X-SPIErience Day 2020

SOUVERAINETÉ NUMÉRIQUE

SPIE

cisco Partner

FORTINET

HUAWEI

SPIE, sharing a vision for the future

X-SPIErience Day 2026
SOUVERAINETÉ NUMÉRIQUE

SPIE

Revue des impacts business et plans de résilience avec la montée des risques géopolitiques

MOHAMED CHAABOUNI

Information Security & Data Privacy Consultant
SPIE ICS

Agenda

- Introduction - risques liés à la dépendance numérique
- Situation géopolitique et contexte
- Outils et comment intégrer les risques dans la planification de la résilience
- Le chemin vers la résilience est un parcours à long terme (Focus sur BIA)
- Points clés à retenir

Monde numérique interconnecté et Stratégie

Souveraineté **Continuité**

Souveraineté Numérique et Continuité d'Activité
Introduction – Cas CPI

Institution internationale :
Cour Pénale Internationale
Signature et ratification du «**Statut de Rome**» par une majorité de pays
Siège : La Haye
Composition : 18 Juges élus

Souveraineté Numérique et Continuité d'Activité
Introduction – Cas CPI

Février 2025:
Sanctions US contre des juges:

- Interdiction voyage
- Gel des avoirs
- Interdiction à toute personne morale ou physique de fournir des services (inclue EU)
- + Sous enquête

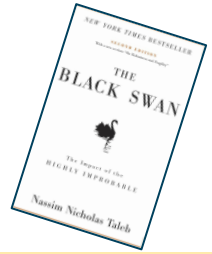
Souveraineté Numérique et Continuité d'Activité
Introduction – Cas CPI

Emails → Proton (CH)
MS → OpenDesk (DE)
Paiements ?...
Autres services ? …
Recherche d'alternatives

EU
CH

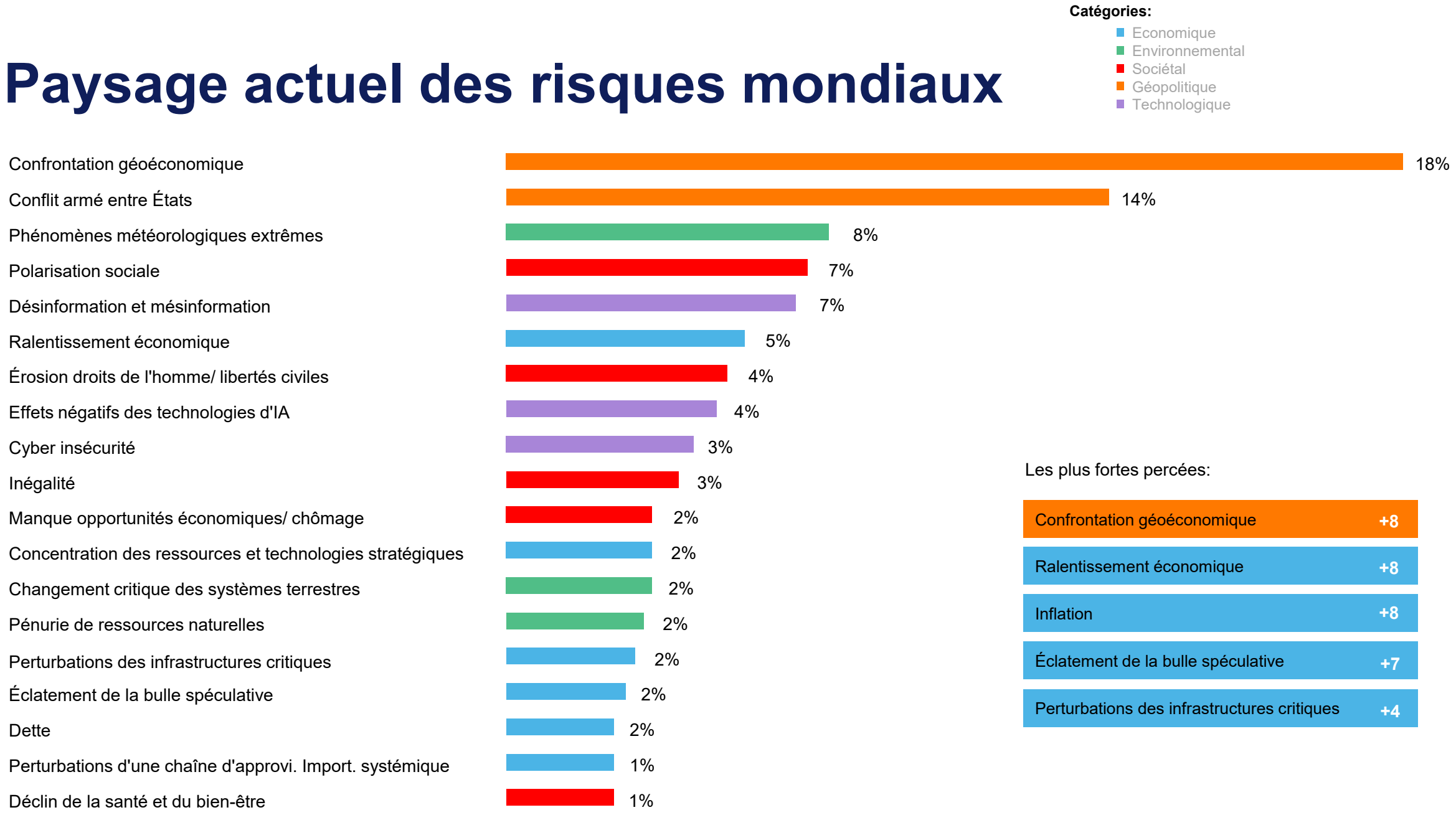
Régulation ≠ Solutions

Etiez-vous préparés?



	Premiers pas 80's – 90's	Années 2000	Années 2010	Années 2020
Légal	BCBS 109 Comite Bâle	BS 25999-1:2006 BS 25999-2:2007 Patriot Act	Bale II ISO 22301:2012 Cloud Act ISO 22316:2017	Bale III EU Cyber Resilience ACT ISO 22361: 2022 NIS 2 FINMA DORA
Evènements	2e Choc pétrolier 3e Choc pétrolier	9.11 Guerre MO	Crise Eco ▲Cybercriminalité	Covid Crise ▲▲ Cybercriminalité Guerre Ukraine Guerre MO
Technologie	Premiers PCA (Banques, Assurances) RAID SMS backup magn Datacenters	Internet VoIP Réseaux Sociaux Clés USB	Cloud IA Mobilité	Gen AI Agentic AI Mobilité Multi-cloud

Paysage actuel des risques mondiaux



Les plus fortes percées:

Confrontation géoéconomique	+8
Ralentissement économique	+8
Inflation	+8
Éclatement de la bulle spéculative	+7
Perturbations des infrastructures critiques	+4

Source : WEF_Global_Risks_Report_2026.

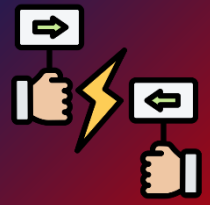
Tensions géopolitiques et conditions extrêmes

Conflits / Guerres

Instabilité / crise économique

Sanctions / Taxes

Polarisation / rivalités



Conditions climatiques extrêmes

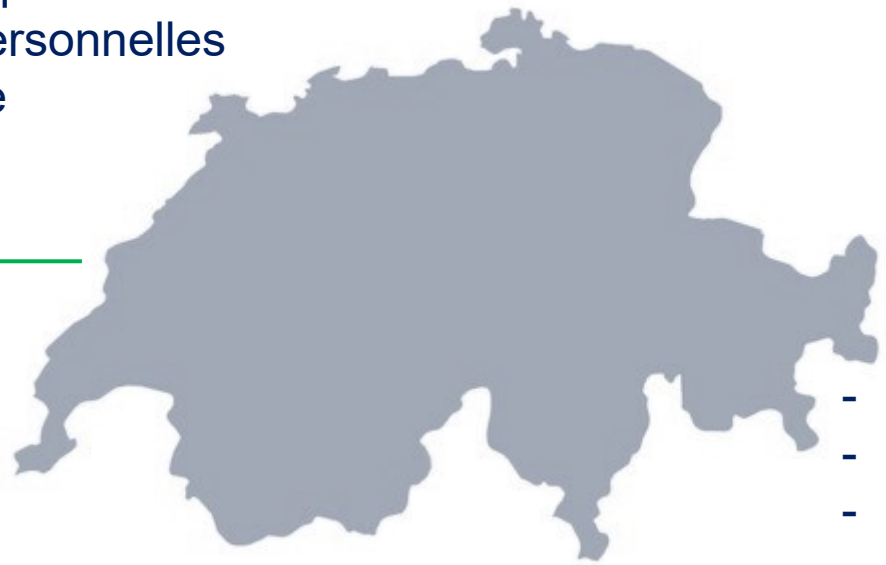
Cyberattaques

Dépendance technologique

Perturbation chaines d'approvisionnement

Situation Suisse

+ Neutralité et stabilité politique
+ Protection des données personnelles
+ Ecosystème Cybersécurité
+ Infrastructure de qualité

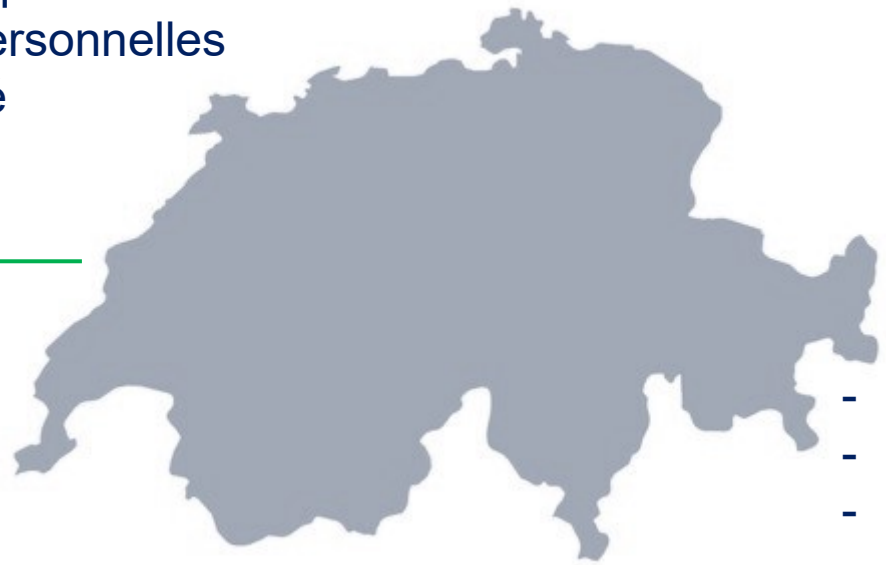


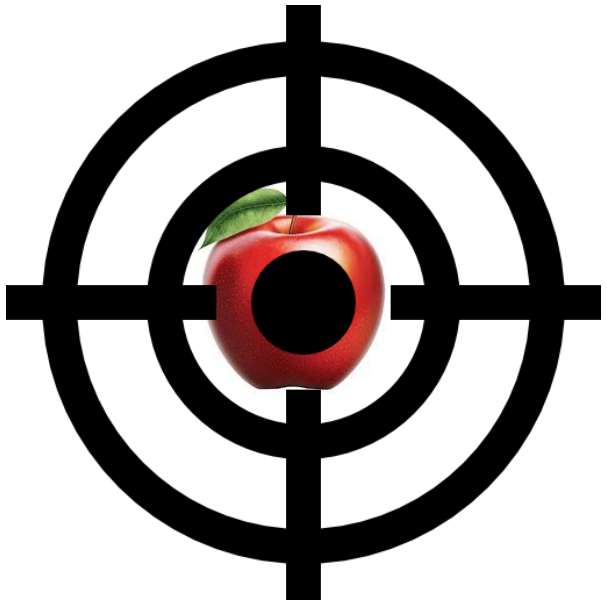
- Coûts de développement élevés
- Dépendance aux fournisseurs étrangers
- Manque de géant techno (taille GAFAM)
- Complexité règlementaire cross-border

Fenêtre de tir étroite,

Situation Suisse

+ Neutralité et stabilité politique
+ Protection des données personnelles
+ Ecosystème Cybersécurité
+ Infrastructure de qualité





- Coûts de développement élevés
- Dépendance aux fournisseurs étrangers
- Manque de géant techno (taille GAFAM)
- Complexité règlementaire cross-border

Fenêtre de tir étroite,

Qu'est-ce que la résilience ?

Latin « Resilientia »

Le « fait de rebondir »

Qu'est-ce que la résilience ?

Solution adaptée:

- A votre contexte et besoin
- Au terrain

« **Permacrise** »
Besoin de redéfinir la notion de résistance aux crises
Admettre et reconnaitre les dangers

Au niveau de l'entreprise - ISO 22301 & ISO 22316

ISO 22301 - Sécurité et résilience — Systèmes de management de la continuité d'activité — Exigences

Au niveau de l'entreprise – Normes ISO

ISO 22361 - Sécurité et résilience — Gestion de crise — Lignes directrices

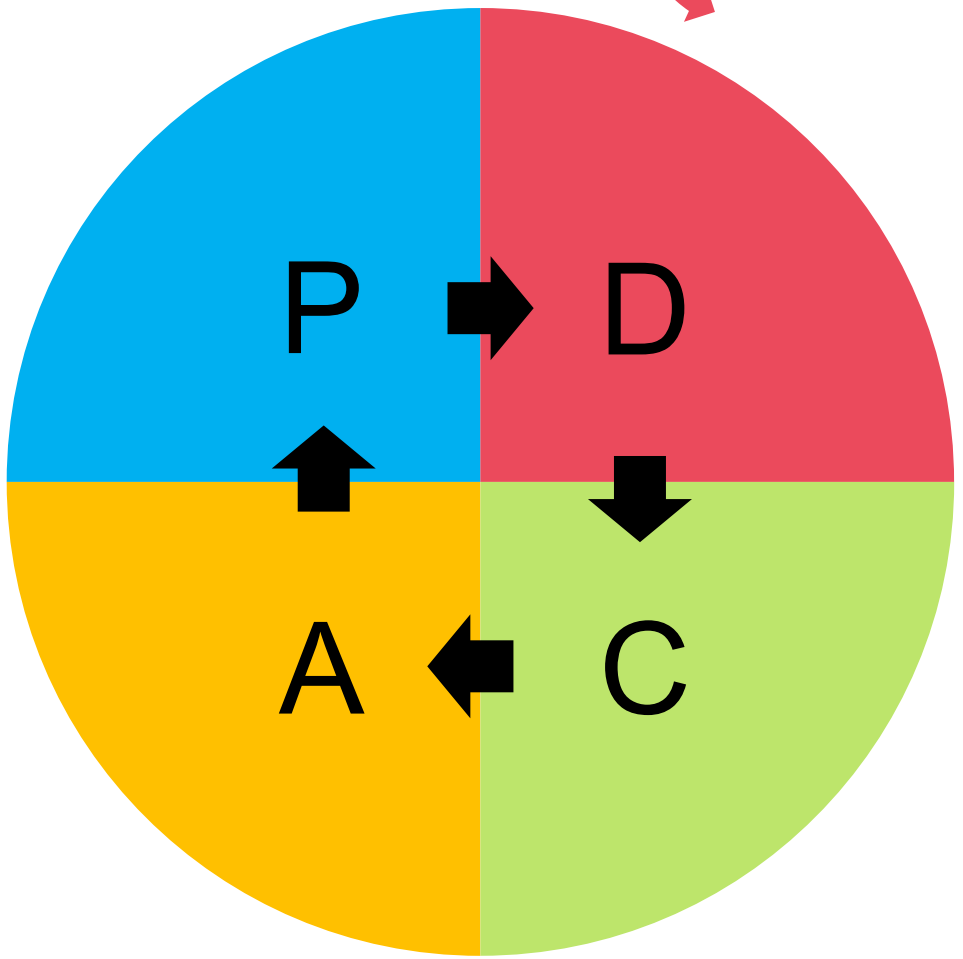
Au niveau de l'entreprise – Normes ISO

ISO 22316 - Sécurité et résilience — Résilience organisationnelle — Principes et attributs

Quelle est la solution ?
La roue (Run Flat)

Intégrer les nouveaux risques !!!

PLAN
Mettre en place:
- Un programme
- Une organisation
- Un système de management et documentation



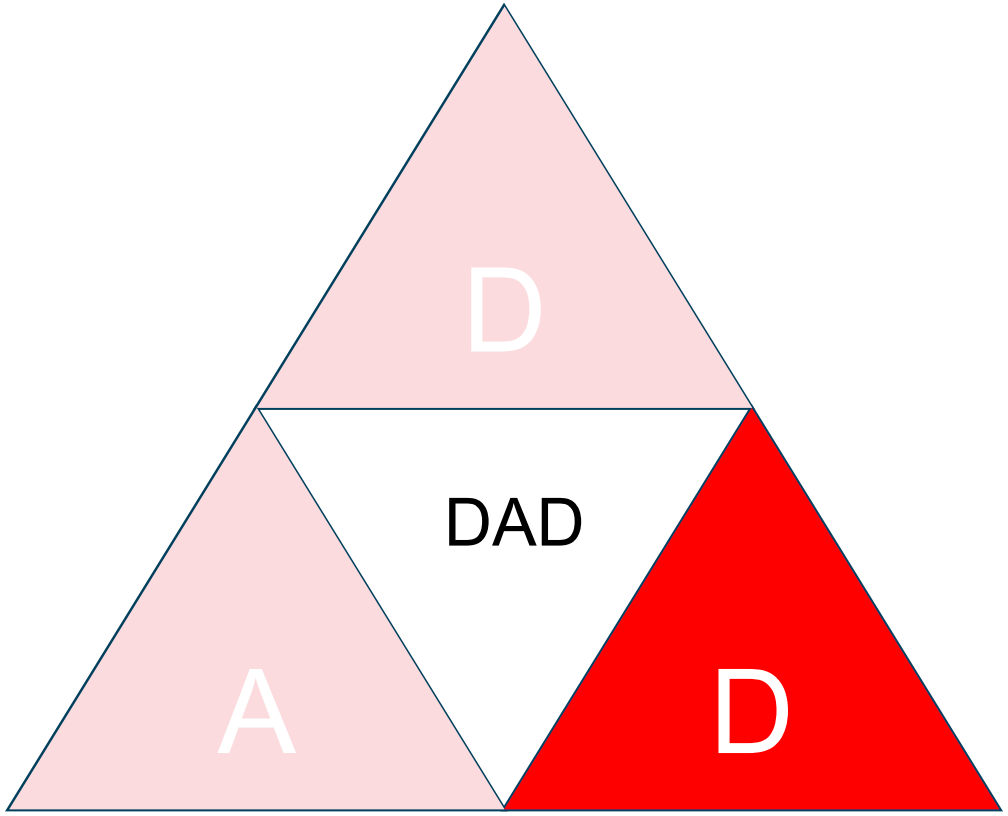
DO
- BIA & Evaluation des Risques
- Définir Stratégie BCP
- Etablir & implémenter (IT)
- Plans & procédures

ACT
- Actions correctives
- Amélioration continue

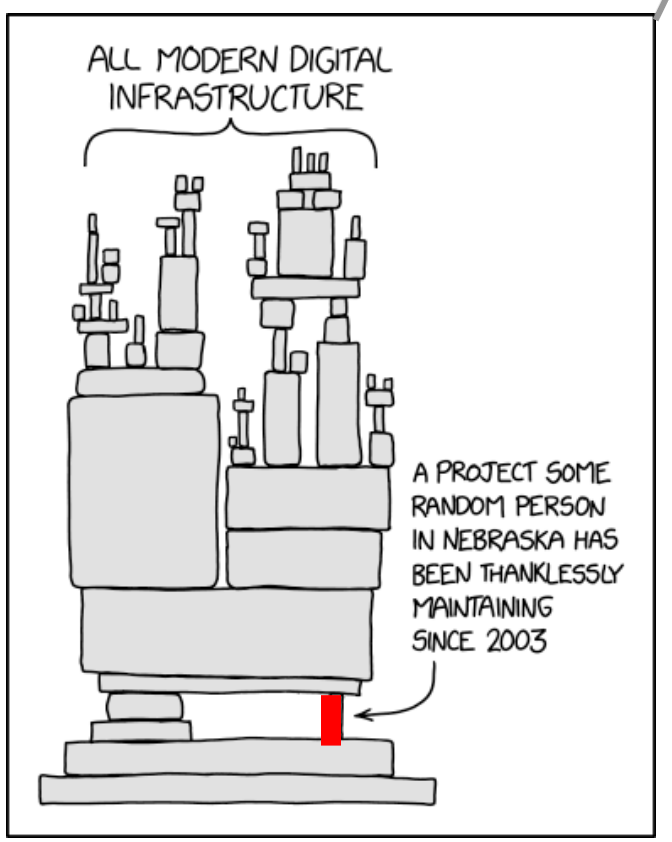
CHECK
- Test et exercices
- Audit interne
- Evaluation performance

Importance du PCA

Que couvre un plan de continuité d'activité ? – Triade pilier Sécurité



CIA : Confidentiality, Integrity, Availability
DAD : Disclosure, Alteration, Destruction



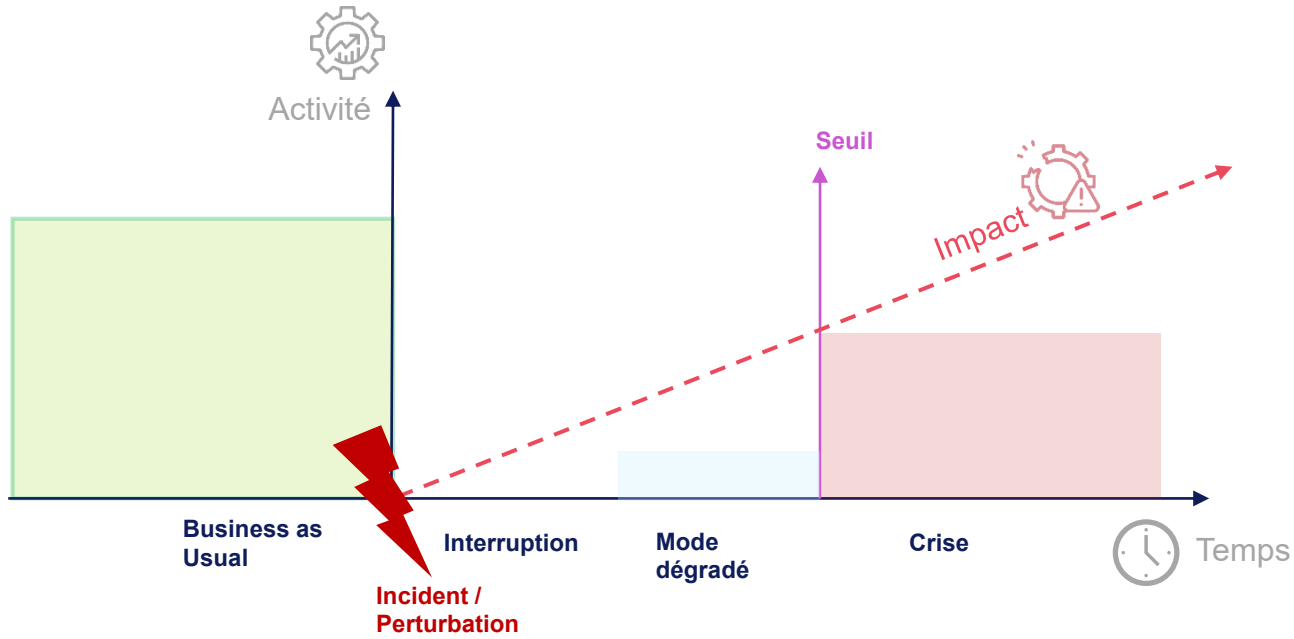
Single Points of Failure

Interdépendances / interruption chaine d'approvisonnement

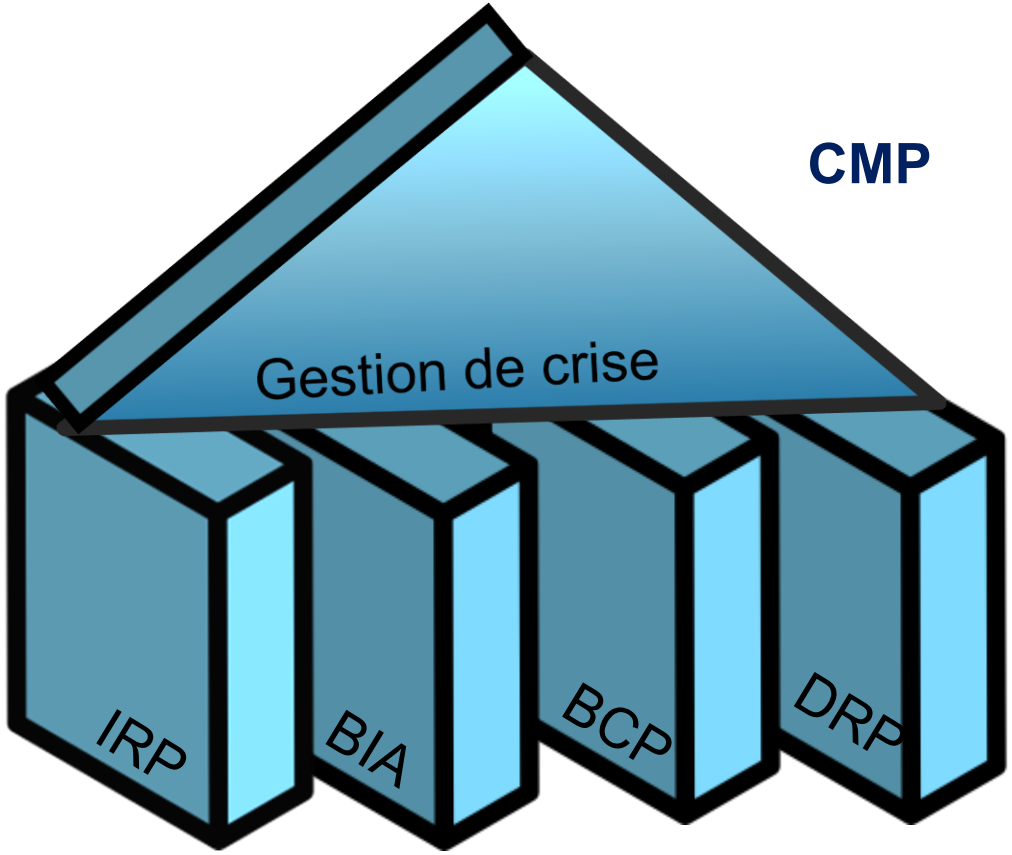
De la gestion d’incidents…

A la gestion de crise

D’une interruption à la gestion de crise

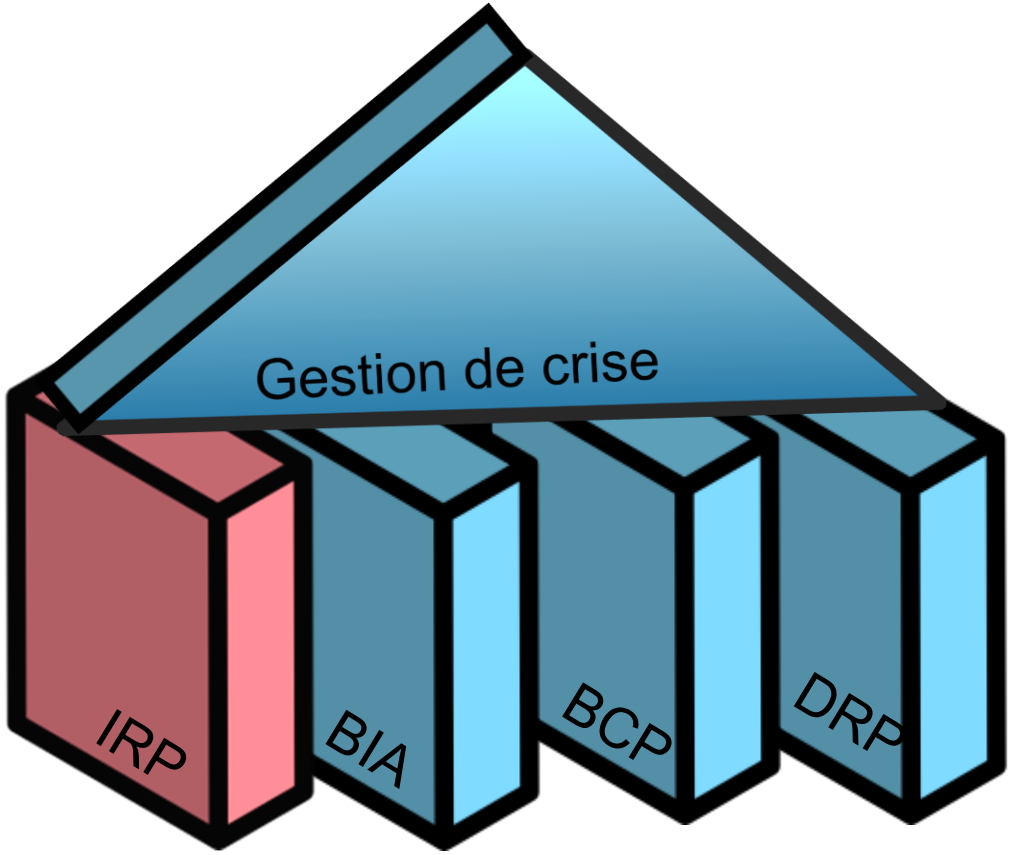


Les piliers de la résilience



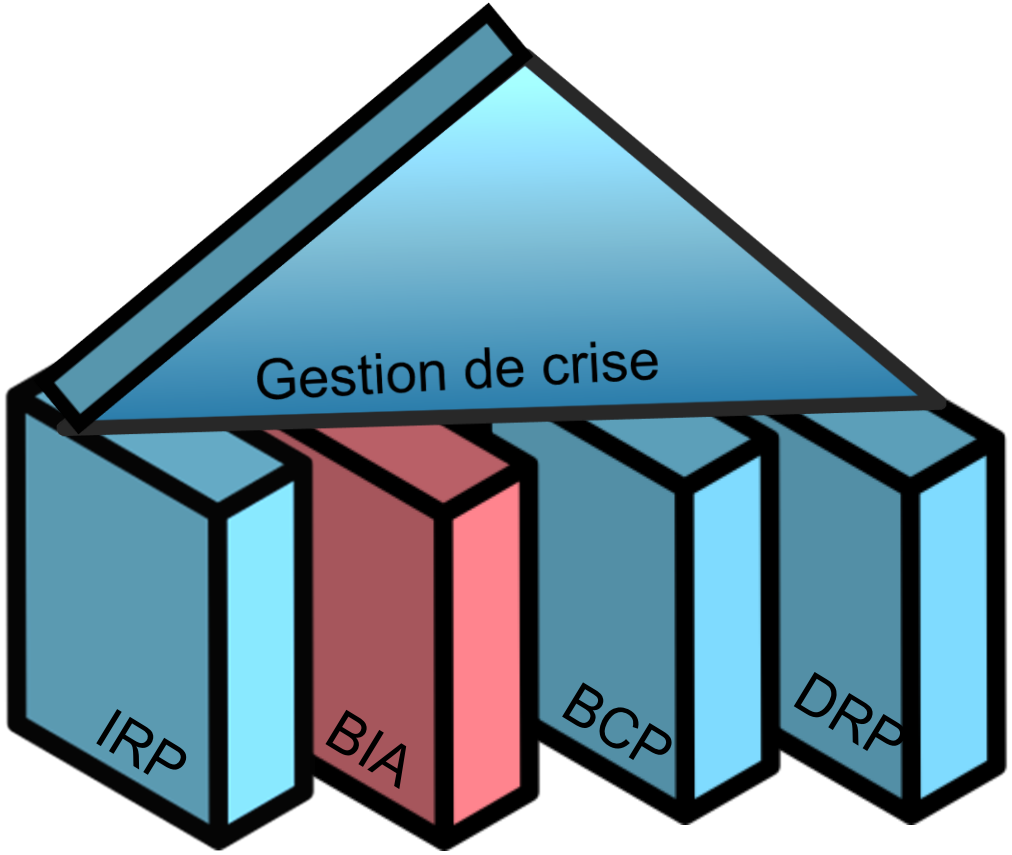
Gestion de Crise : **CMP**
Gestion des incidents : **IRP**
Bilan d'Impact sur Activité : **BIA**
Plan de Continuité d'Activité : **PCA**
Plan de Reprise d'Activité : **PRA**

Les piliers de la résilience



L'Incident Response Plan (IRP) est un plan détaillé qui définit comment une organisation doit détecter, répondre et se rétablir face à des incidents de sécurité ou perturbations majeures. Ce document spécifie les rôles, responsabilités et procédures pour traiter efficacement une menace ou une attaque.
L'IRP vise à **contenir l'incident**, **limiter l'impact** sur les opérations et protéger les actifs essentiels de l'organisation. Il prévoit également des étapes pour analyser la cause de l'incident et améliorer les dispositifs de protection. Des exercices réguliers permettent de tester la réactivité et l'efficacité du plan afin d'assurer la préparation de tous les acteurs impliqués.

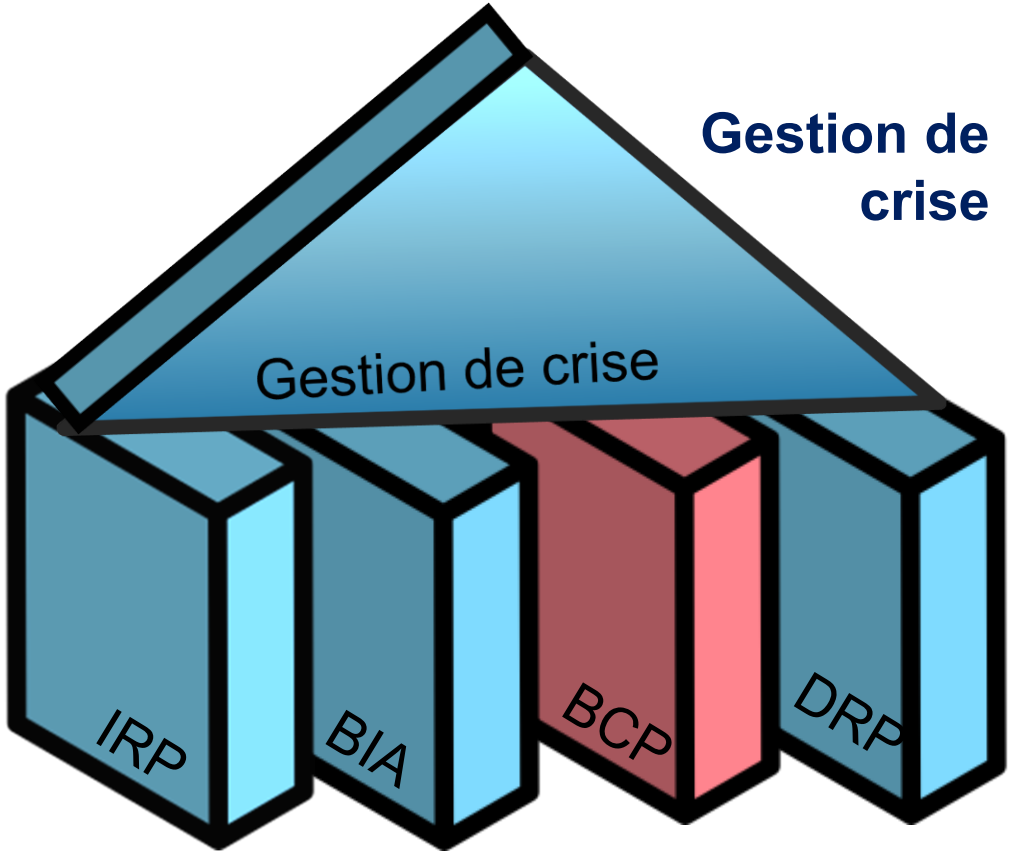
Les piliers de la résilience



Le BIA permet d'identifier les processus critiques de l'organisation et d'évaluer les conséquences d'une interruption.

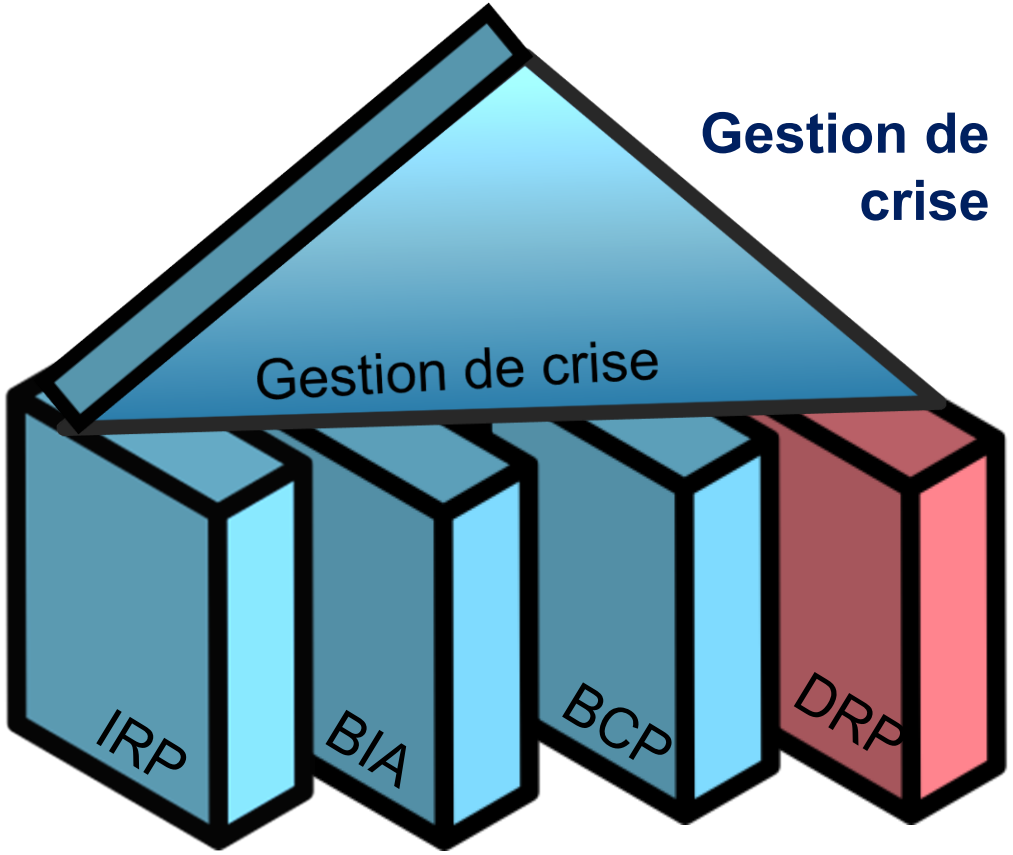
Il aide à définir les priorités de reprise et à estimer les pertes potentielles.
Le BIA est un outil clé dans la préparation à la continuité d'activité. Il sert aussi de base à l'élaboration des plans de reprise.
Ce diagnostic guide les investissements en matière de résilience.

Les piliers de la résilience



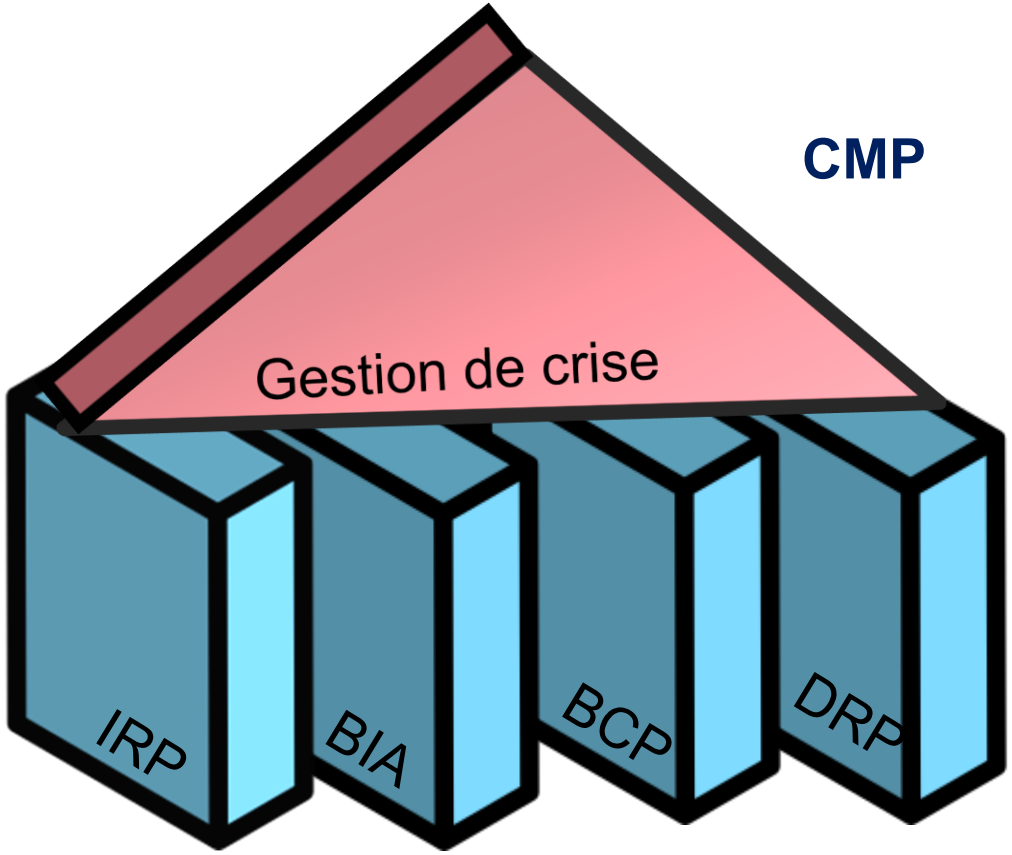
Le **BCP** documente les mesures à prendre pour maintenir ou rétablir les activités vitales de l'organisation en cas de perturbation majeure. Il décrit les ressources, les processus et les équipes responsables. Son objectif principal est de minimiser les interruptions et les dommages pour la société. Le PCA doit être testé régulièrement pour garantir son efficacité. Il fait partie intégrante de la gestion des risques.

Les piliers de la résilience



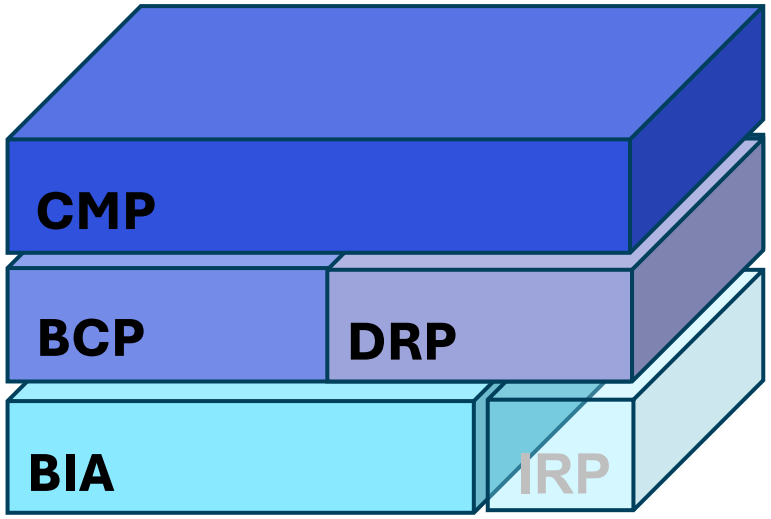
Le **DRP**, établit les procédures pour restaurer l'infrastructure informatique et les données après un incident majeur. Son but est de réduire le temps d'indisponibilité des systèmes critiques. Il détaille aussi la chaîne de communication et les responsabilités de chacun. Le DRP agit en complément du PCA mais se concentre principalement sur les aspects techniques et informatiques. Une bonne planification de la reprise garantit la résilience numérique de l'organisation.

Les piliers de la résilience



La **gestion de crise** regroupe l'ensemble des actions coordonnées pour faire face à une situation exceptionnelle qui menace la pérennité de l'organisation.
Cela comprend la **mobilisation** d'une **cellule de crise** et la communication interne et externe.
Son objectif est de **protéger les personnes**, les **actifs** et **l'image** de la société.
Une gestion efficace de la crise permet de prendre des décisions rapidement et de restaurer la confiance. Elle repose sur une préparation, des exercices réguliers et un retour d'expérience systématique.

Les piliers de la résilience



En réalité:

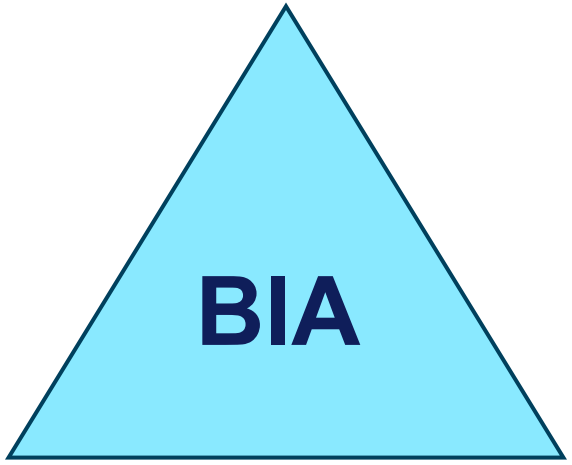
- **Le CMP** s'appuie sur ces éléments
- **Le DRP est une partie du BCP**
- **Le BIA** est en réalité est le socle

Les dimensions du BIA

Ressources essentielles

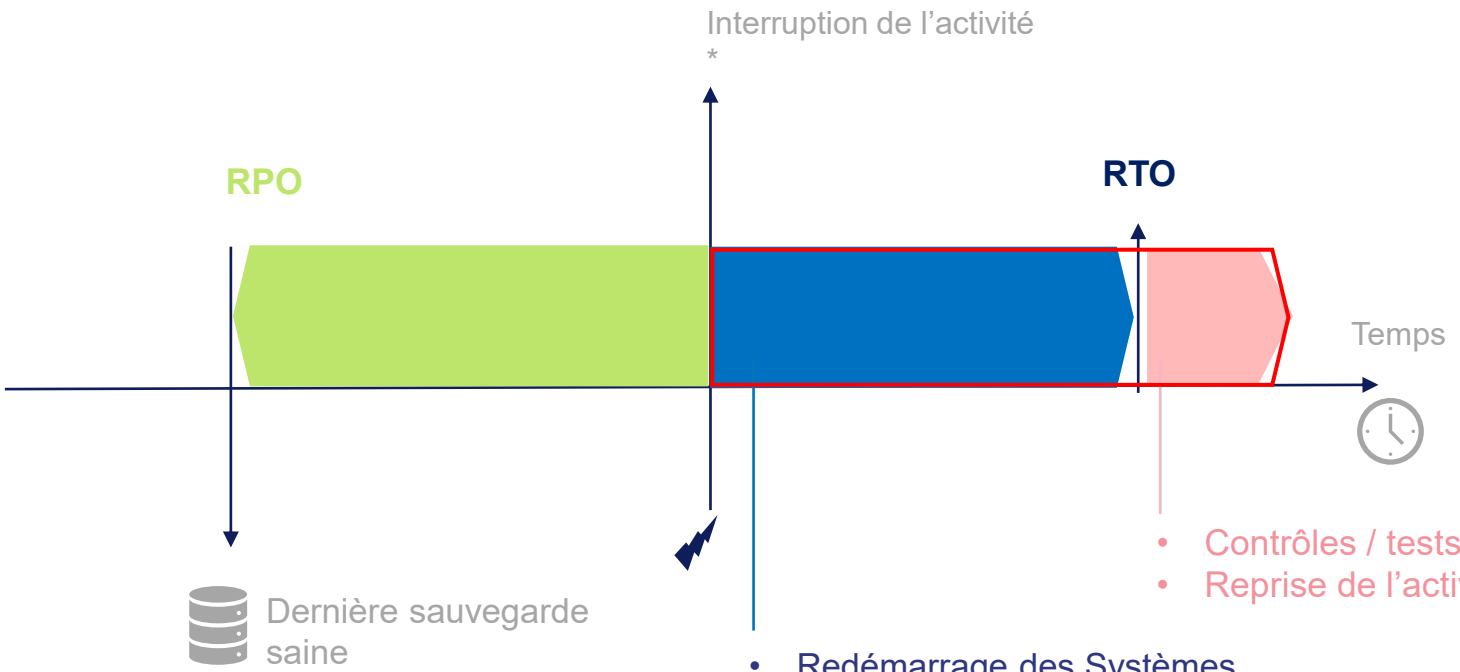
RH /
Capacités humaines

Equipment /
logistiques



IT /
Applications

Paramètres BIA



- Contrôles / tests...
- Reprise de l'activité

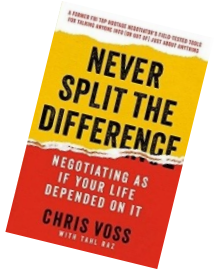
- Redémarrage des Systèmes
- Postes de travail, accès et habilitations
- Redémarrage de(s) application(s)
- Récupération des données

(*) Scénarii:
- Incident majeur IT
- Cyberattaque
- Perte bâtiment / Datacenter
- ...

Distinguer:
Demande métier & Offre IT

DMIA !

Objectifs de reprise



Impacts Possibles (cyberattaque ou perturbation prolongée)

Impacts Financiers
Impact financier direct

institution financière ou autre

Impacts légaux
Impact juridique et légal peut se traduire en impact financier. Pénalités élevées par exemple si protection de données personnelles non assurées

Impacts RH
Touchant la santé d'employés. Stress, anxiété.
Impact direct de patients dans des hôpitaux, Organismes humanitaires

Impacts de réputation
Impact de réputation pour personne ou pour l'image de l'entreprise. Peut se traduire en deuxième temps en impact financier

Impacts globaux
Impact sociétal ou environnemental

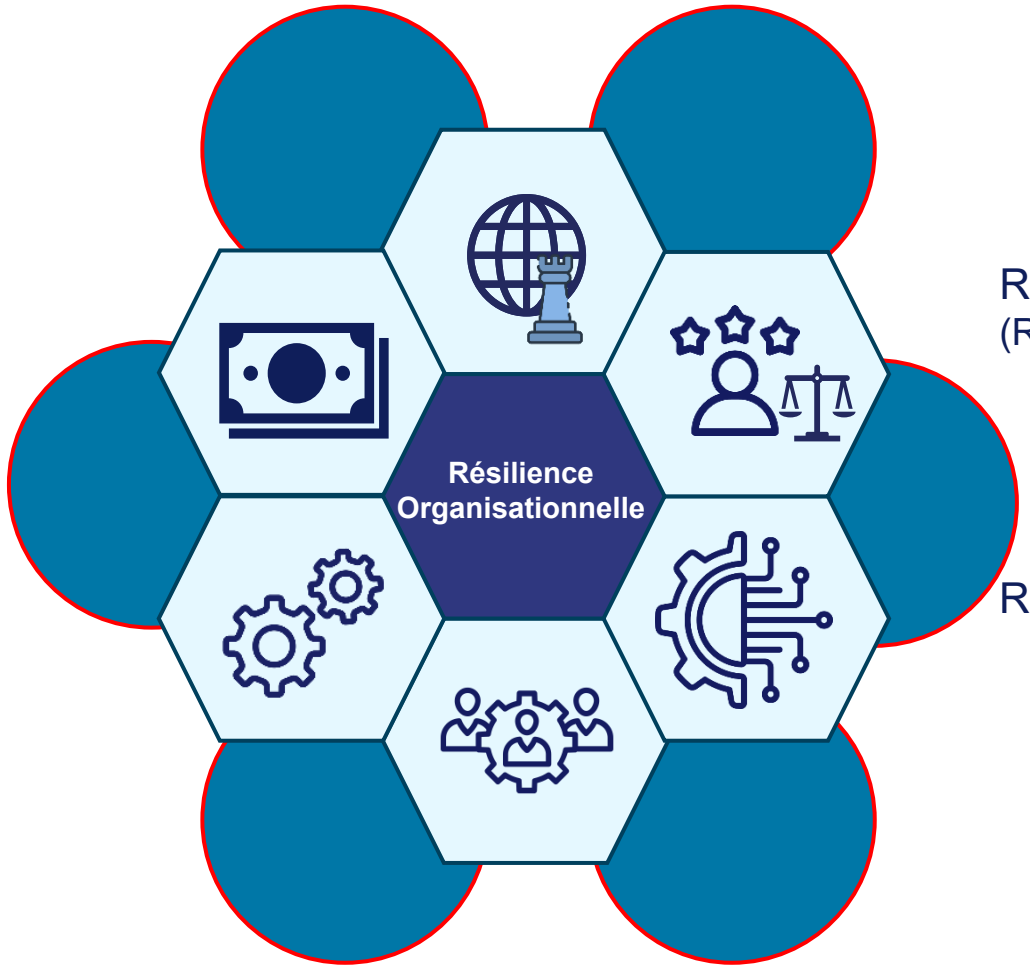
Impact Opérationnel
Touchant directement une production, peut se traduire en impact financier

Résilience Organisationnelle

Résilience Stratégique

Résilience Financière

Résilience de l'Image de Marque
(Réputation)



Résilience Opérationnelle

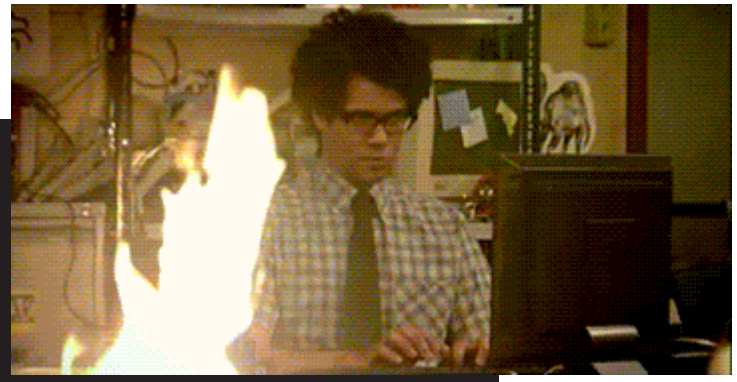
Résilience Technologique

Résilience du personnel et des dirigeants

Dualité Business / IT

Perception IT dans votre société

Selon vous, quel est le rôle de votre service informatique dans votre entreprise ?



« **What if** Question » – Questionner tout.
Moment de remise en question.

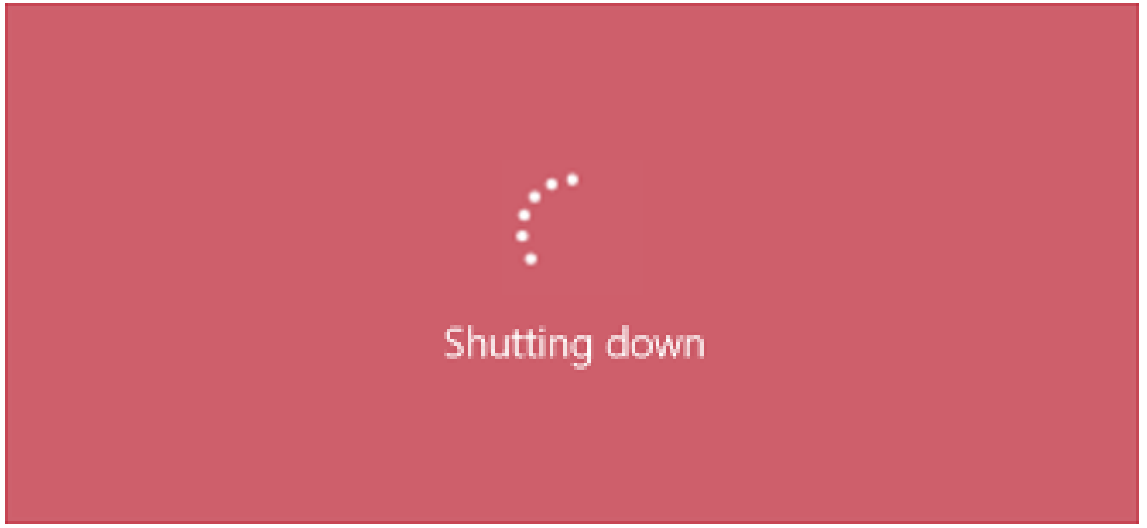
Construction des plans en coordination:
IT + Métiers + Direction

What If ?

kill switch

Imaginez les conséquences pour votre entreprise !

- Pas d’emails ni teams
- Pas d'accès aux documents électroniques
- Votre accès Cloud est coupé
- Votre carte de paiement ne fonctionne plus?



Quels sont vos outils les plus critiques?
Dixit « BIA »

Votre interlocuteur chez SPIE ICS

« La résilience est un marathon, pas un sprint. »

spie.ch/gouverner

Mohamed Chaabouni

Information Security & Data Privacy Consultant

Tél. +41 79 395 92 68

Mail mohamed.chaabouni@spie.com