Risques de cyber sécurité et résilience dans le secteur financier: Retour d'expériences tunisiennes 'Cas de la BCT'

Jalel Zagrani

Septembre 2019

Jalel.Zagrani@bct.gov.tn

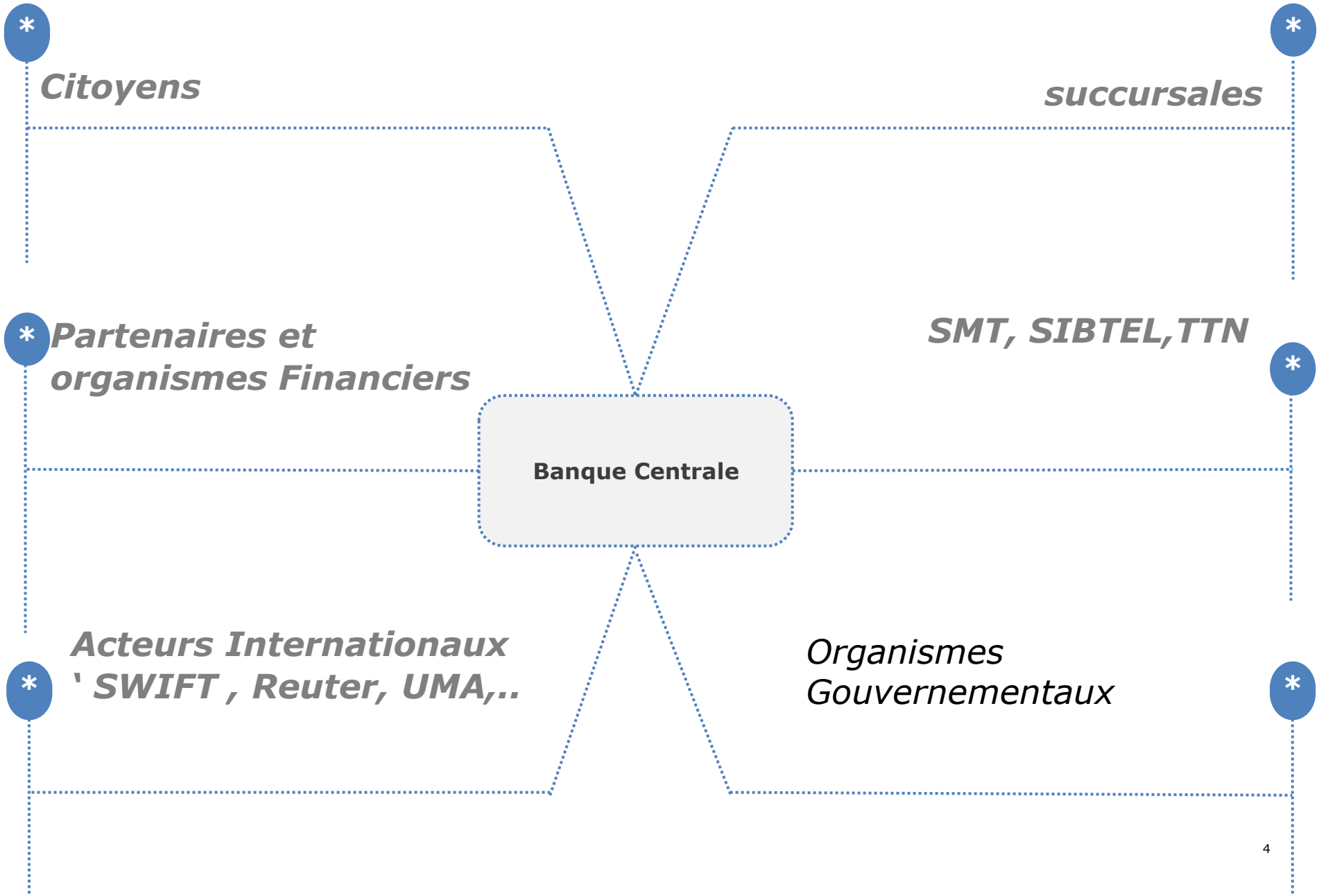
Agenda

1) Introduction
2) ‘ Vue globale ’ de l’écosystème et SI de la BCT
3) Organisation de la sécurité à la BCT
4) Plan de continuité
5) **Exemple de g**estion d’un risque métier
6) Coordination & communication
7) Vision & orientation future
8) Conclusion

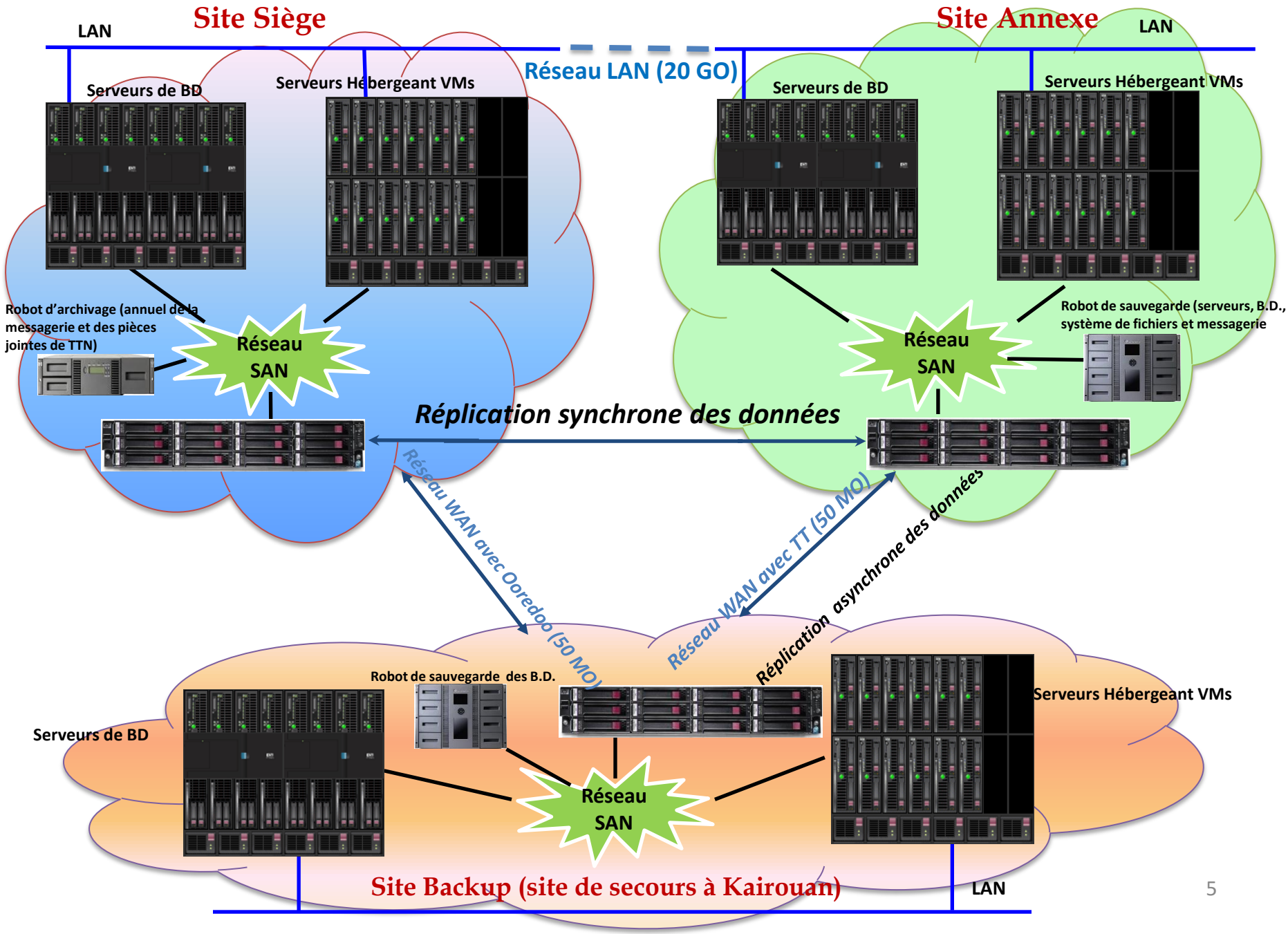
1- Introduction

- Le secteur financier est une cible potentielle et privilégiée de cyber-attaques,
- Présence d'un 'contexte socio-économique difficile'
- Quel est le rôle de la BCT 'le régulateur' face à ces risques ?
- Quels moyens et mesures déployés ?

2-Vue globale de l'écosystème

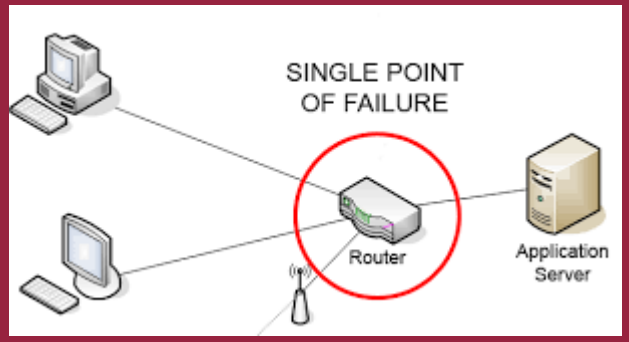


Vue globale du SI actuel



Caractéristiques du SI

- Disponibilité
- Résilience
- Intégrité
- Absence de SPoF



Quels enjeux et défis pour le SI ?

- **Ouverture nécessaire : augmentation des menaces et exposition à de nouveaux risques ,**
- **Croissance ,complexité et diversification des équipements: nécessité de compétences spécifiques difficile à trouver et retenir ,**
- **Lancement de nouveaux acteurs : bureaux de change , établissement de paiements ,FinTech**
- **Jouer un nouveau rôle comme provider de 'PaaS' pour des instances nationales :ACM, FGDB**

Les menaces

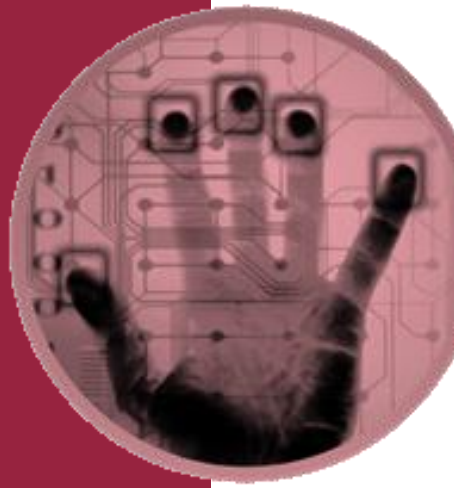

défaillance
information
humaines
respect
corruption
effets
manque
anticipés
mise
abus
Sabotage
écoute
droits
pannes
accidents
sociale
bord
vol
secrets
légales
personnel
terrorisme
DDOS
erreurs
non
systémes
ingénierie
identité
catastrophes
naturelles
ressource
pandémie
divulgation
intrusion
Modifications
exigences

3- Organisation de la sécurité

❖

❖Structure chargée de la gestion de la sécurité opérationnelle ‘ DSI’ rattachée à l’IT:

- ❑ Contrôle d’accès ,
- ❑ Sécurité des données et gestion opérationnelle ,
- ❑ Sensibilisation et formation des utilisateurs,
- ❑ PCA



❖Structure chargée de management des risques rattachée à l’Organisation,

❖Structure chargée management de la conformité rattachée au département juridique,

❖ Structure de l’audit et contrôle interne rattachée au gouvernement de la Banque


Réaction
Stratégie de la DSI
Détection
Prévention

4- Le Plan de Continuité

1. **Preparation & analyse**
   - Gestion de projet
   - Revue de la situation existante
   - Analyse des risques & business impact

2. **Construire du plan**
   - Prendre des mesures préventives / correctives
   - Fonction des stratégies de recouvrement pour les fonctions / systèmes / processus
   - Communication

3. **Implementation**
   - Test & maintenance

Préalable et préparatifs techniques

- Mise en place d’une cellule de crise ,
- Choix d’un site de repli,
- Aménagement d’un site de secours,
- Communication,
- …

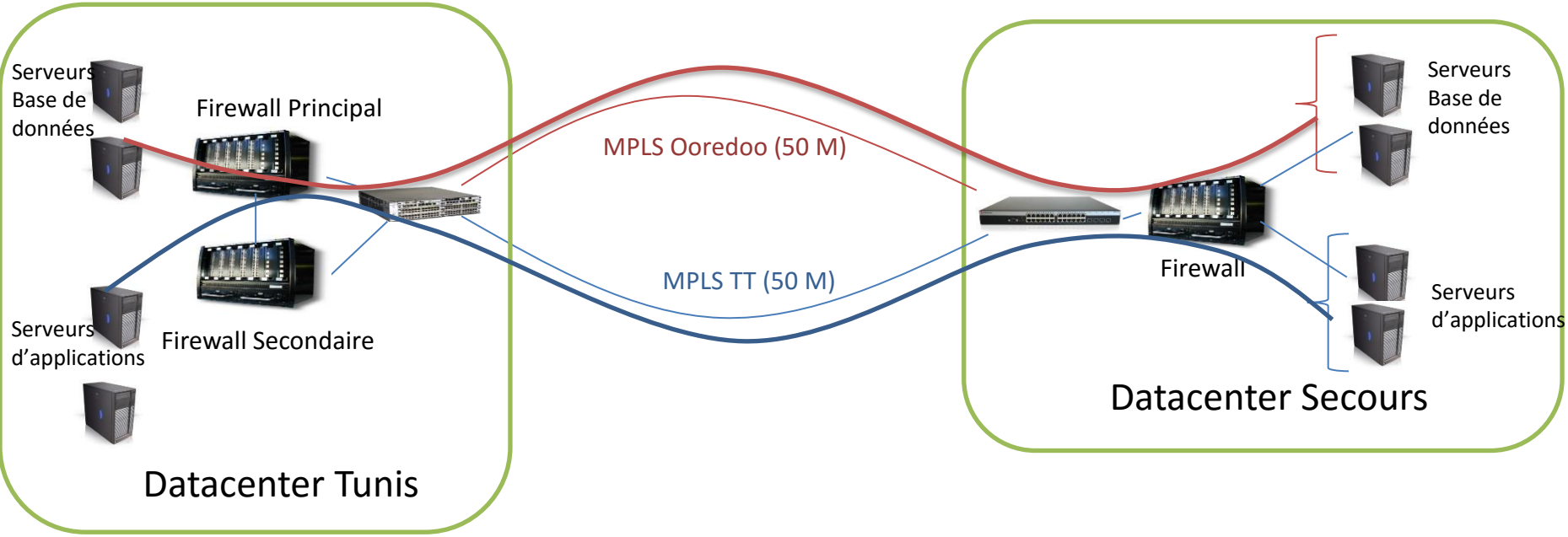
Présentation de l'environnement de test

- Un site de repli temporaire :
  - Salle aménagée à l'étage au niveau de la succursale de Kairouan ,
  - Mise en place d'un réseau spécifique pour le test
  - Une dizaine de postes de travail configurés pour les besoins du test.

Périmètre du premier test PCA

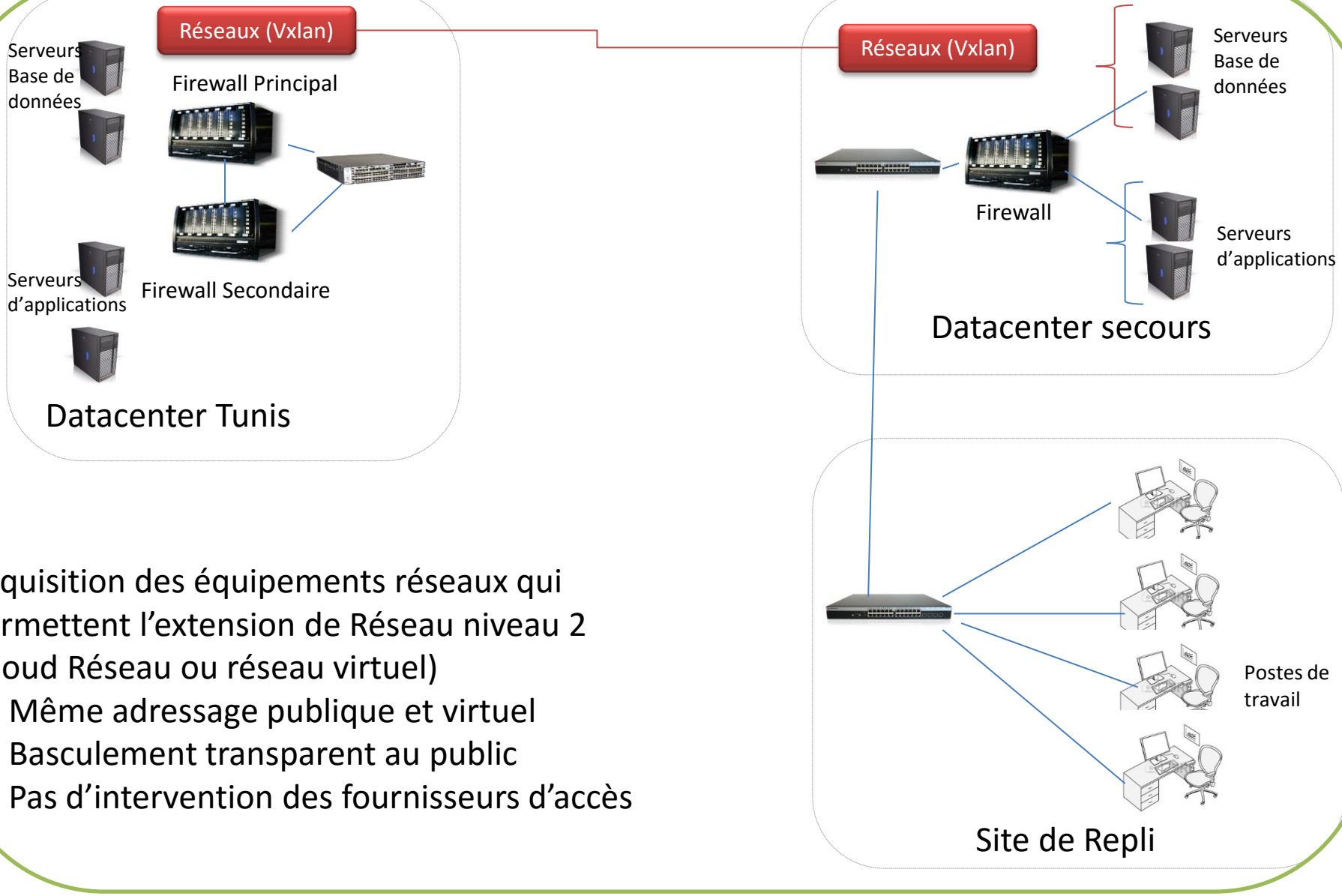
- Comme il s'agit d'un premier test en grandeur nature et en présence des utilisateurs concernés :
  - Mise en place d'un site de repli temporaire (en attendant de se fixer un choix définitif),
  - Réduire le périmètre du test en se limitant (*site de secours nécessite une mise à niveau réseau & sécurité*) :
    - **aux services internes**
    - **sans faire appel à des partenaires externes**
- **Ces mesures et limites restrictives sont relatives au premier test uniquement**,

ARCHITECURE ACTUELLE



Basculement Manuel

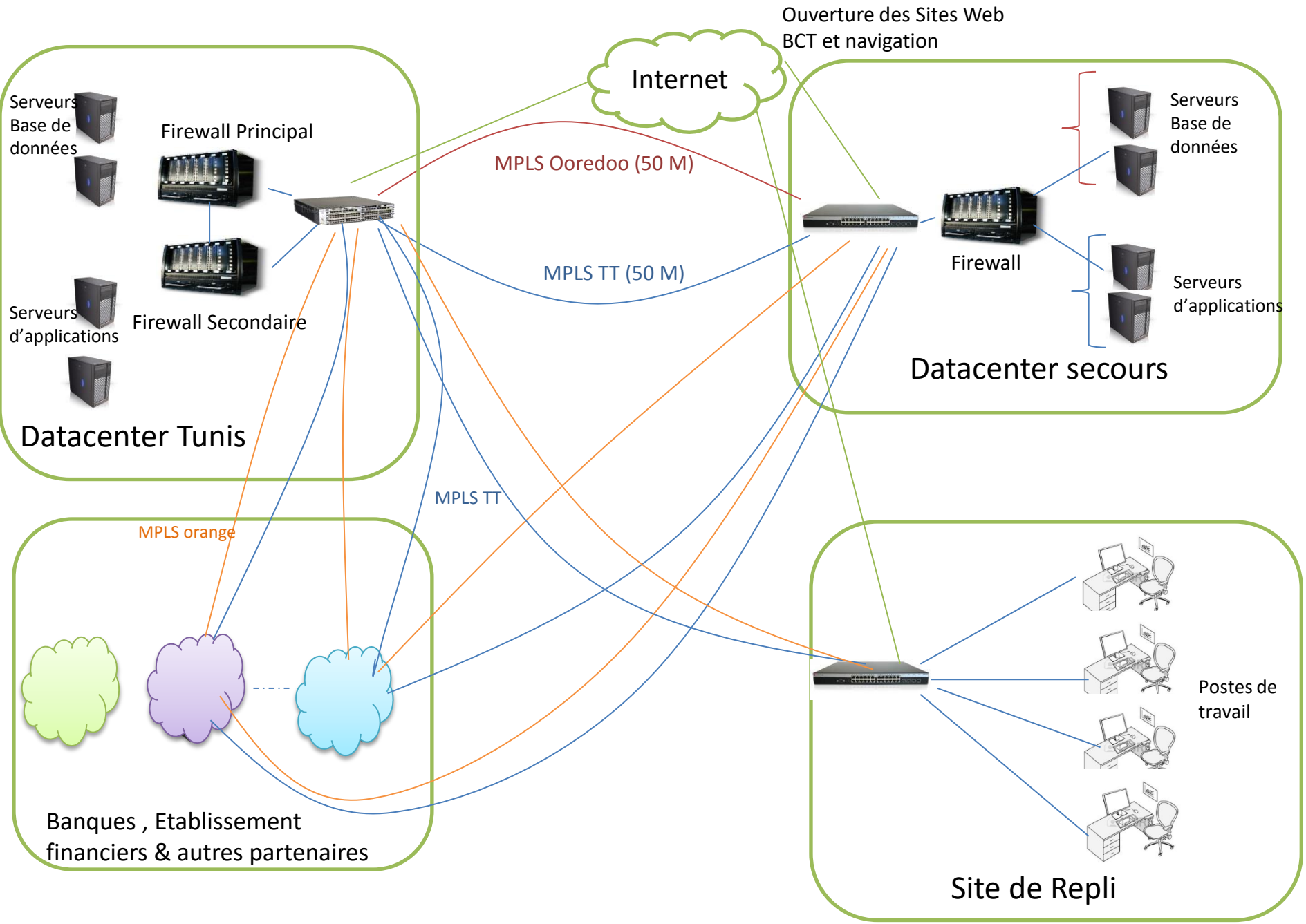
Mise à niveau du site secours



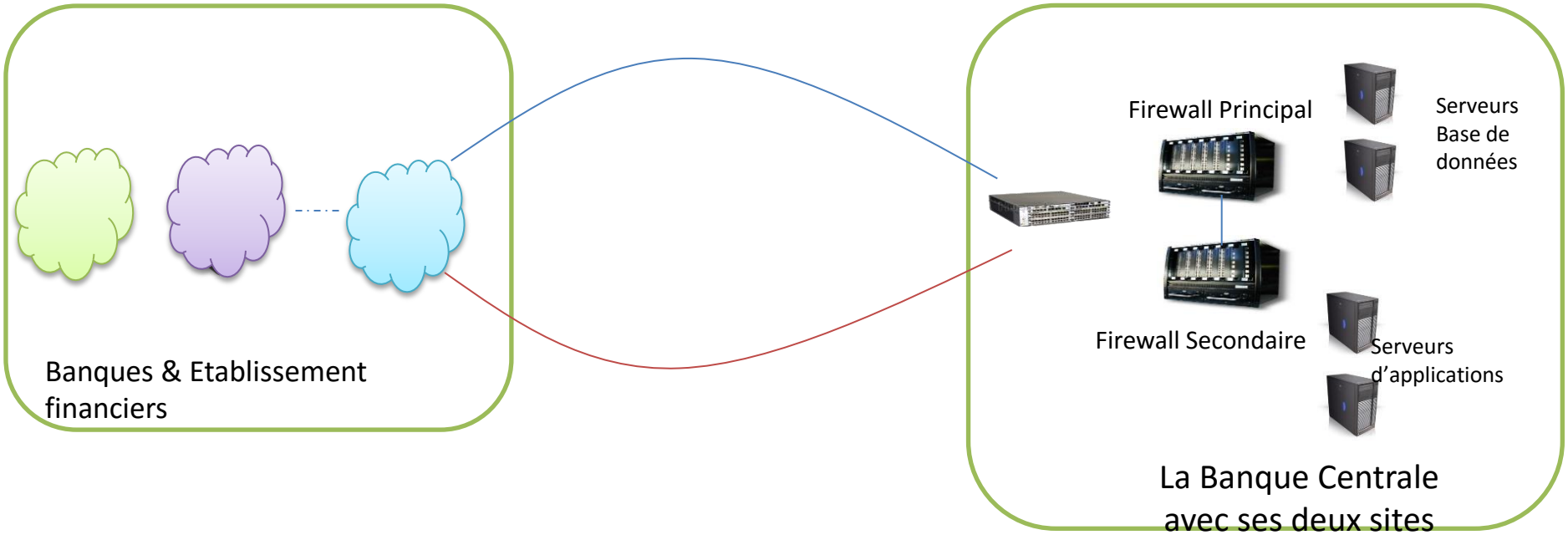
Acquisition des équipements réseaux qui permettent l'extension de Réseau niveau 2 (Cloud Réseau ou réseau virtuel)

- Même adressage publique et virtuel
- Basculement transparent au public
- Pas d'intervention des fournisseurs d'accès

Architecture cible



Les deux sites convergent vers un cluster de type ACTIF-ACTIF pour tous les services (internes et externes)



Le basculement vers le site de secours est complètement transport aux banques et partenaires externes

5- Exemple de gestion de risque metier

❖**Avril 2013 : Publication par le Comité de Bâle sur le contrôle bancaire 'Basel Committee on Banking Supervision' (BCBS) relative à la gestion du risque de liquidité quotidien 'intraday',**

❖ **Les Banques centrales et les organismes régulateurs cherchent des outils et moyens efficaces pour maitriser ce risque :**

- **Solution qui satisfait le spectre intégral d'un logiciel BI qui couvre (collecte, transformation , stockage et visualisation des data) ,**
- **Permet l'amélioration du contrôle du flux des devises en temps réel**

5- Coordination

❖Organisation de journées de sensibilisation pour les utilisateurs avec l'assistance de l'ANSI

❖Publication des vidéos de sensibilisation sur l'intranet de la BCT

❖ Participation à des actions de sensibilisation du secteur financier sur les risques et enjeux de la cyber sécurité avec l'APBEFT

❖Recours à des missions d'assistance techniques avec des organismes internationaux tels le FMI, FMA, BM,BAD

❖Collaboration , échanges d'expériences et de conventions avec des banques centrale étrangères

6- Visions…

- **Mise en place d'une solution de gestion des vulnérabilités,**
- **Mise en place d'une solution de lutte contre la fuite des données et assurer leur protection,**
- **Généraliser l'usage des contrôles du programme 'CSP' de SWIFT à toutes les composantes du système d'information,**
- **Développer un Framework spécifiques pour le secteurs financier comprenant les exigences nécessaires de lutte contre la cybercriminalité et le blanchiment d'argent (travail complémentaires à celui de la CTAF) ,**
- **Superviser la conformité des Banques aux contrôles de CSP,**

7- Conclusion…

Voici nos objectifs …

- **Renforcer l'image de la BCT en tant que garant de la stabilité du système bancaire**
- **Sécuriser les autorités sur la capacité de la BCT à gérer incidents/désastres graves**
- **Etre une locomotive pour le secteur financier pour la mise en place de programmes de Sécurité et de Continuité d'Activités**
- **Gagner la confiance des investisseurs et places financières internationales en disposant d'un PCA et d'une PSSI implémentés**

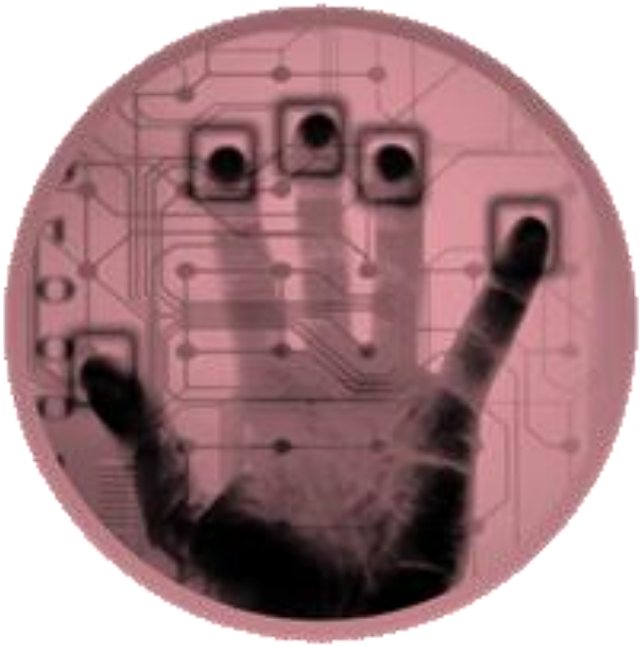
Q&A ?

Vue générale du CSP

❖ le programme de sécurité client (CSP) de SWIFT a été créé pour aider les institutions financière ‘clients’ dans la lutte contre les cyber-attaques,

❖ Il introduit un ensemble commun de normes de sécurité (combinaison de 3 normes PCI –DSS , ISO 27002 et NIST),

❖Il établit un ensemble de contrôles de sécurité pour tous les clients de SWIFT.

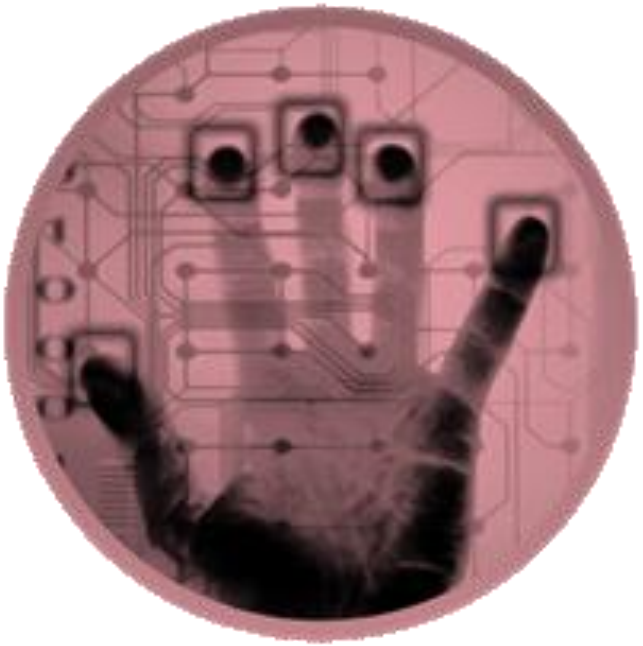


Vue générale du CSP

- il décrit comment ils seront évalués et mesurés à l'aide d'un ‘framework’ mis à la disposition des clients,

- Les contrôles de sécurité obligatoires établissent une base de référence de sécurité pour l'ensemble de la communauté,

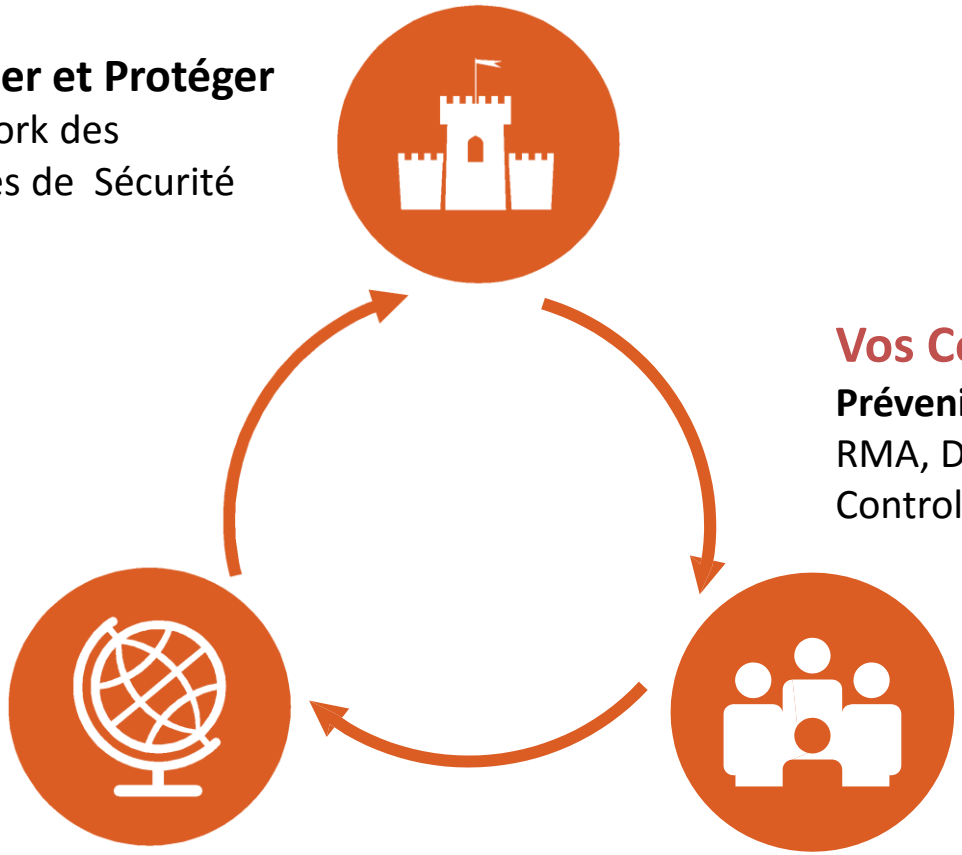
- Cet ensemble de contrôles de sécurité est destiné pour tous les clients de SWIFT.



Vue générale du CSP

Vous

Sécuriser et Protéger
framework des
contrôles de Sécurité



Vos Contreparties

Prévenir et Détecter
RMA, DVR, Payment
Controls

Votre Communauté

Préparer et partager
Partage de l'intelligence
Portal ISAC de SWIFT

Vue générale du CSP

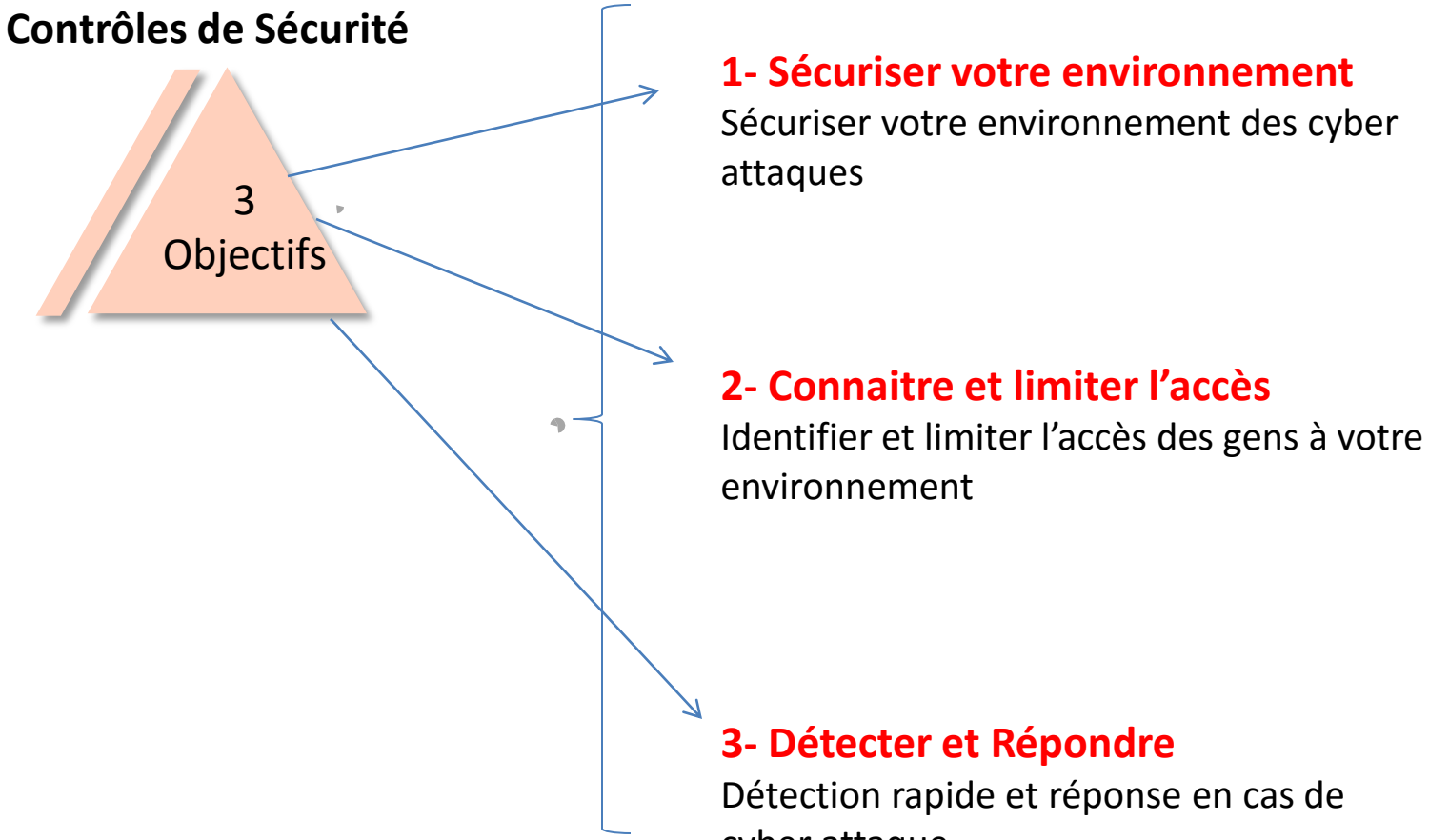
❖ SWIFT a introduit un ensemble de contrôles de sécurité que chaque client SWIFT doit mettre en œuvre.

❖ Ces contrôles de sécurité sont obligatoires pour tous afin de définir **une ligne de base de sécurité** pour l'ensemble de l'industrie financière.

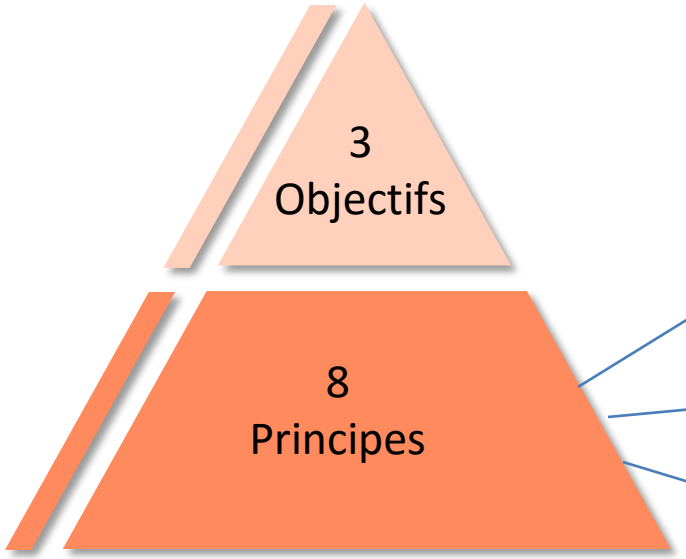
❖ Les clients doivent **implémenter** ces contrôles et **attester** leur niveau de conformité avant la fin de 2017.

SWIFT crée ainsi une ligne de base pour la sécurité
'SWIFT is creating a security baseline'

Vue générale du CSP



Vue générale du CSP



Sécuriser l'environnement

- 1- Limiter l'accès à Internet
- 2-Séparer les systèmes critiques de l'environnement informatique général
- 3-Réduire la surface d'attaque et les vulnérabilités
- 4-Sécuriser physiquement l'environnement

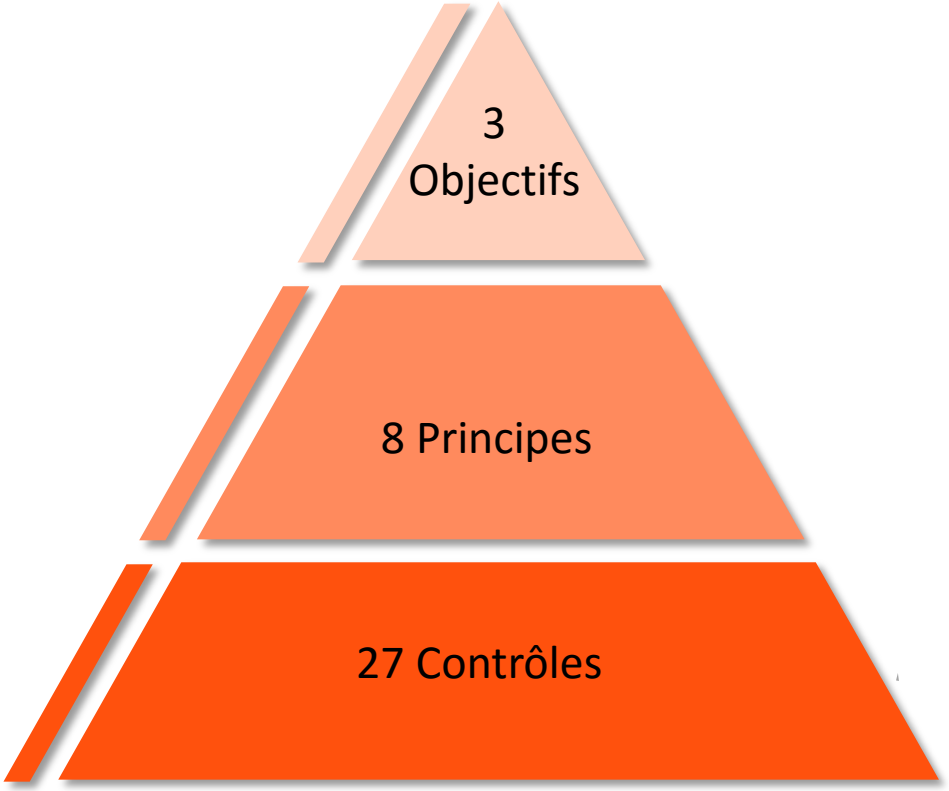
Connaitre et limiter les accès

- 5-Empêcher la compromission des informations d'authentification
- 6- Gérer les identités et 'ségrégâtes les privilèges

Détecter et répondre

- 7-Détecter une activité anormale du ysstème
- 8- Etablir un plan de réponse à un incident

Vue générale du CSP

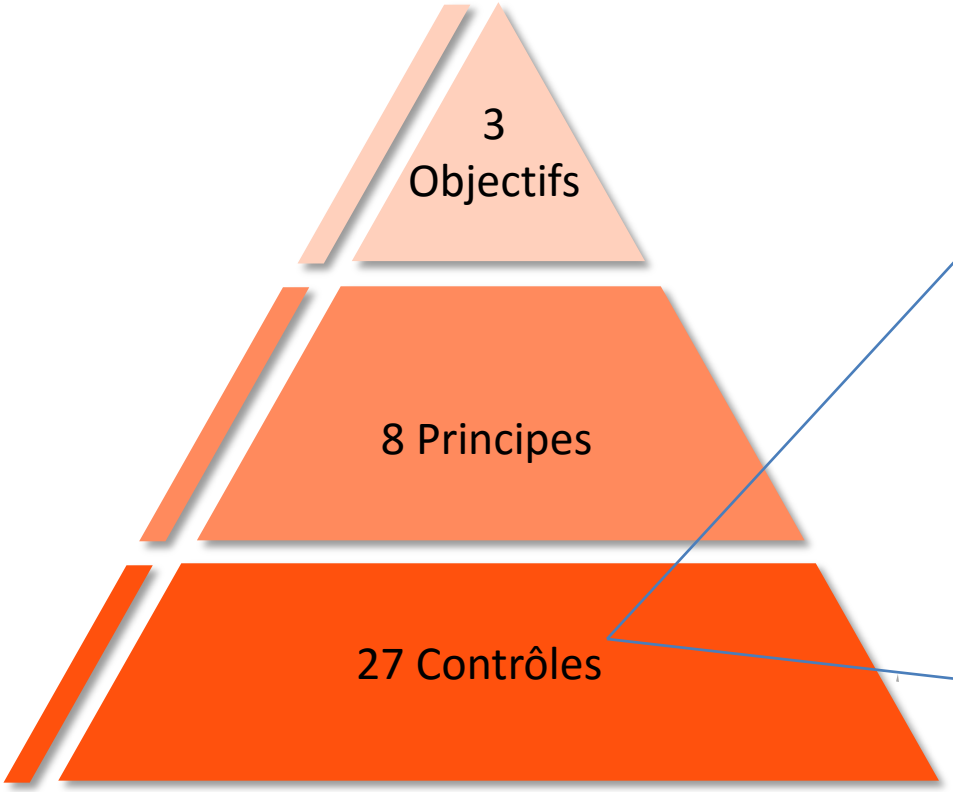


❑ **Mise en œuvre des 8 principes à l'aide de 27 contrôles (16 obligatoires, 11 optionnels) :**

- en ligne avec certaines normes existantes de la sécurité de l'information,

- devraient évoluer en fonction de l'évolution du paysage des menaces cybernétiques

Vue générale du CSP



❑**Les 16 contrôles obligatoires**

-établir une base de référence de sécurité pour toute la communauté

-tous les utilisateurs doivent **auto-attester** de la conformité de leur infrastructure SWIFT locale,

-fixer à court terme un objectif réaliste , tangible pour plus de de sécurité et moins de risques.

❑**Les 11 contrôles optionnels**

-Basées sur des bonnes pratiques que SWIFT recommande d'implanter