De la Cyber-Sécurité à la Cyber-Résilience

☎ +32 (0) 2 347 59 71
✉ info@synergit.be

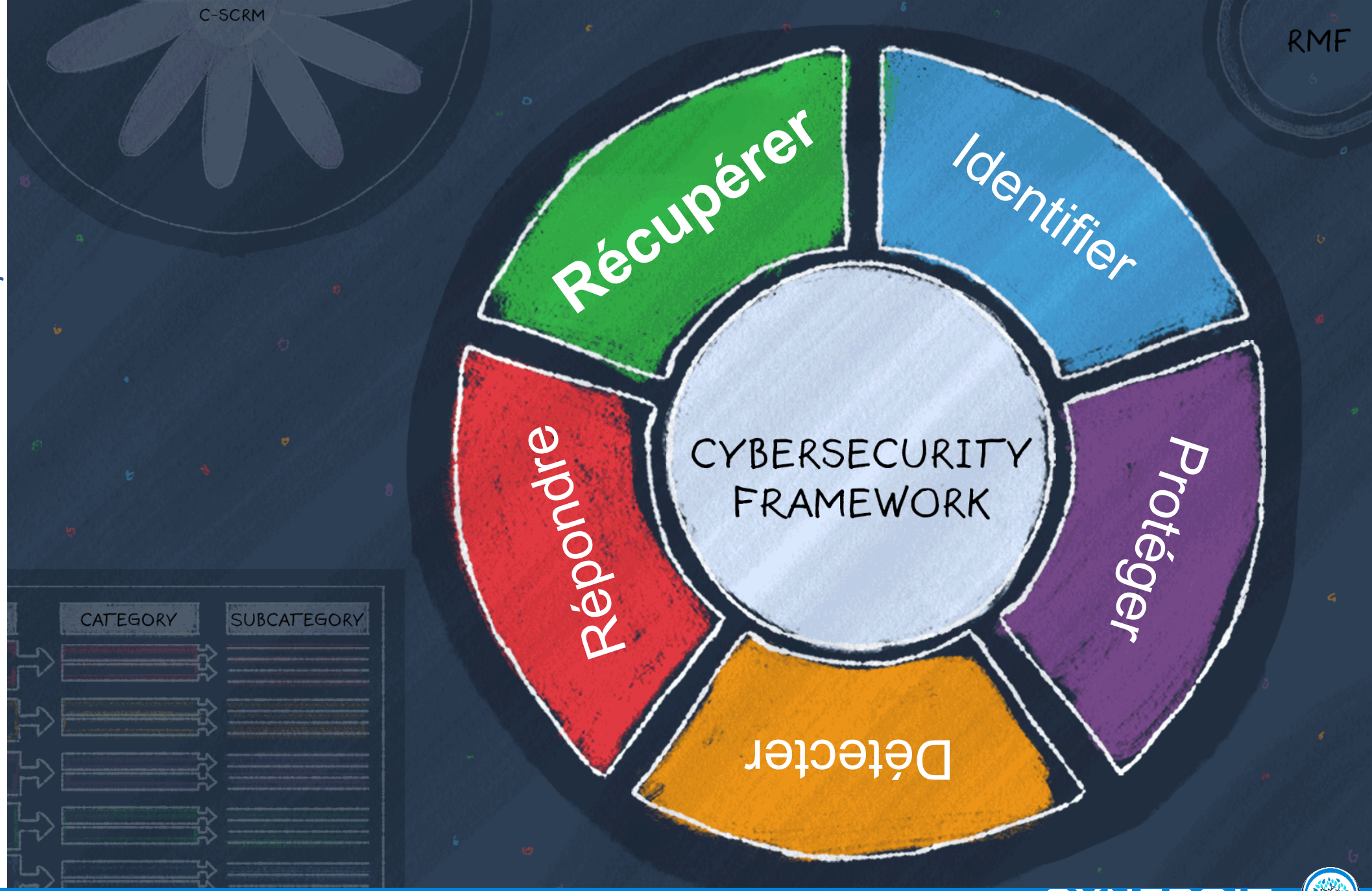
Christian De Boeck - 04/10/2022

http://www.SYNERGIT.be


Business Continuity / Résilience
IT-Service Continuity Management
Assessments,
Audits &
Tests
Coaching, Mentoring , Training &
Gestion du Changement
Transition Bas-Carbone

Quelques références

NIST Cyber Security Framework v2.0 à venir



NIST - Recover

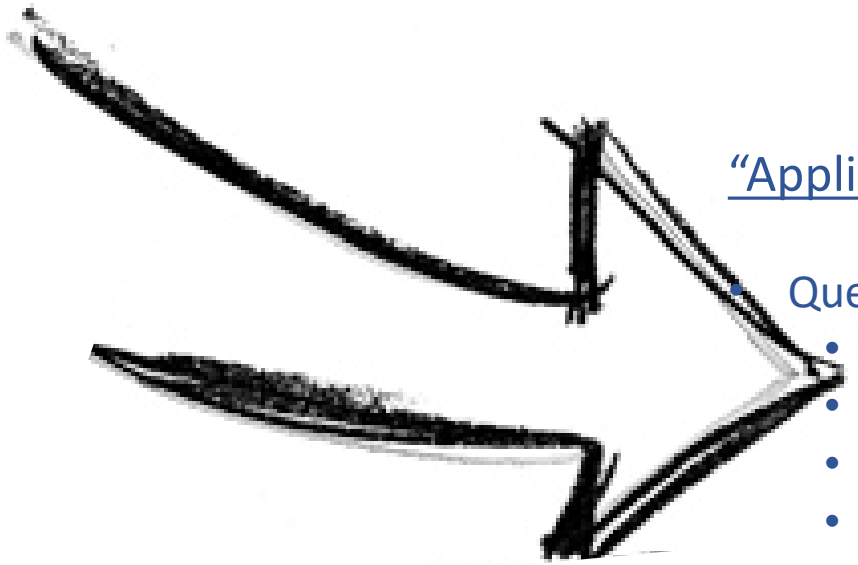
- *Recovery Planning* (RC.RP):
  - *Recovery processes and procedures* are executed and *maintained* to ensure *restoration* of systems or assets affected by cybersecurity incidents.
- Improvements (RC.IM):
  - Recovery planning and processes are *improved* by incorporating lessons learned into future activities.
- Communications (RC.CO):
  - Restoration activities are *coordinated with internal and external parties* (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).

Méthodes de mise en oeuvre de la continuité

Métiers

Business Impact Analysis (BIA):

- Que protéger?
  - Activités
  - Fonctions
  - Processus
    - Moyens Humains
    - ***Moyens IT***
    - Moyens non-IT, …



Informatique

"Applications Impact Analysis" (AIA):

Que protéger?

- Infrastructures
- Connectivité
- Applications
- Partenaires / Fourniseurs (SaaS,…)
- (ITIL Business Services)

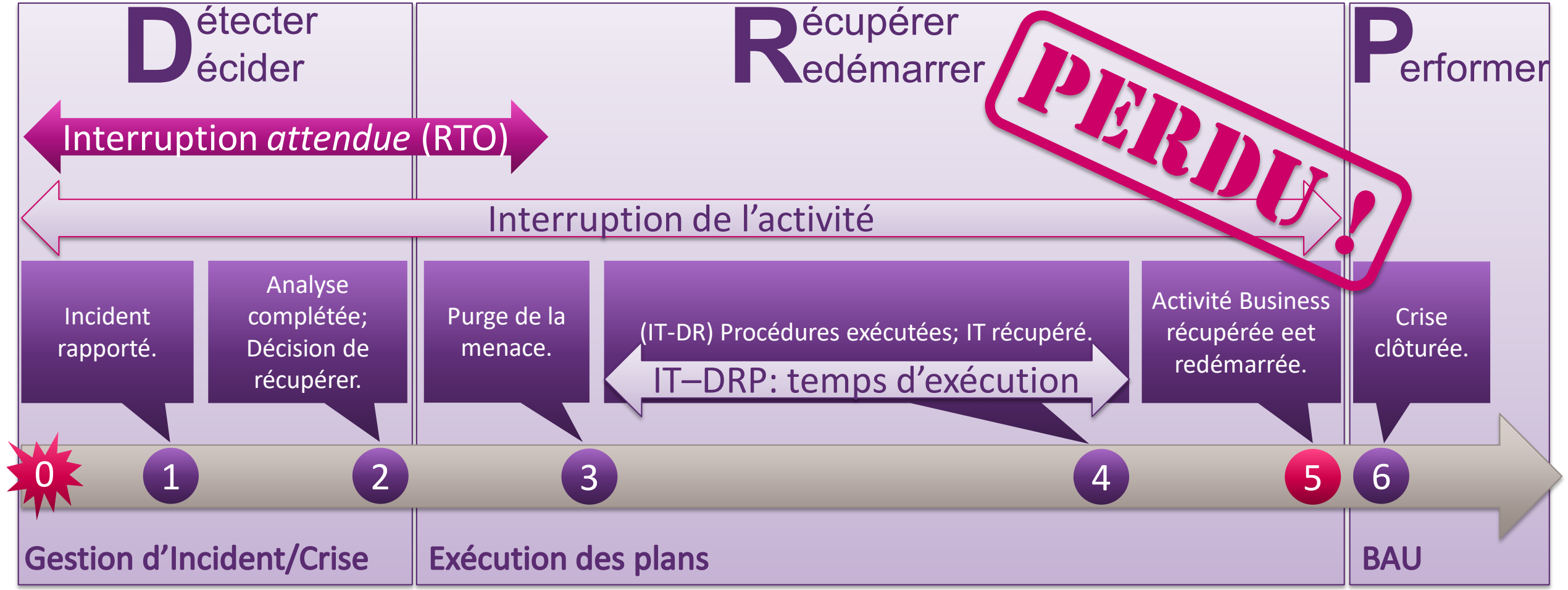
→ ***Ecosystème complet***

Risk Assessment (RA):

- Quelles catastrophes?
  - Pandémie
  - Défaut d'un fournisseur
  - Perte d'un site de production / IT
  - Guerre, …
  - ***Cyber-attaque***
  - Vol de données (GDPR)
  - Crise financière,…

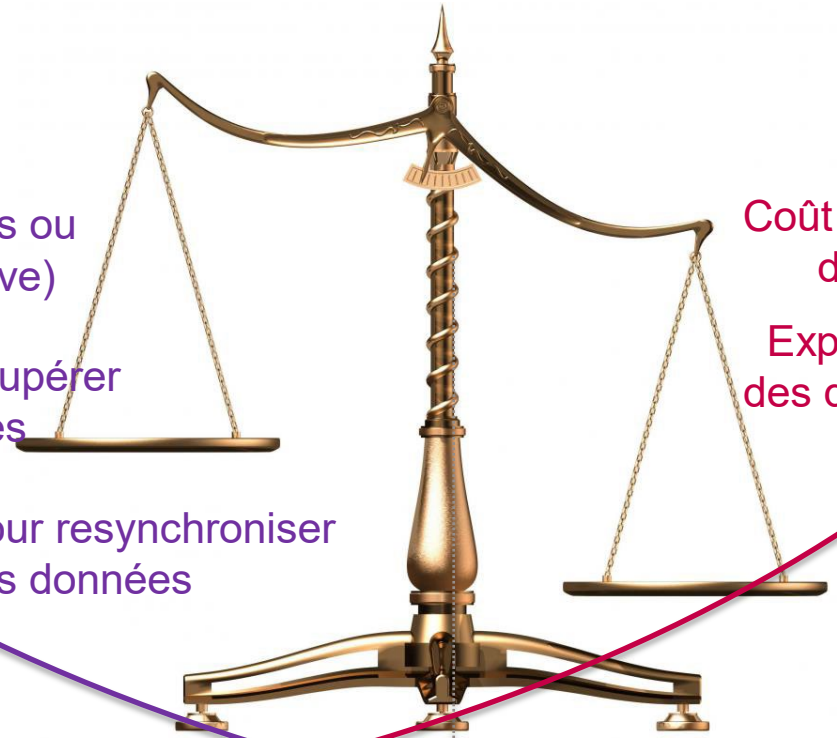
- IT pour IT (couvert par le BIA de l'IT, p. ex. Backup/restore, monitoring,…)

Chronologie d'une crise "Cyber": Récupérer



www.SYNERGIT.be

Chronologie d'une crise "Cyber": Récupérer les données



Coûts (data / temps / argent)

RPO (Perte de données ou Recovery Point Objective)

Temps pour récupérer les données

Temps pour resynchroniser les données

Coût de la protection des données

Exposition des données

Détecter
Décider

Incident rapporté.

Analyse complétée; Décision de récupérer.

0

1

2

+ Perte de données jusqu'à un point de récuperation "transverse"

Backup & restore

Réplication basée sur Journal / Log shipping

Réplication Asynchrone

Réplication Synchrone

Gestion d'Incident/Crise

Ou mettre les copies des données?

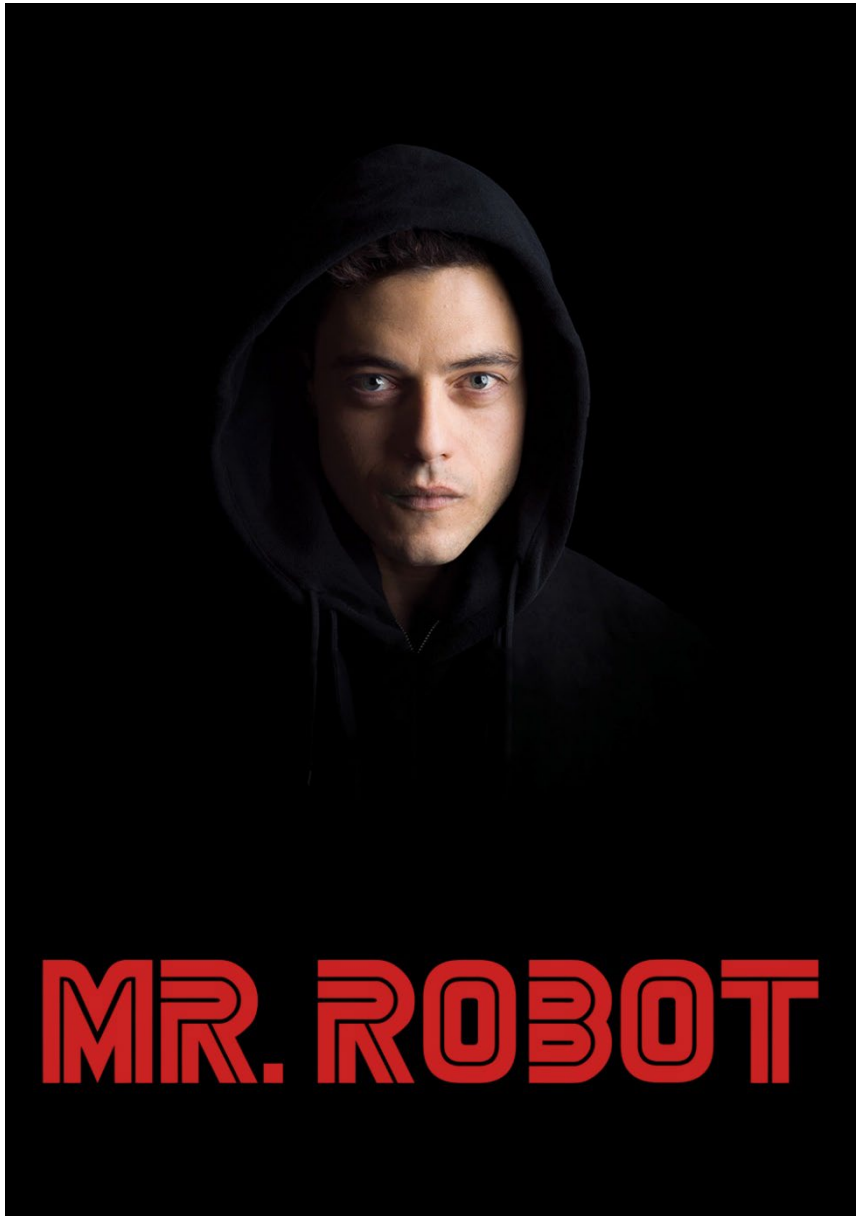
Sur site / site distant:

- Données:
  - Sur des disques (replication)
  - Sur des disques “isolés” (rejouer les transactions, pare feu)
- Sauvegardes:
  - Sur des disques
  - Sur des disques en lecture seule / media à écriture unique

Dans le “Cloud”:

- Données:
  - Rejouer les transactions
  - Stockage dans le cloud
- Sauvegardes:
- “Backup as a Service”

Attention: les pirates visent à compromettre ***toutes*** les copies de vos données!

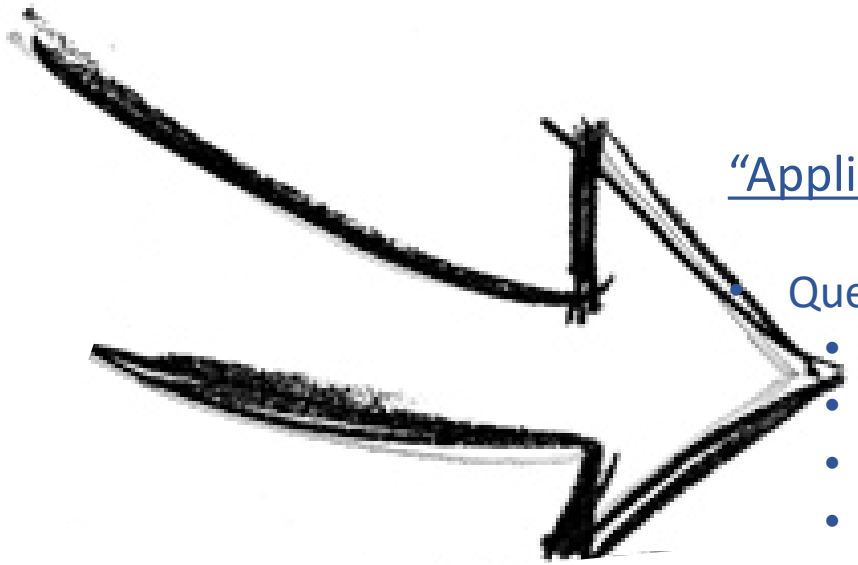


Méthodes de mise en oeuvre de la continuité

Métiers

Business Impact Analysis (BIA):

- Que protéger?
  - Activités
  - Fonctions
  - Processus
    - Moyens Humains
    - ***Moyens IT***
    - Moyens non-IT, …



Informatique

"Applications Impact Analysis" (AIA):

Que protéger?

- Infrastructures
- Connectivité
- Applications
- Partenaires / Fourniseurs (SaaS,…)
- (ITIL Business Services)

→ ***Ecosystème complet***

- IT pour IT (couvert par le BIA de l'IT, p. ex. Backup/restore, monitoring,…)

Risk Assessment (RA):

- Quelles catastrophes?
  - Pandémie
  - Défaut d'un fournisseur
  - Perte d'un site de production / IT
  - Guerre, …
  - ***Cyber-attaque***
  - Vol de données (GDPR)
  - Crise financière,…

Méthodes de mise en oeuvre de la continuité

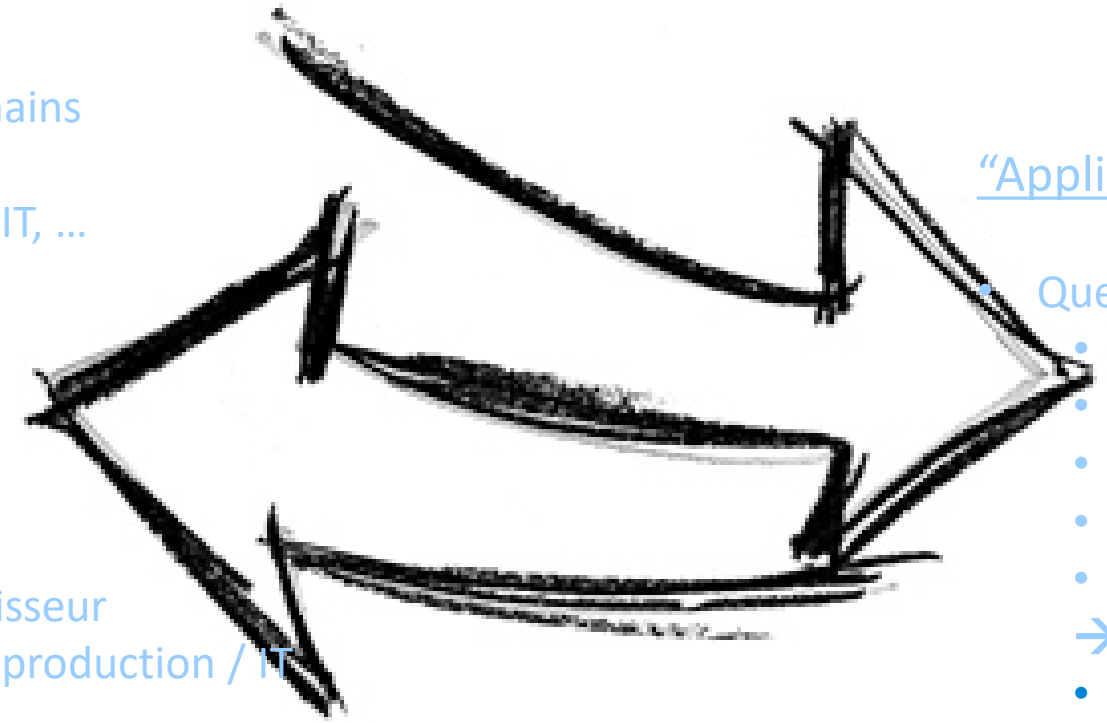
Métiers

Business Impact Analysis (BIA):

- Que protéger?
  - Activités
  - Fonctions
  - Processus
    - Moyens Humains
    - ***Moyens IT***
    - Moyens non-IT, …
    - ***Alternatives***

Risk Assessment (RA):

- Quelles catastrophes?
  - Pandémie
  - Défaut d'un fournisseur
  - Perte d'un site de production / IT
  - Guerre, …
  - ***Cyber-attaque***
  - Vol de données (GDPR)
  - Crise financière,…



Informatique

"Applications Impact Analysis" (AIA):

Que protéger?

- Infrastructures
- Connectivité
- Applications
- Partenaires / Fourniseurs (SaaS,…)
- (ITIL Business Services)

→ ***Ecosystème complet***

- ***Alternatives & optimisation***

- IT pour IT (couvert par le BIA de l'IT, p. ex. Backup/restore, monitoring,…)

Chronology of an (IT) crisis and its resolution

www.SYNERGIT.be

Take away:

- BCM & DRP peuvent aider la cyber-sécurité:

  Les méthodes et objectifs sont similaires;
- Le plus souvent, l'IT seule est impuissante;
- Les métiers doivent développer des

  alternatives pour redémarrer plus rapidement

  suite à une cyber-attaque;
- Il faut tester tous ces nouveaux plans en

  situation la plus réelle possible.

Merci

☏ +32 (0) 2 347 59 71
✉ info@synergit.be

http://www.SYNERGIT.be