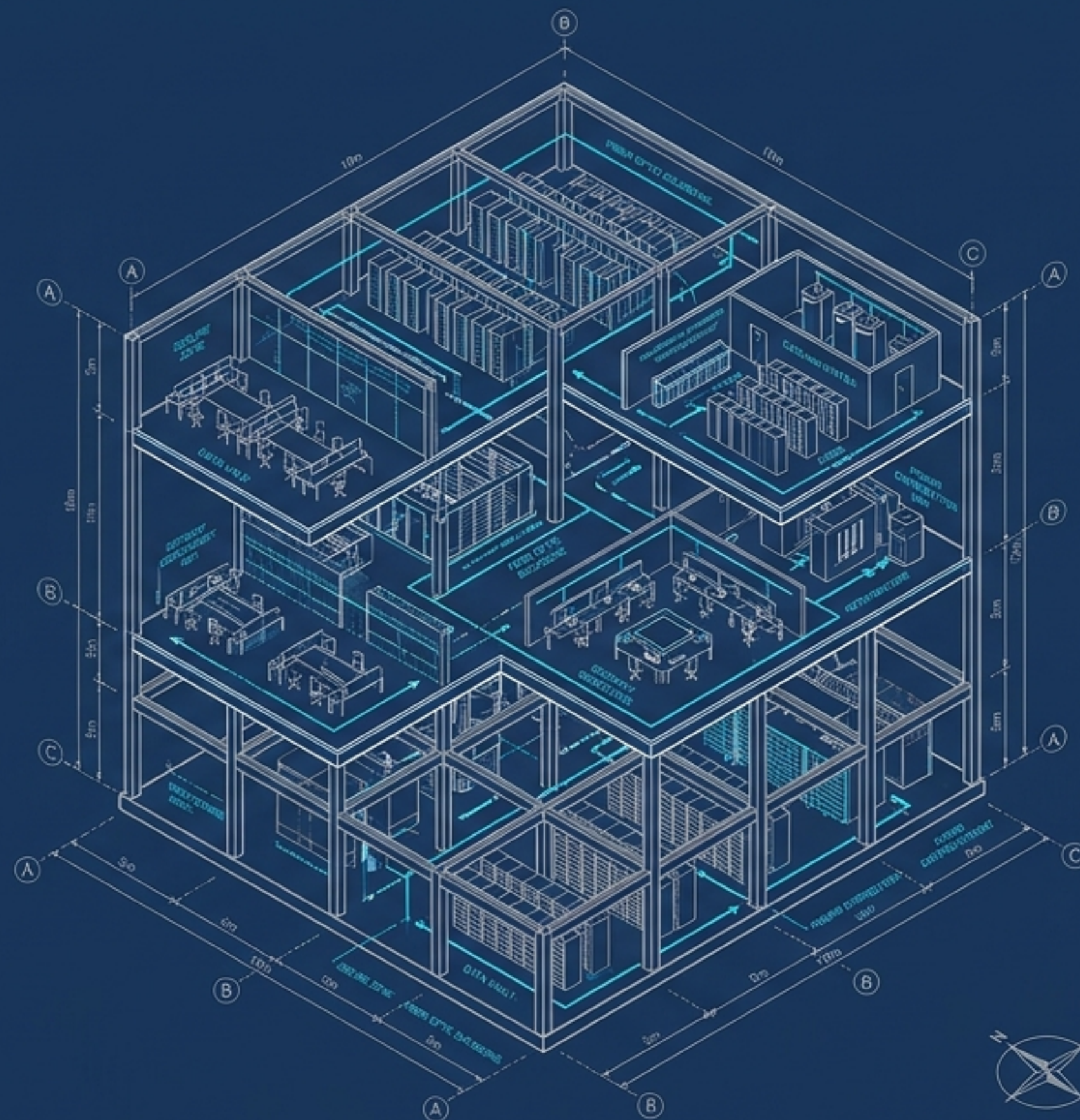


Surtitre: "Le Guide Stratégique en 5 Étapes"

L'Architecture d'un SOC Performant : Évaluer avant de Bâtir

Sous-titre: "Méthodologie d'évaluation des capacités des opérations de sécurité selon les normes COBIT."



Citation Centrale: « Donnez-moi six heures
pour abattre un arbre et je passerai les quatre
premières à affûter ma hache. »
— Abraham Lincoln

Explication: "La mise en place d'un Centre d'Opérations de Sécurité (SOC) exige une planification rigoureuse. Avant de définir une feuille de route, il est indispensable de comprendre l'environnement de référence : vos capacités actuelles en termes de personnel, de processus et de technologies."

PREP. STAGE: SHARPENING THE TOOLS

GRID REFERENCE: PLANNING & STRATEGY

EXEC. STAGE: INFRASTRUCTURE BUILD

WIRE FRAME: FUTURE SOC FACILITY

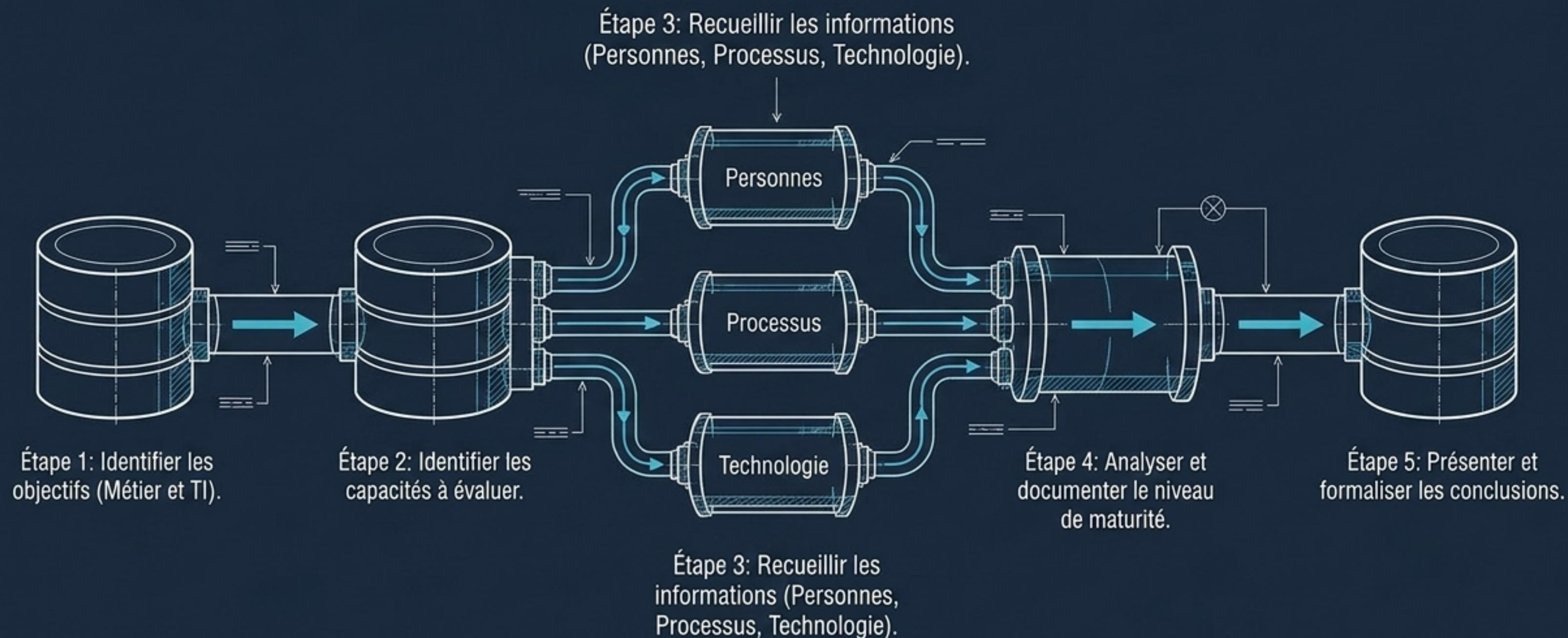
SCALE: 1" = 100'

PROJECT: SOC ROADMAP DEF.

SHEET: 01 OF 01

La Méthodologie d'Évaluation en 5 Étapes

SCALE 0 1 2 3 4 5 6 11m



Note de conception: "Ce processus doit être perçu comme un programme continu d'adaptation aux menaces, et non comme un audit ponctuel."

SCALE 0 1 2 3 4 5 6 11m

PROJECT: SOC ROADMAP DEF.

SHEET: 01 OF 01

Étape 1 : Cartographier les Attentes des Parties Prenantes

Matrice de Diagnostic des Parties Prenantes

ZONE 1 (RISQUE & RÉSILIENCE - CA / CRO)

Comment gérer l'ensemble des risques liés aux TI ? Le système est-il performant et résilient en cas de crise ?

ZONE 2 (FINANCE & CONFORMITÉ - PDG / AUDIT INTERNE)

Quel est le dépassement moyen des budgets informatiques ?
Le SI respecte-il les réglementations (ex: PCI DSS) ?

ZONE 3 (RESSOURCES & PERFORMANCE - DRH / CIO)

Dispose-t-on d'un effectif suffisant et compétent ?
L'informatique réagit-elle aux urgences plutôt que d'améliorer les processus ?

ZONE 4 (AGILITÉ - DIRIGEANTS D'ENTREPRISE)

Comment les TI peuvent-elles améliorer l'agilité globale de l'entreprise face aux nouvelles opportunités ?

La Cascade d'Alignement : Du Métier à la Technique



Objectif Métier :
Assurer la pérennité et la
conformité légale de l'entreprise.

Objectifs TI : Gérer les risques
liés aux TI (COBIT)

Assurer la sécurité de
l'information et des infrastructures.

Processus TI : Surveiller le
trafic du centre de données

Gérer une technologie de
prévention des pertes de
données (DLP)

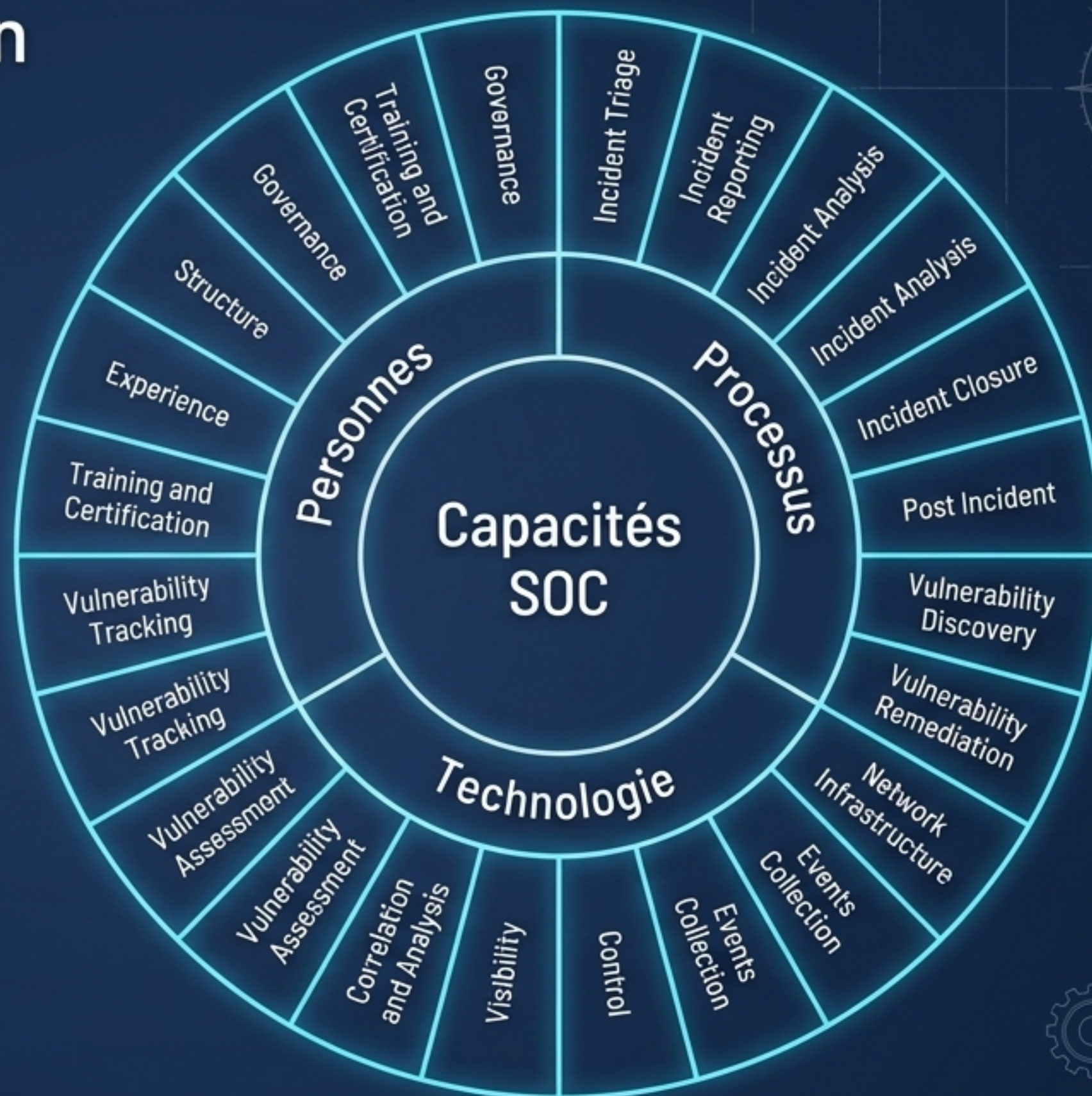
Insight Clé: "Une faille au niveau d'un processus technique fissure la fondation de l'objectif métier global."



Étape 2 : L'Anatomie d'un SOC (Modèle PPT)

Concept : Établir une liste exhaustive des capacités est complexe, mais la structure PPT (Personnes, Processus, Technologie) fournit un cadre universel pour évaluer les processus informatiques identifiés à l'Étape 1.

L'objectif est que chaque tranche de cette roue atteigne un niveau de maturité de 4 ou 5.



Décomposition des Capacités à Évaluer

Capability Triad Matrix

Personnel

Gouvernance (implication de la direction),
Structure (conflits d'intérêts, modèles de reporting),
Expérience (Investigations numériques avec EnCase, SIEM, Big Data),
Formation & Certifications.

Processus

Gestion des incidents (SLA, triage, plans de réponse).

Signalement (automatisation, hors heures ouvrables).
Analyse, Détection et correction des vulnérabilités.

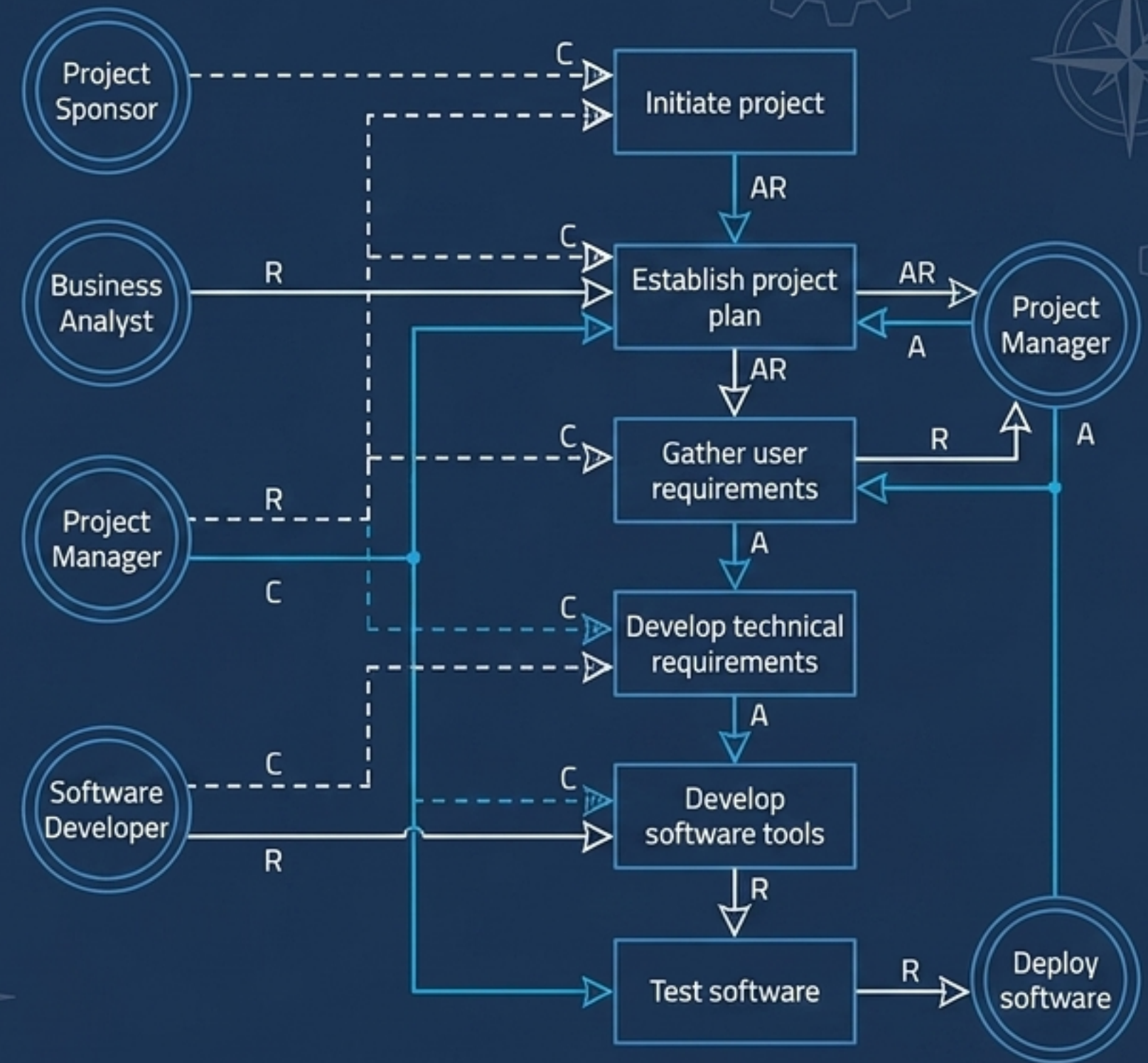
Technologie

Infrastructure (réseau hors bande, haute disponibilité),
Collecte et corrélation (évolutivité, cas d'usage spécifiques).
Surveillance (paquets réseau, angles morts, prévention d'intrusion),
Gestion des journaux.

Étape 3 : Orchestrer la Collecte de Données (La Matrice RACI)

Contexte: "Pour éviter toute 'contamination des données' ou influence biaisée, l'auditeur doit agir comme un consultant réunissant de multiples points de vue (PMO, ingénierie, gouvernance)."

La Méthode RACI: "Utiliser le modèle Réalisateur, Approbateur, Consulté, Informé (RACI) pour identifier les bons interlocuteurs lorsque les titres de postes sont flous. L'indépendance et l'exigence de preuves factuelles sont cruciales."



La Preuve Tangible : Cartographie de l'Existant

Blueprint Evidence Board



REGISTRE DES RISQUES

Date	Impact	Probabilité	Mesures Pré
1	9	22	
2	0	22	
3	0	15	
4	0	26	
5	0	27	
6	1	22	
7	0	21	
8	0	19	
9	0	27	
10	0	15	
11	0	22	
12	0	15	
13	0	22	
14	0	15	
15	4	20	
16	0	21	
17	0	27	
18	6	21	
19	0	21	

Données Techniques Requises :

- Listes des actifs et registres des risques.
- Schémas de réseau (attention aux informations obsolètes).
- Outils de surveillance et éléments de contrôle de sécurité.
- Fichiers de configuration et normes techniques.
- Documentation du modèle de sécurité et systèmes de billetterie (mesure de la santé des opérations).

FICHIERS DE CONFIGURATION

Server Name: 1107936

Server Name:

Server So:

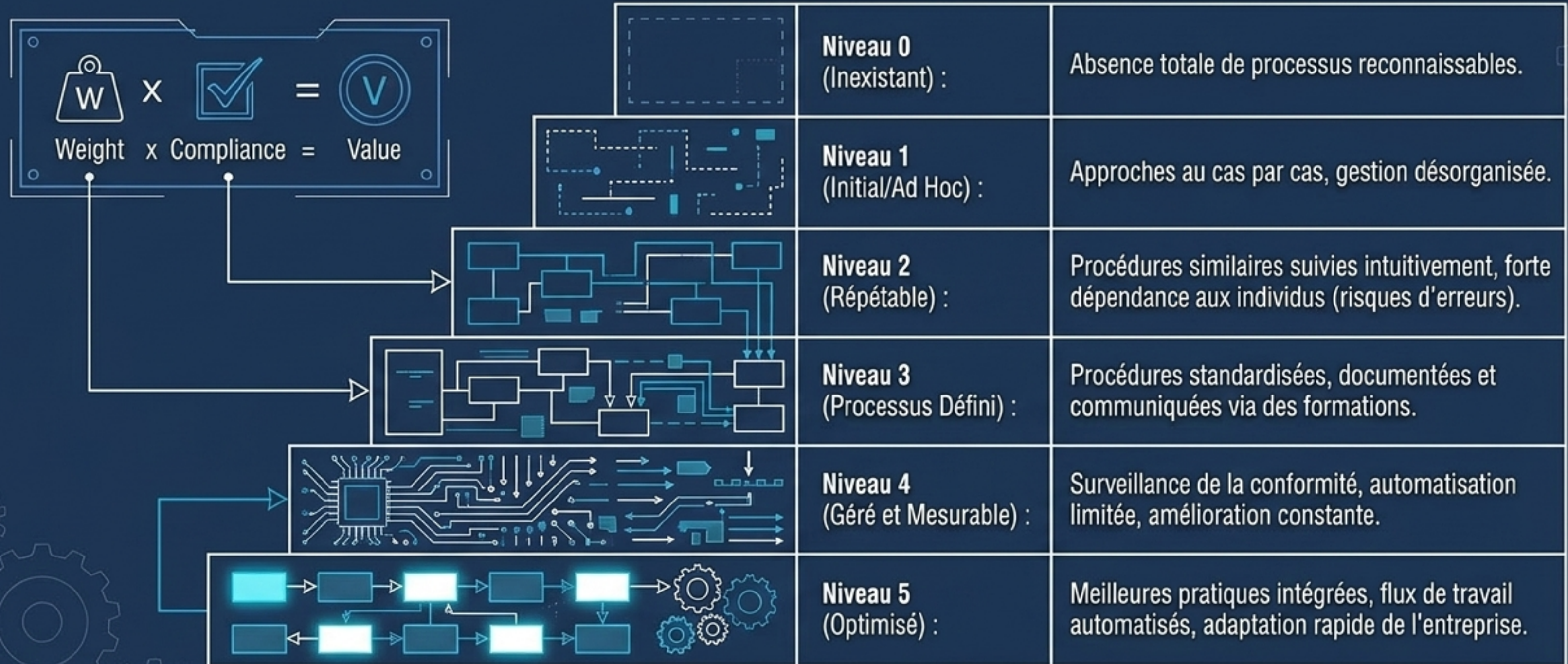
Parameters:

FICHIERS DE CONFIGURATION

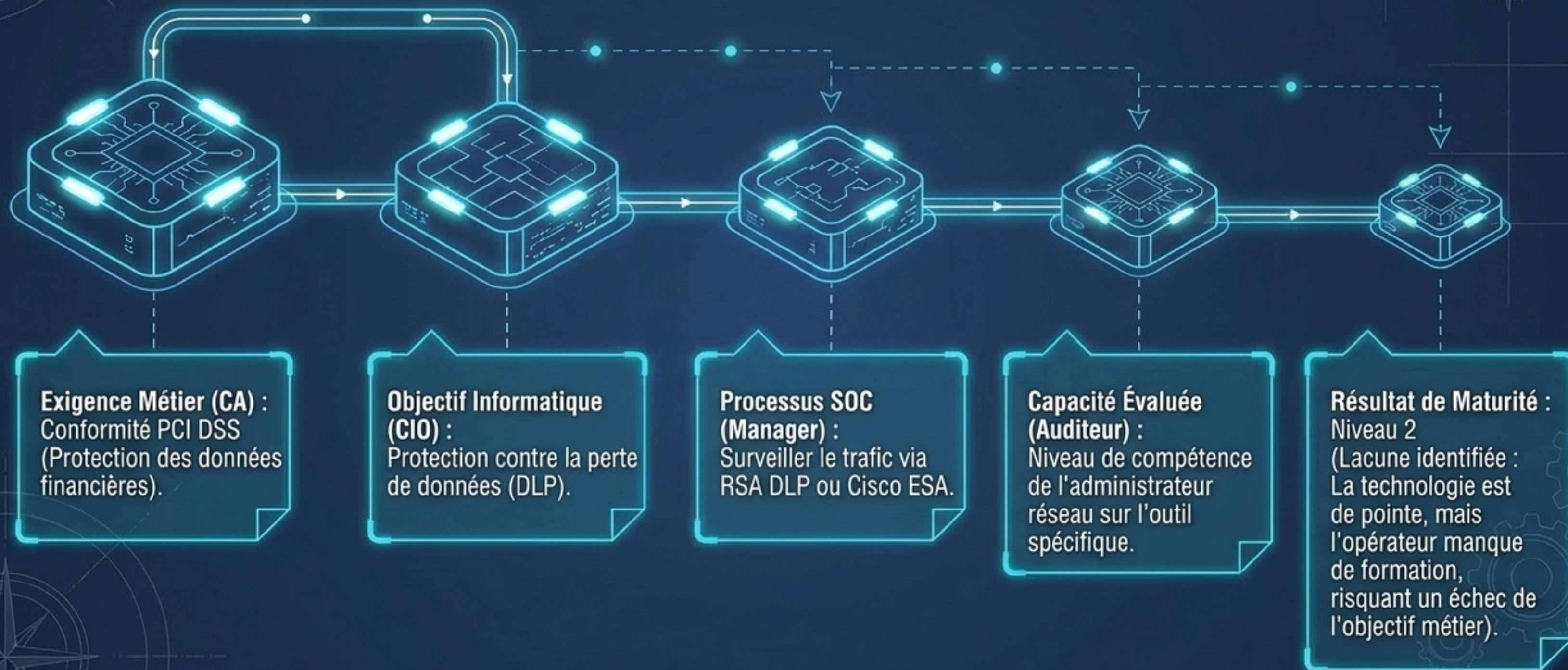
```
parameters (
  name: "test"
  parameter: "test"
)
parameters (
  name: "test"
  parameter: "test"
)
```

Action : "Ne jamais se fier uniquement aux déclarations orales. Vérifier systématiquement l'exactitude des rapports générés par les outils actuels."

Étape 4 : La Matrice de Diagnostic de Maturité COBIT



Synthèse : Le Moteur d'Alignement en Action



Étape 5 : Architecturer le Rapport Exécutif

1. Vision et Stratégie

Aligner les constats sur la stratégie de l'entreprise. Les lacunes stratégiques (SI vs Métier) doivent être exposées.

2. Exigences de Conformité

Mettre en évidence les risques légaux (ex: restrictions transfrontalières sur l'externalisation du SOC).

3. Paysage des Menaces

Justifier l'existence du SOC en cartographiant les menaces sectorielles et l'historique des incidents internes.



4. Budget et Parrainage

Définir clairement le parrain du SOC et relier les niveaux de maturité cibles à des analyses coûts-avantages concrètes.

La Hache est Affûtée : Prêt à Bâtir



Conclusion : L'évaluation des capacités n'est pas une fin en soi. C'est le retrait de l'incertitude. L'état actuel de votre sécurité est désormais quantifié, les dépendances sont cartographiées, et les lacunes sont exposées.

Prochaine Étape : Vous possédez maintenant les fondations factuelles nécessaires pour concevoir une stratégie SOC véritablement performante, financée et alignée sur la pérennité de votre entreprise. L'exécution peut commencer.