



INSTITUT
POLYTECHNIQUE
DE PARIS

STRATÉGIES DE RÉSILIENCE CYBER : REGARD CROISÉ SECTEUR PUBLIC/PRIVÉ

SÉMINAIRE C4 – 15 OCTOBRE 2026



Présentateur:
Hervé AMOUIN – MS Cyber 2024-2025

SOMMAIRE

- De la Cybersécurité à la Cyberrésilience
- Paysage commun de la menace
- Cadres réglementaires convergents
- Initiatives Secteur Public
- Initiatives Secteur Privé
- Tableau comparatif

DE LA CYBERSECURITÉ À LA CYBERRESILIENCE



Le centre hospitalier de Pontarlier dans le Haut-Doubs. • © Mary Sohier, France 3 Franche-Comté

CHI Pontarlier – Ransomware :

- 18/10/25: Attaque par « Cryptolocker »
- 03/26 : Origine inconnue
- 09/2026 : Système rétabli à 80%
- Retour complet estimé au printemps 27

DE LA CYBERSECURITÉ À LA CYBERRESILIENCE



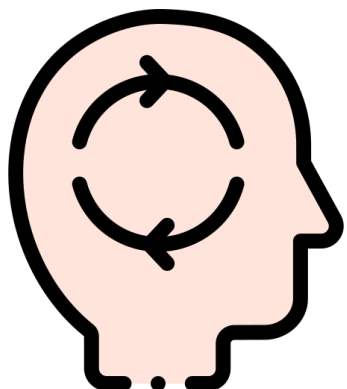
FinTech Française Harvest – Ransomware :

- 26/02/25: compromission de messageries utilisateurs et intrusion dans les systèmes et le site web (www.harvest.eu), coupure de plusieurs centres de données, et exfiltration de données.
- 10/04/25 : Revendication par Le groupe de cybercriminels **Run Some Wares**
- 4600 Sociétés clientes dont AXA, BNP Paribas, HSBC, ... aux activités perturbées

DE LA CYBERSECURITÉ À LA CYBERRESILIENCE

Changement de Paradigme :

Attaque = Incident certain À échéance incertaine.



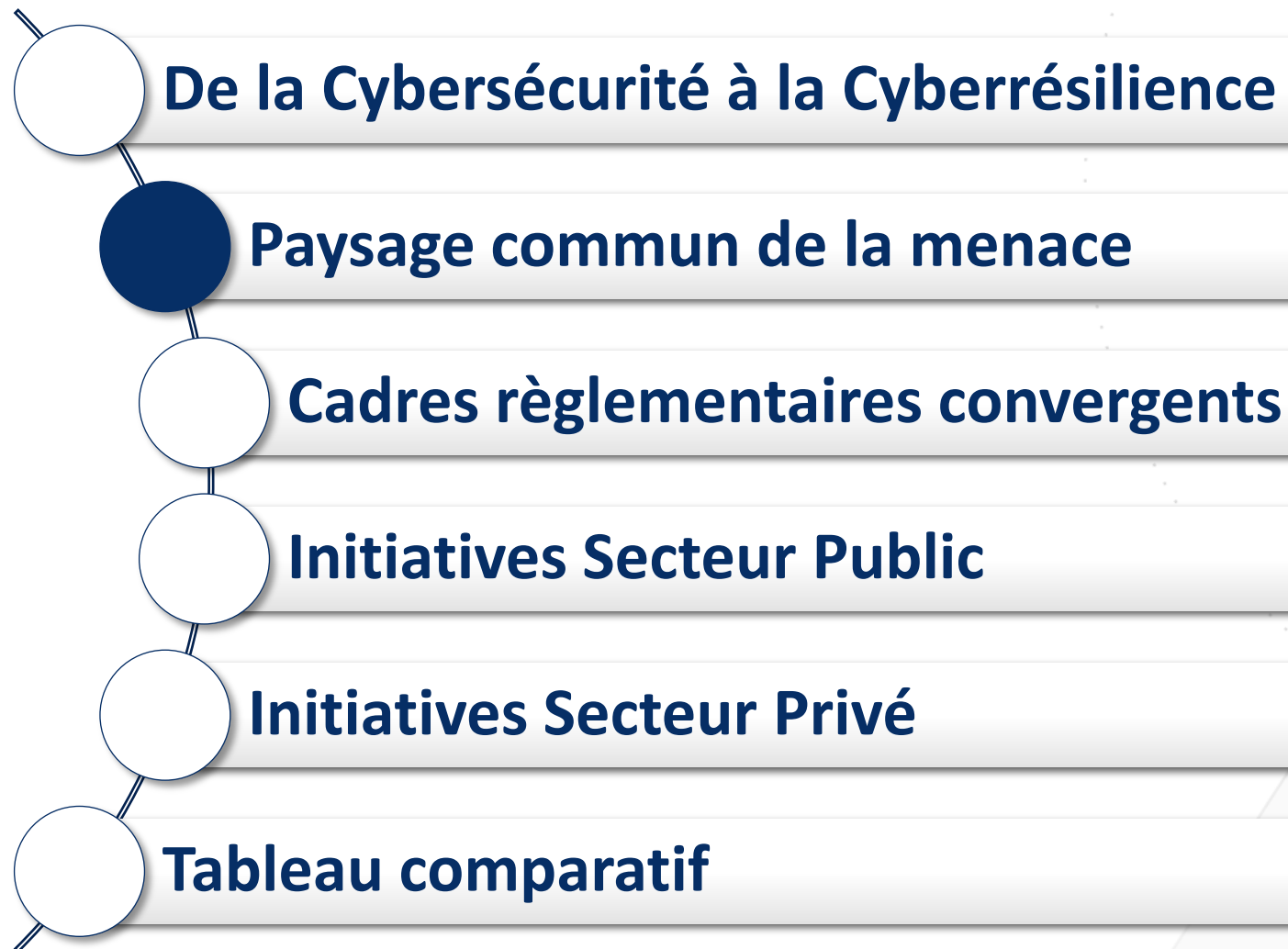
La Forteresse ne suffit plus:

Tiers critiques Risque systémique omniprésent.

Vers une Réassurance :

la reconstruction comme ligne de défense.

SOMMAIRE



LES MENACES COMMUNES

Ransomiciels :

Prolifération des **organisations criminelles**, finalités lucratives

Menaces sur la chaine d'approvisionnement :

Surface d'attaque étendue, **contrôles complexes**

Menaces Etatiques :

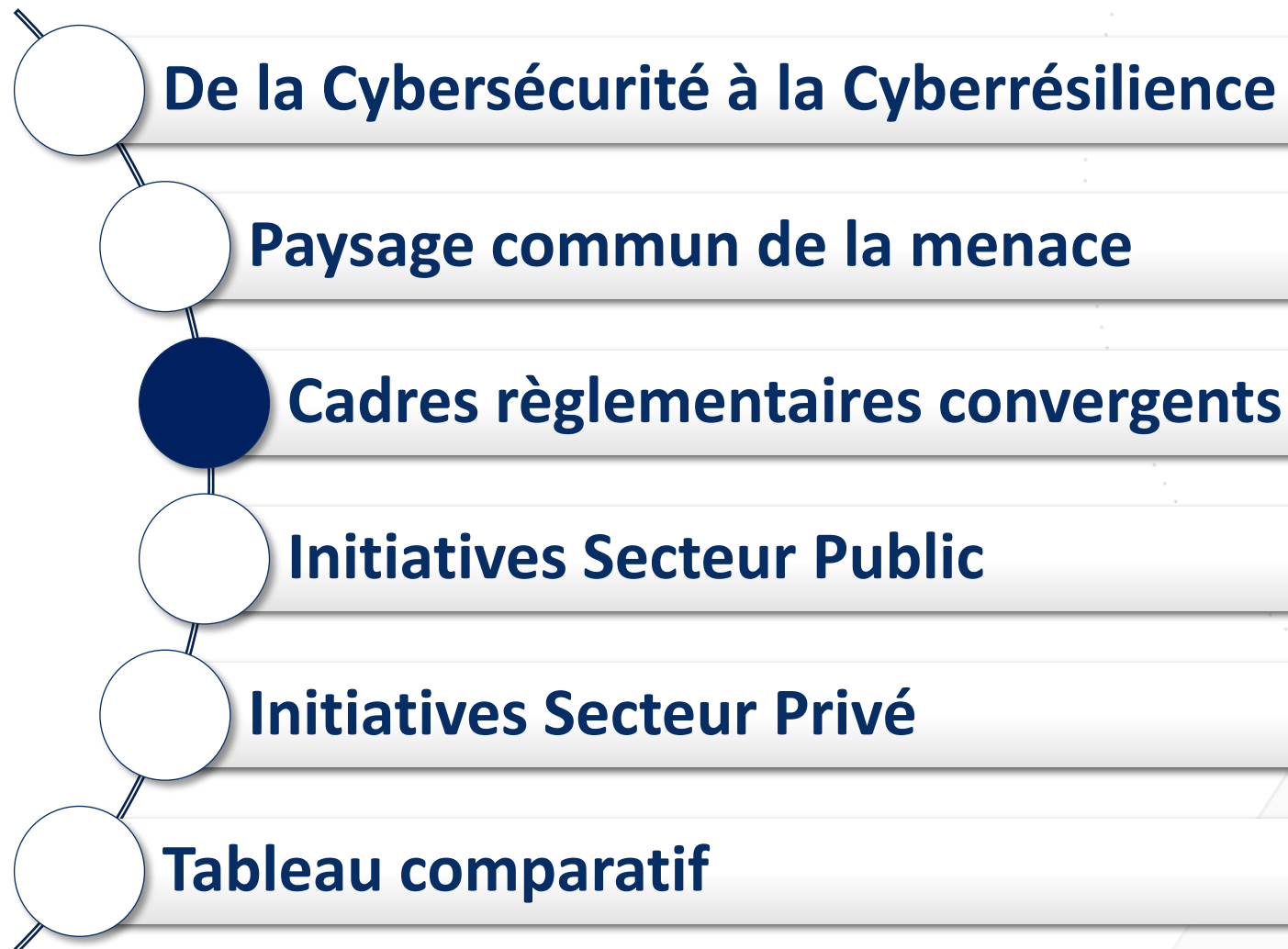
Instrument de **guerre** électronique et de **déstabilisation**

Menaces internes:

Productivité vs contraintes de **cybersécurité**



SOMMAIRE



CADRES RÉGLEMENTAIRES CONVERGENTS



Directive NIS2 :

- OSE, exigences fortes pour les acteurs du secteur privé et public
- Adopté en dec. 2022

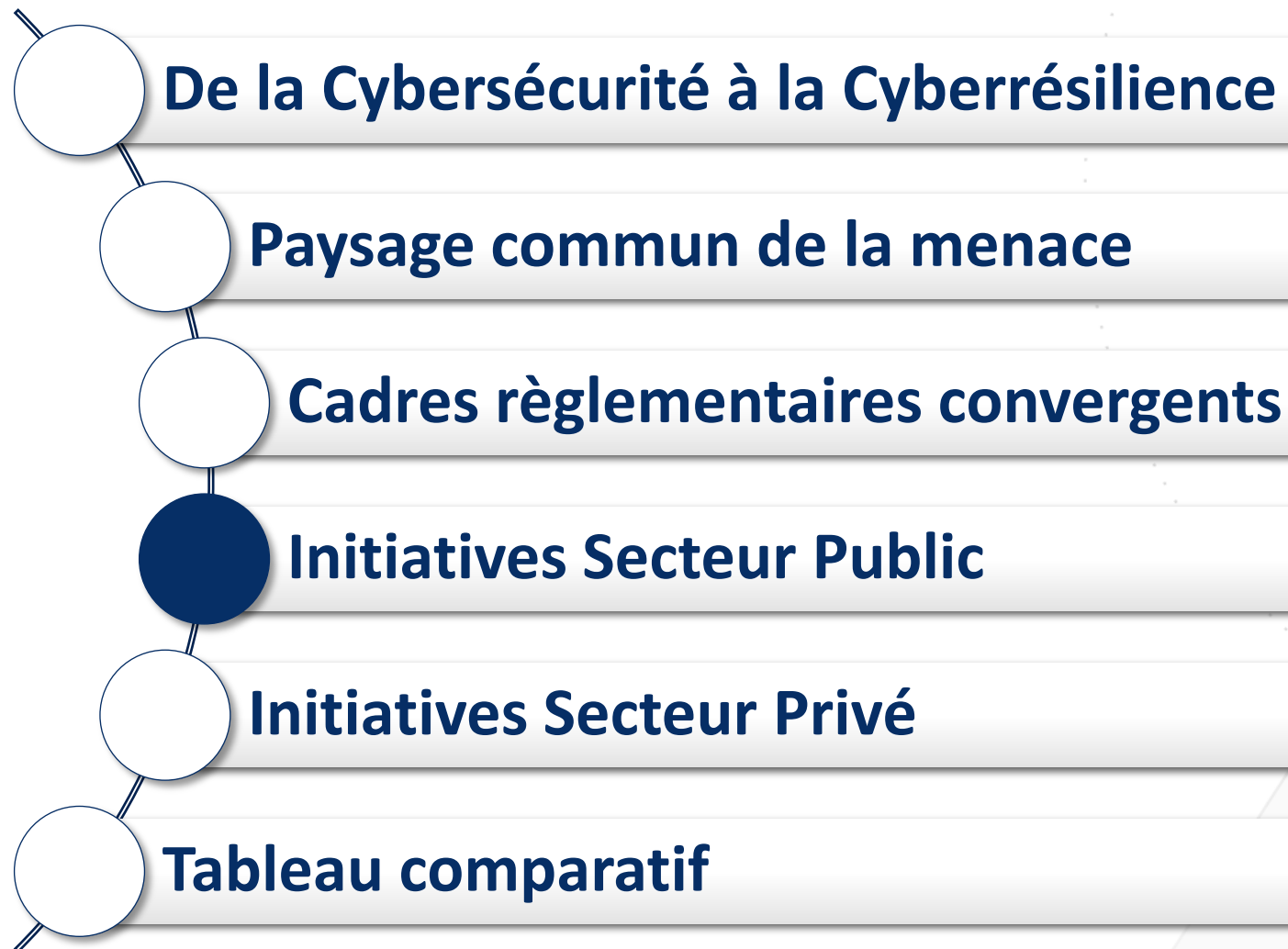
Règlement DORA:

- Ex speciali : exigences fortes pour les acteurs du secteur financier
- Entrée en vigueur le 16/01/2023 application au 17/01/2025

Règlement CRA (Cyber Resilience Act) :

- Entrée en vigueur le 10/12/2024 application au 11/12/2027
- Tout logiciel ou matériel comportant des éléments numériques
- Exigences fortes pour la gestion des vulnérabilités fournisseurs

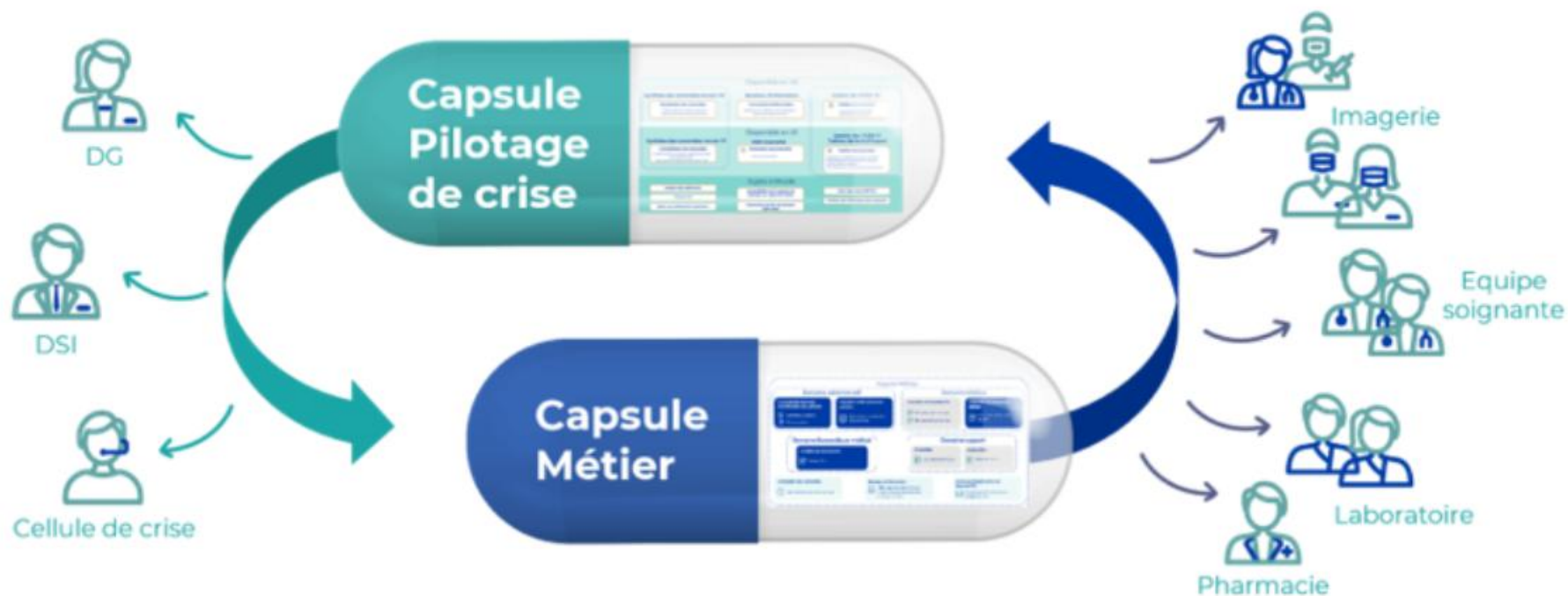
SOMMAIRE



INITIATIVE SECTEUR PUBLIC – SAAS CKISA

« CKISA, un projet innovant pour garantir la continuité des soins en cas de crise et renforcer la résilience des établissements hospitaliers. »

Source : <https://dsih.fr/articles/5779/ckisa-un-projet-innovant-pour-garantir-la-continuite-des-soins-en-cas-de-crise-et-renforcer-la-resilience-des-etablissements-hospitaliers>



INITIATIVE SECTEUR PUBLIC - CARE

Programme ANS de montée en maturité axé sur 15 compétences :

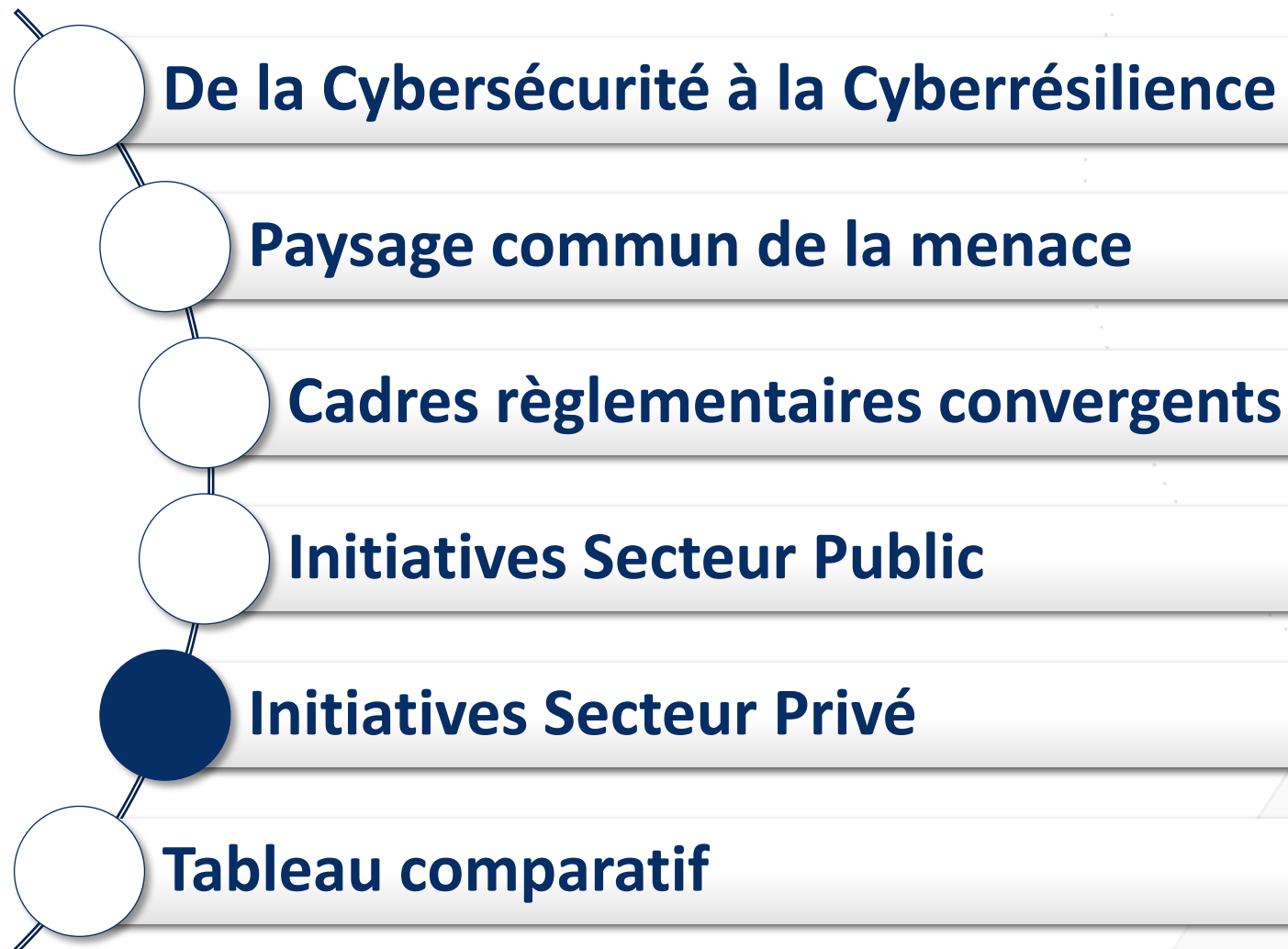
C09 – Reconstruction IT (coeur de confiance, infra critique, outils administrations, Network, etc)

ES MCO, ESMS

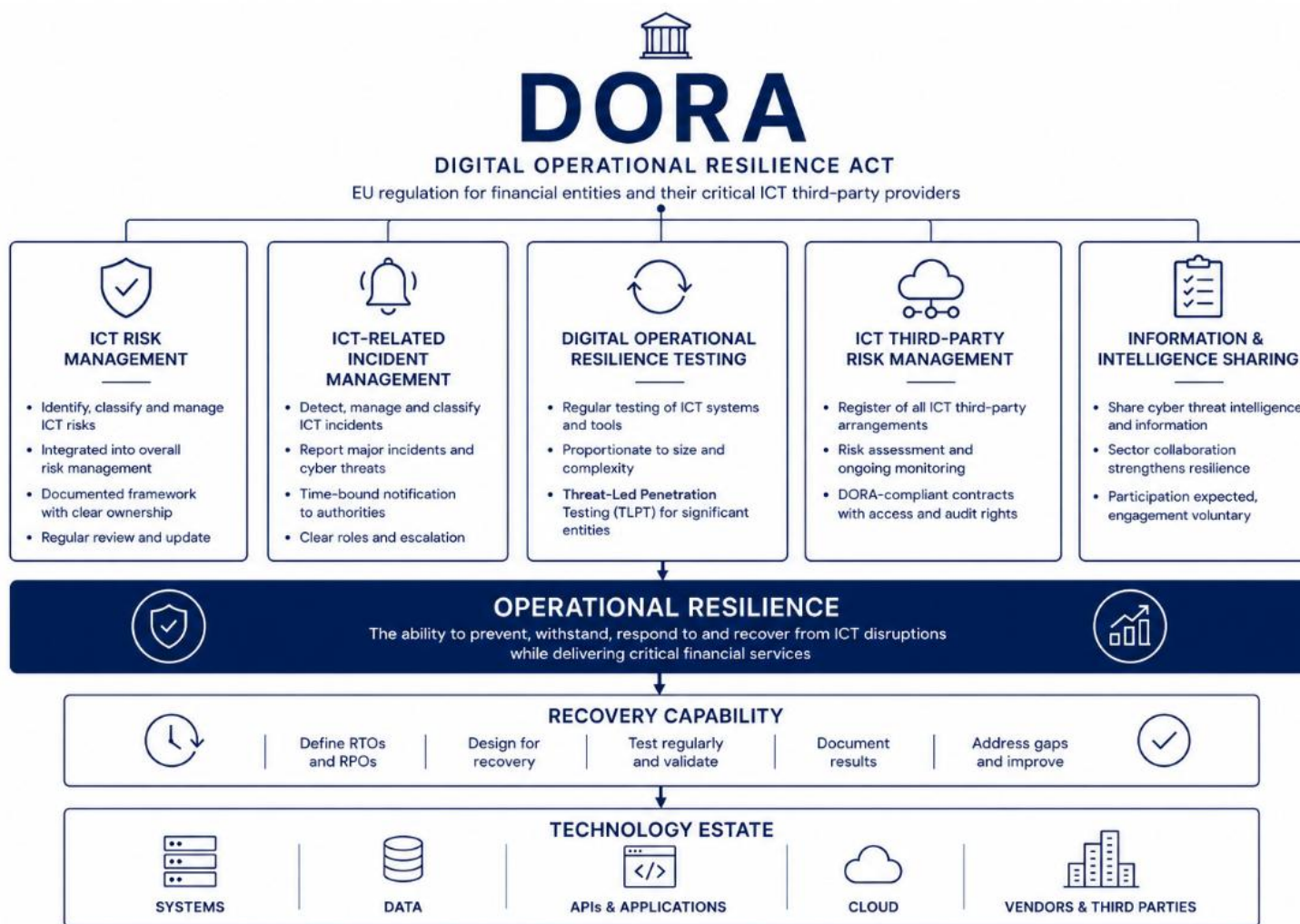
Savoir-Faire	Cellules Concernées			*Niveau			
	Décisionnelle	Technique	Stratégique	0	1	2	3
Reconstruire un "coeur de confiance"(infrastructures critiques, réseaux, outils d'administrations, outils de sécurités, ...) (Créer un socle système et réseau hors de portée de l'attaquant)		x					x
Rendre des outils bureautiques (en priorité aux membres des cellules de crise (mail, téléphonie, outils collaboratifs,...))		x			x		
Vérifier l'état des sauvegardes	x	x			x		
Définir la stratégie de reconstruction (où, avec quelles ressources, sous quel délai estimé, via quel procédure)		x					x
Remonter les applicatifs métiers une fois la santé de leurs sauvegardes validées		x					x
Assurer la continuité ou le redémarrage d'un service vital pour l'établissement dans un délai bref		x				x	
Retrouver dans un délai raisonnable un fonctionnement et une activité de production nominaux au sein de l'établissement		x					x
Reprendre le contrôle du SI		x					x
Mettre en place une protection durable pour éviter de reproduire une situation comparable (durcissement, revue des process,...)		x					x
Anticiper la réintégration des données produites pendant l'attaque dans les nouveaux systèmes remontés		x					x

*Niveau 0 : Socle de base; Niveau 1 : Débutant;
Niveau 2 : Intermédiaire; Niveau 3 : Confirmé

SOMMAIRE



INITIATIVE SECTEUR PRIVE - DORA



SOMMAIRE

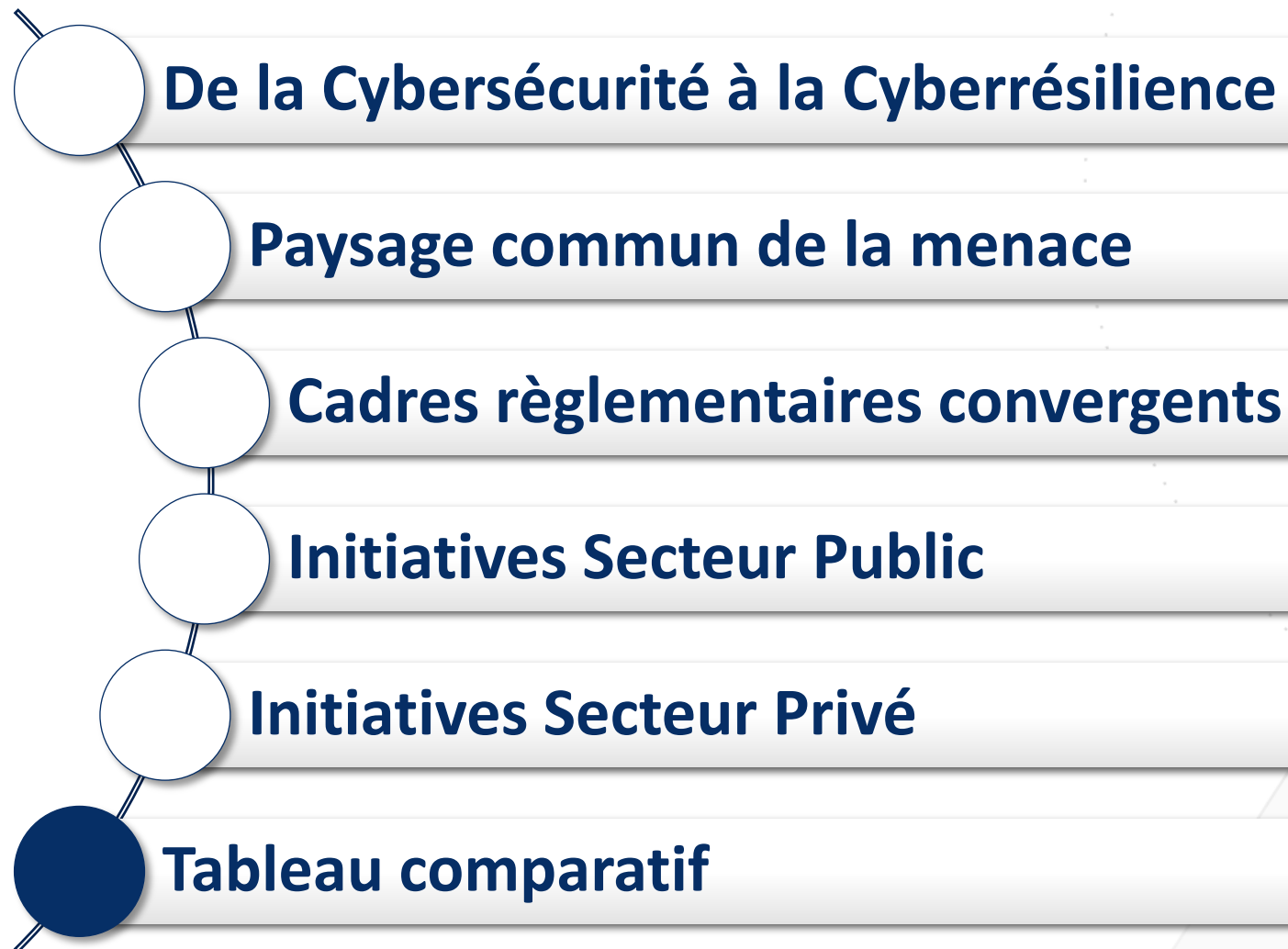


TABLEAU COMPARATIF



	Gouvernance	Gestion des risques	Gestion des tiers	Exercices / Techniques	Documentation
PUBLIC	++	++	+	+++	++
PRIVE	+++	++	++	+++	++

- ❖ **Gouvernance** : Anticiper le fonctionnement en mode dégradé, RACI, Comitologies.
- ❖ **Gestion des risques** : Cartographier les actifs, évaluer les risques
- ❖ **Gestion des Tiers** : Classer les tiers, Maitriser la chaine d'approvisionnement
- ❖ **Exercice/ Technique** : Circuit de communication, la sensibilisation, la réalisation d'exercices de crise, capitaliser
- ❖ **Documentation** : Corpus documentaire (PRI, fiches reflexes, etc.)

QUESTIONS

