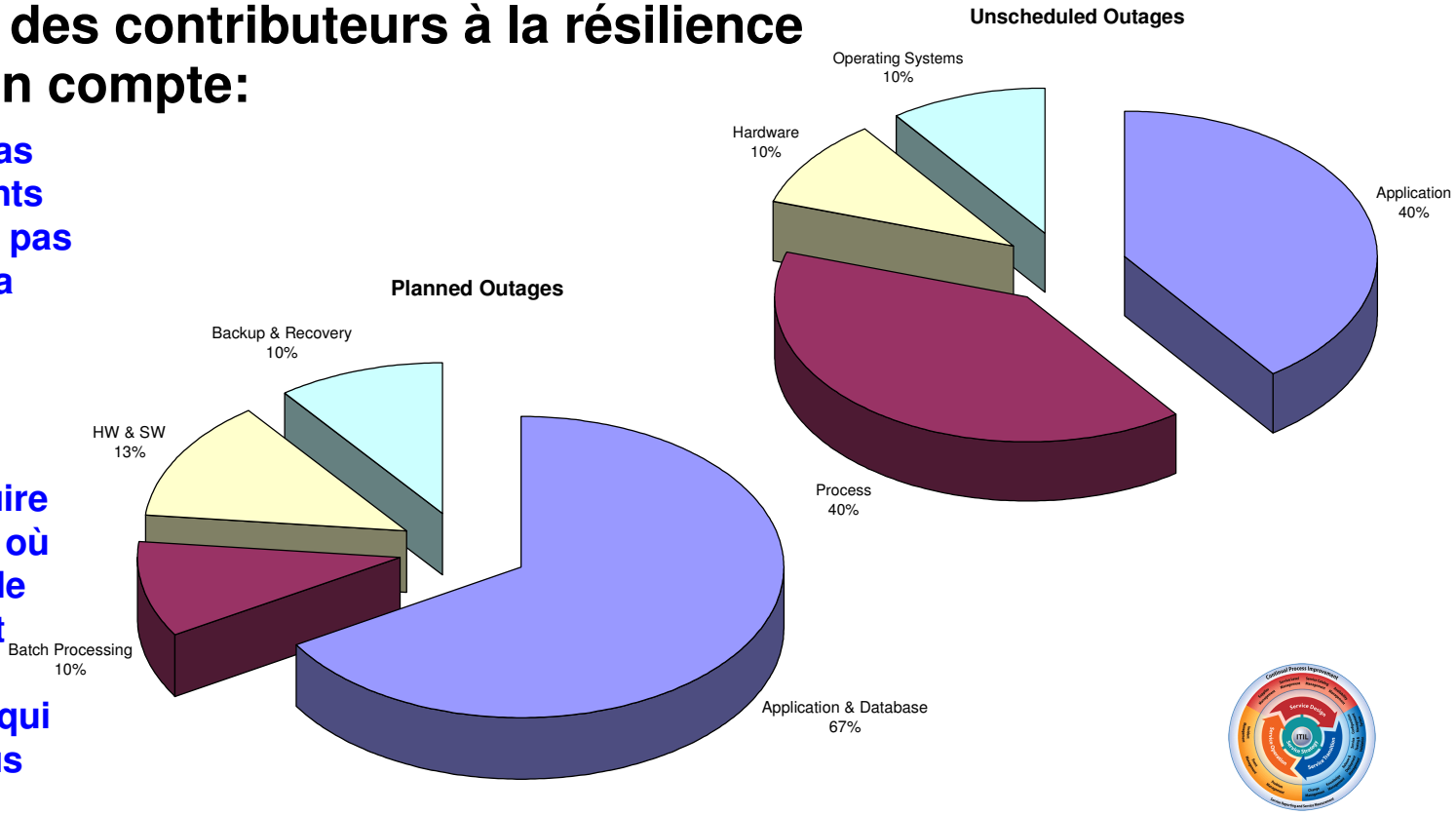
L'automatisation du redémarrage oriente le RTO



- **Le Recovery Time inclut:**
  - **La détection du sinistre**
  - **[Le temps de prise de décision]**
  - **Le redémarrage des systèmes, sous-systèmes, réseau**
  - **La restauration des données (ou leur validation)**
  - **Le redémarrage des applications**

Comment les processus de gestion de l'IT influencent la résilience

- **Si l'on se contente d'analyser les composants HW et SW, seuls environ 20% des contributeurs à la résilience seront pris en compte:**



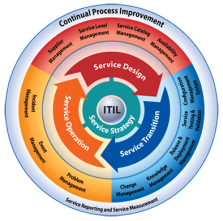
- **Cela ne signifie pas que les composants HW & SW ne sont pas importants pour la résilience…**
  → Ils en sont les fondations.
  → Leur fiabilité permettra de réduire le nombre de fois où les mécanismes de résilience devront être invoqués.
  → Et ce sont eux qui ont l'impact le plus élevé…

Nous devons prendre en compte la partie processus de gestion de l'IT (personnels, procédures, documentation, test, changements…).

- **La partie applicative est également un très fort contributeur...**

Comment les processus de gestion de l'IT influencent la résilience

- **Qu'est-ce que le framework ITIL (**Information **T**echnology **I**nfrastructure **L**ibrary**)?**
  - ITIL définit la plupart des processus nécessaires au support et au delivery de l'informatique :
    - Niveau de service
    - Configuration
    - Incidents
    - Problèmes
    - Changements
    - Capacité
    - Disponibilité
    - Alerte…



  - ITIL fournit un ensemble standard de concepts et de terminologie.
  - ITIL est un guide pratique pour plusieurs processus clés.
  - **ITIL établit une distinction entre la gestion des incidents et la gestion des problèmes.**
  - **ITIL se focalise sur le service rendu aux utilisateurs.**
  - *ITIL en tant que tel ne garantit pas un haut niveau de résilience ni une haute qualité de service.*

Améliorer la disponibilité de l'infrastructure IT → évaluer les contributeurs clés

- **Revue de l'architecture:**
  - Parcourir les transactions clés des applications les plus critiques.
  - Comprendre chacun des composants d'infrastructure HW & SW qui supportent ces transactions.
  - Identifier les **limitations ou les points faibles** qui pourraient affecter la disponibilité (***"Que se passerait-il si…"***) → Component Failure Impact Analysis (CFIA).

- **Identifier et résoudre les Single Point of Failure (SPoF):**
  - Un composant est un SPoF si le service délivré aux utilisateurs est interrompu en cas d'arrêt (planifié ou non).
  - Ce peut être un composant logiciel (http server, WAS, DB2, Oracle), un composant applicatif, un canal, une partition logique, une machine serveur, un sous-système de disques, etc...
  - Vis à vis de la disponibilité, tous les SPoF doivent être résolus à l'aide de solutions technologiques (majoritairement basées sur **la tolérance de panne utilisant la redondance et la bascule automatique de la charge**).
  - *La panne d'un composant doit être adressée par des capacités/solutions de Disponibilité Continue, et non pas par des solutions de PRA…*

Améliorer la disponibilité de l'infrastructure IT → évaluer les contributeurs clés

- **Rev**
  - P
  - C ent ces tr
  - Id d (CFIA).
- **Ide**
  - U ou en c
  - C posant a tème d
  - V lutions te **t la r**
  - *L D*

Améliorer la disponibilité de l'infrastructure IT …

- **Stratégie de maintenance:**
  - Sachant qu'environ ~20% des incidents auraient pu être évités par un correctif disponible depuis 6 mois ou plus, il est recommandé d'appliquer une stratégie de maintenance préventive, même si nous sommes conscients qu'*une stratégie unique de maintenance ne peut pas s'appliquer à tous les environnements…*
    - Exemple de recommandations IBM pour la maintenance System z:
      - Installer les Recommended Service Upgrades (RSU) au moins 2 à 4 fois par an permettra de réduire les risques d'incidents liés à des bugs.
      - Mettre en place les mêmes niveaux de RSU pour tous les produits majeurs permettra de réduire les risques de conflits inter-produits et de tirer bénéfice des tests intégrés d'IBM.
      - Surveiller régulièrement les correctifs HIPER (High Impact) et Programming Error (PE) APAR.
      - Revoir et installer régulièrement les HIPER HW.
      - Installer les nouveaux niveaux de micro-code recommandés par IBM (MicroCode Level (MCL)), au minimum chaque trimestre.
- **Stratégie de test:**
  - Tester et valider à la fois les changements systèmes et applicatifs avant de les appliquer en Production:
    - Dans un environnement de test **séparé** qui a la même architecture que celui de Production: cluster PowerHA, Oracle RAC, données (type et volumétrie), charge (nb de transactions) → **de bout en bout**.
  - Planifier attentivement le passage en Production (utiliser les possibilités de "rolling change" de l'infrastructure).

Améliorer la disponibilité de l'infrastructure IT …

- **Automatiser:**
  - L'automatisation permet **des réactions plus rapides, plus fiables et répétables** en cas d'incident:
    - Exemples: PowerHA, System Automation, GDPS… *Les SW ne subissent pas de stress !*
- **Maintenir et améliorer le niveau de compétences des opérateurs:**
  - Les opérateurs sont les **pilotes** de votre IT:
    - Ils sont souvent les premiers avertis d'un incident.
    - Ils doivent être préparés à réagir en utilisant des procédures pré-testées (*si non automatisées*).
    - Ils doivent se focaliser sur la **restauration du service aux utilisateurs** (*et non pas sur la correction du problème*).
- **Capacity planning:**
  - Il convient de s'assurer que les systèmes de backup ont toutes les fonctionnalités et la capacité de tenir la charge en cas de bascule.

Améliorer la disponibilité de l'infrastructure IT …

- **Automatiser:**
  - L'automatisation permet **des réactions plus rapides, plus fiables et répétables** en cas d'incident:

…n, GDPS… *Les SW ne subissent pas de stress !*

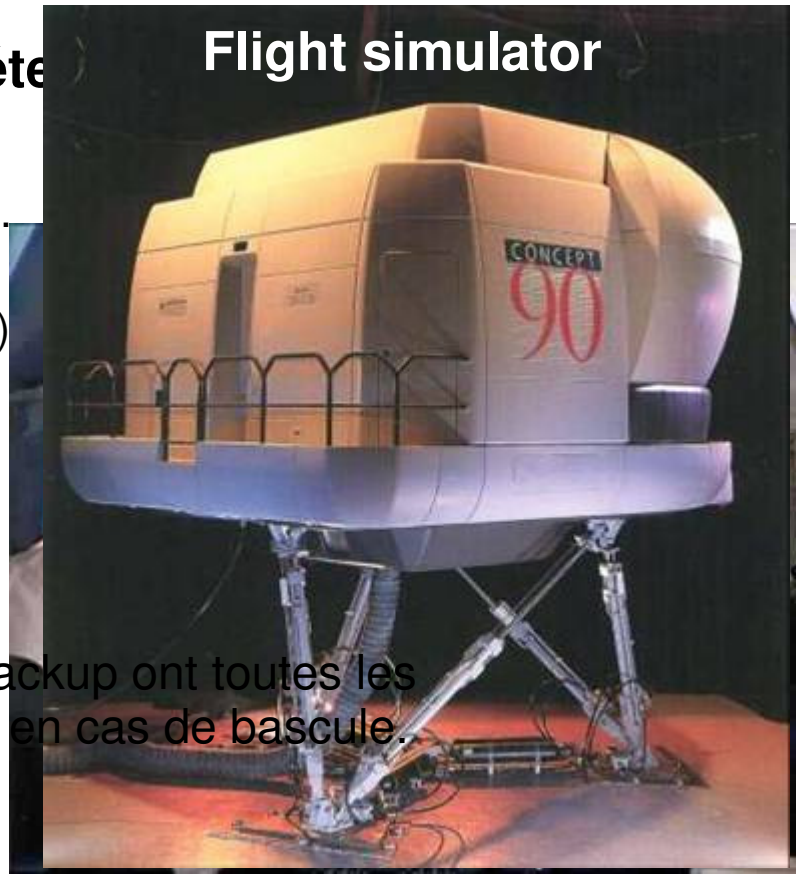
…compéte…

…e IT:

…incident.

…ant …*matisées*)

…n du …*la*

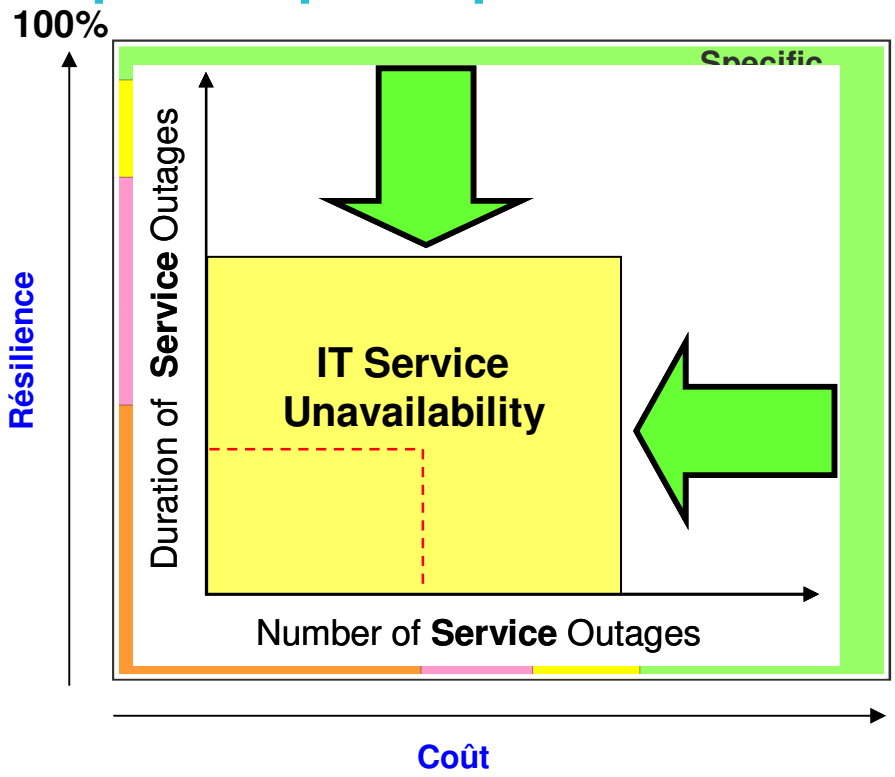


- **Capacity planning:**
  - Il convient de s'assurer que les systèmes de backup ont toutes les fonctionnalités et la capacité de tenir la charge en cas de bascule.

Voleriez-vous dans cet avion ?

Conclusion: la résilience IT commence par des produits fiables, mais ne peut être atteinte sans processus de gestion efficaces et sans prise en compte d'un design adapté et spécifique

1. Commencer par des produits fiables.
2. Mettre en place des processus de gestion des services efficaces.
3. Enfin étudier des solutions spécifiques pour la résilience.



Les améliorations de résilience peuvent résulter de la mise en œuvre d'une des étapes ou de plusieurs, mais… la *résilience* nécessite une approche équilibrée de toutes ces solutions.

La résilience IT est un projet sans fin…

Résilience de l'infrastructure informatique

jdenis@fr.ibm.com

- Comment le **HACoC** de Montpellier (High Availability Center of Competency) **peut vous aider à améliorer la résilience de votre infrastructure informatique ?**

Mission du HACoC (High Availability Center of Competency)

- **L'entité High Availability Center of Competency est une équipe IBM cross organisations (STG, SWG, GTS) dont la mission consiste à:**
  - Travailler avec les clients pour les aider à améliorer la résilience de leur ***infrastructure IT*** et leurs ***processus de service management.***

- **L'équipe HACoC-Europe (IBM Client Center, Montpellier - France):**

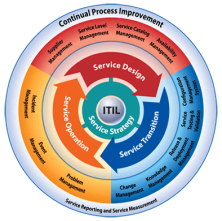
Jocelyn Denis
Engagement Leader
Team Leader

Pierre Dejean
Engagement Leader

Christian Monvoisin
Service Management Specialist

Site web HACoC-Europe:

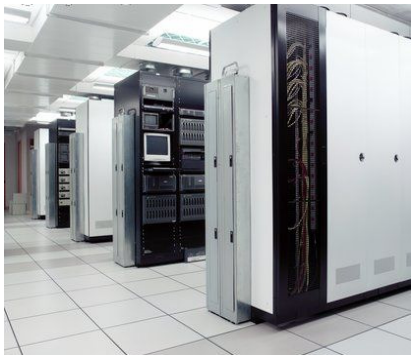
http://www.ibm.com/ibm/clientcenter/montpellier/dc-ha.shtml



Comment le HACoC peut vous aider sur la résilience de l'IT

Nous aidons les clients à **atteindre les objectifs de résilience** de leur infrastructure IT pour **limiter les risques** et **améliorer le service rendu aux utilisateurs et clients**. Concrètement, un assessment HACoC peut vous aider à répondre aux questions et aux problèmes suivants:

Où en êtes vous **en terme de disponibilité et/ou PRA ?**



Quelle est votre **situation actuelle** en terme de résilience de votre infrastructure IT ?

(technologie & processus)

Où devez vous aller **en fonction de vos besoins métiers ?**

Combien de données acceptez vous de perdre ?

Combien de temps pouvez vous rester sans informatique ?

Comment y parvenir **à partir de votre infrastructure et de vos processus ?**

Nous vous proposons une **étude d'architecture** et une **roadmap** d'implémentation en accord avec vos objectifs de résilience.

Méthodologie du workshop HACoC

En fonction des **besoins métiers** et des **objectifs de continuité des opérations**, nous allons effectuer une revue de l'infrastructure IT, et de la façon dont la technologie et le service rendu sont gérés (au sens ITIL).

A l'issue des 2 jours de workshop, nous fournirons un rapport de **recommandations technologiques et processus « haut niveau »,** ainsi qu'une **roadmap** d'implémentation pouvant aider le client à atteindre ses objectifs de résilience.