

Agile peut accélérer votre projet ou votre incident (de sécurité)

Fabrice De Paepe

Journée Agile – 22 Mai 2026

*« On fait
attention aux
vulnérabilités
dans le code »*

Et parfois un peu aux injections SQL...

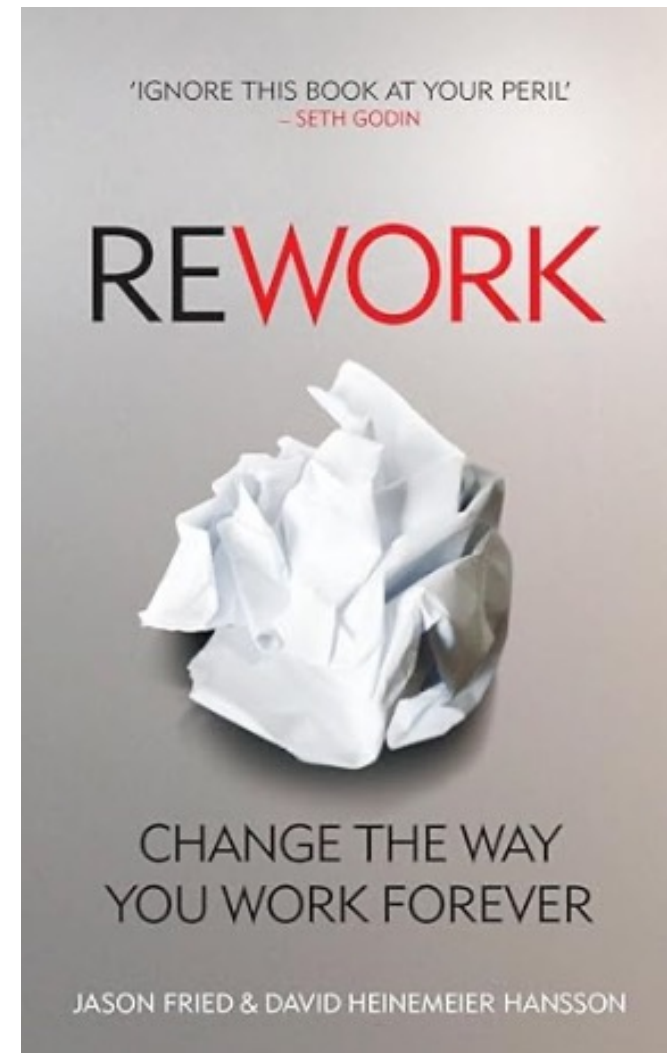
Nous n'avons
jamais livré aussi
vite

Mais nous n'avons
jamais été exposés
à autant de risques

- Virtualisation
 - CI/CD
 - Cloud
 - Microservices
 - Amélioration continue
 - Et maintenant l'IA – le Vibe Coding
-
- L'agilité a profondément transformé la manière dont les organisations développent leurs produits numériques.

Nous n'avons jamais
livré aussi vite

Aller vite
Eviter la bureaucratie
Simplifier
Meetings are toxics
Autonomie
Itération rapide
Less is More
Planning is guessing
Start making
something



Est-ce que nous livrons plus vite...

... ou est-ce que nous livrons les incidents (de sécurité) plus vite ?

Le problème



LA GOUVERNANCE

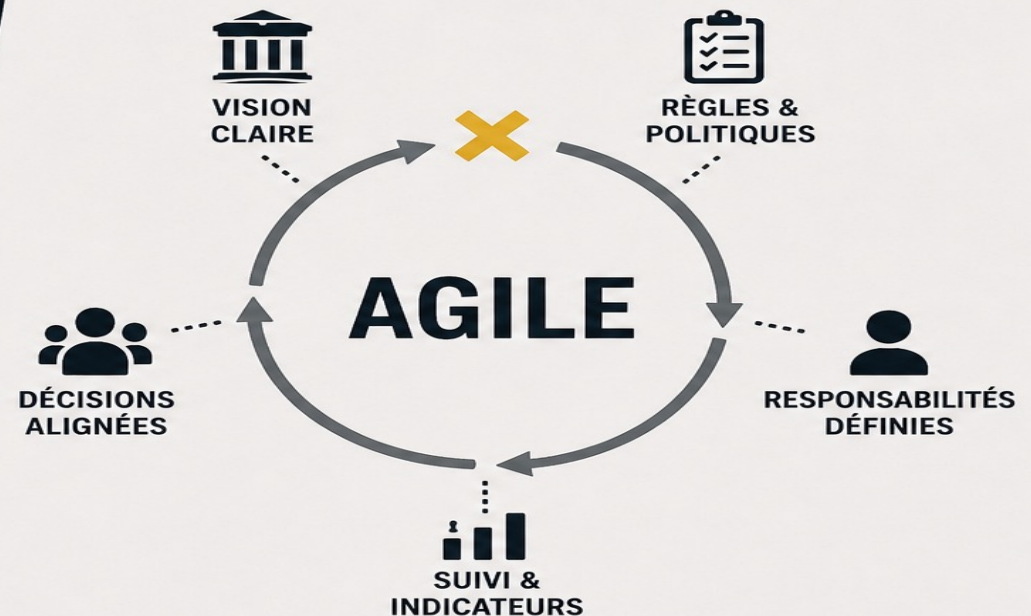


Le problème
n'est pas **Agile**.

Agile ne va pas résoudre
des problèmes si votre client
a déjà **très peu de Gouvernance**.



AGILE AMPLIFIE CE QUI EXISTE DÉJÀ. Sans Gouvernance, il **amplifie** le **chaos**.



Due Diligence

Prouves moi que tu t'es
posé les bonnes
questions

- Audits
- Risques
- Evaluation des fournisseurs
- Veille réglementaire
- KPI, etc.

Due Care

Montres moi ce que tu as mis
en place pour protéger

- Implémenter des contrôles
- Former les employés
- Sécuriser les systèmes
- Appliquer des « standards »
et politiques etc.

Agis – Protèges...



Construire une maison

- Scrum
- Une petite équipe
- Des outils simples
- On avance étape par étape et on parle souvent au proprio

Mais on ne commence pas par la salle de bain

10 équipes – 10 bâtiments

1 seul réseau de **route**, **d'eau**, **d'électricité**



**ON FONCE TÊTE BAISSÉE,
LIVRER TOUTES LES MAISONS ASAP**



- ❌ REWORK
- ❌ INCIDENTS
- ❌ SURCOÛTS
- ❌ RISQUES
- ❌ DETTE TECHNIQUE
- ✅ DETTE SÉCURITÉ

**OU ON S'ASSURE QU'IL Y A
QUAND MÊME QUELQUES
STANDARDS EN PLACE ?**



- ✅ COHÉRENCE
- ✅ SÉCURITÉ
- ✅ QUALITÉ
- ✅ RÉSILIENCE
- ✅ MAINTENABILITÉ
- ✅ PERFORMANCE

LeSS (Large-Scale Scrum)

**La réponse était honnête
mais révélatrice ...
il manque un truc.**

- ✗ Suppression profils sécurité
(Architectes, Security Champion, Threat Analyst, etc.)
- ✗ Autonomie *(on ne veut pas de sécurité)*
- ✗ PO non sensibilisé à la sécurité
- ✗ Moins de structure
- ✗ Equipe sincère
(+/- 70 développeurs...)



L'agilité sans sécurité,
c'est de la vélocité dans la mauvaise direction.

LeSS vs SaFe® (Scaled Agile Framework)



LeSS fonctionne très bien quand les équipes sont déjà *matures en sécurité*



LeSS réduit la structure



SaFe structure d'avantage le traitement du risque



Plus d'autonomie sans culture sécurité = *plus de surface d'attaque*



SaFe facilite davantage l'intégration systémique de la sécurité que LeSS



Aucun framework n'est « secure » par nature.
C'est l'implémentation qui l'est.

SAFe :



Architecture



Gouvernance



Rôles transverses de sécurité (optionnels)



Gestion de portefeuille



Risk Management



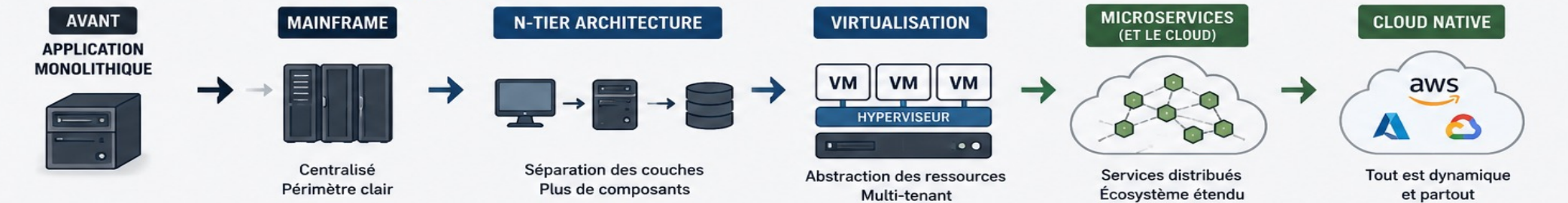
plus facile pour intégrer la sécurité



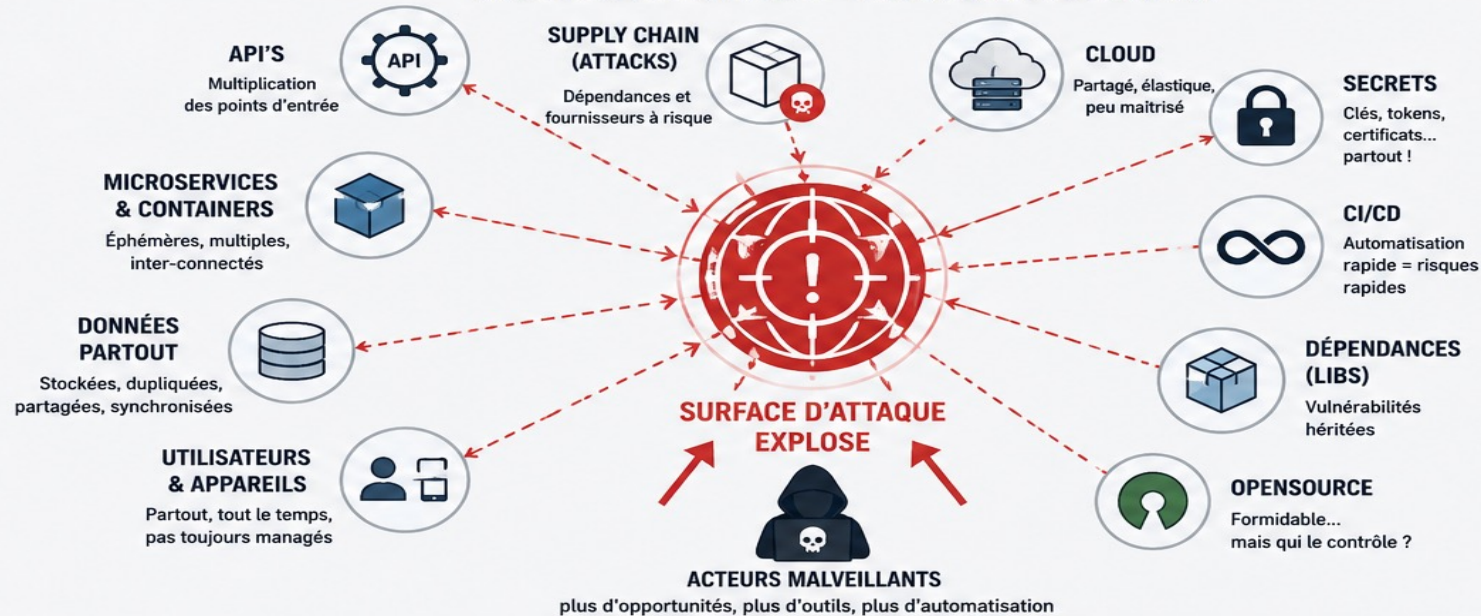
Mais lourdeur, et bureaucratie possible

POURQUOI LA SÉCURITÉ A CHANGÉ

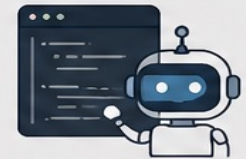
L'architecture a évolué. **Les risques aussi.**



UN MONDE PLUS CONNECTÉ = PLUS DE SURFACE D'ATTAQUE



ET MAINTENANT...



Claude Code, GitHub Copilot, IA...

Le code est généré plus vite que jamais.
Les erreurs aussi.



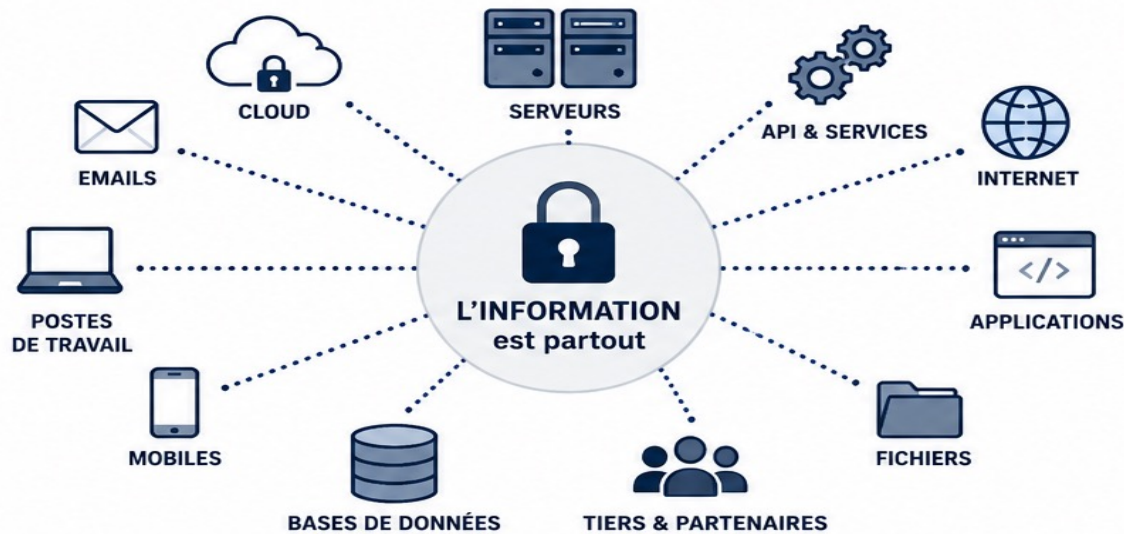
LA SURFACE D'ATTAQUE EXPLOSE – ET L'INFORMATION EST PARTOUT

Plus de technologie = plus de complexité = plus de risques

L'INFORMATION EST PARTOUT

et on doit la protéger en termes de

CONFIDENTIALITÉ, INTÉGRITÉ, ET DISPONIBILITÉ



ON DOIT LA PROTÉGER
selon la triade CIA



CONFIDENTIALITÉ

S'assurer que l'information n'est accessible qu'aux personnes autorisées.



INTÉGRITÉ

S'assurer que l'information est exacte, complète et non modifiée de manière non autorisée.



DISPONIBILITÉ

S'assurer que l'information est accessible et disponible quand elle est nécessaire.



De plus, en fonction de certains contrats et autres **lois et réglementations**, il arrive de devoir être en mesure d'auditer tout cela par :



TRAÇABILITÉ

Être capable de suivre et reconstituer les actions et événements.



LOGS

Conserver des journaux détaillés : qui a eu accès à quoi, qui a fait quoi, quand, depuis où, etc.



CONTRÔLE DES ACCÈS

Savoir qui a accès à quoi, avec quels droits, et à quel moment.



NON RÉPUDIATION

Pouvoir prouver qu'une action a été réalisée par une personne et ne peut pas être niée.



Ces exigences ne sont pas optionnelles : elles découlent de contrats, de lois et de réglementations (RGPD, ISO 27001, NIS2, DORA, HIPAA, SOX, etc.).

LE RÉGLEMENTAIRE ARRIVE >>>



**MOVE FAST
AND BREAK THINGS...**
ÇA C'ÉTAIT AVANT.



NOUVELLE RÉALITÉ

Vitesse, oui. Mais avec contrôle,
traçabilité, sécurité et conformité.



ALLER VITE

+



ÊTRE SÉCURISÉ

+



ÊTRE CONFORME

+



ÊTRE RÉILIENT

AUJOURD'HUI,
ON DOIT ÊTRE **COMPLIANT ET RÉILIENT.**



GDPR

Protection des données
personnelles



NIS2

Cybersécurité et résilience
des entités critiques



DORA

Résilience opérationnelle
du secteur financier



AI ACT

Régulation des systèmes
d'intelligence artificielle



CRA

Cyber Resilience Act
(sécurité des produits
numériques)



L'INNOVATION SANS COMPLIANCE EST UN RISQUE. L'AGILITÉ SANS GOUVERNANCE EST UNE FAILLE.

POURQUOI FAUT-IL UNE INFORMATION SECURITY GOVERNANCE ?



un large % de société n'adressent pas correctement les **menaces**, les **risques**, les **nouvelles technologies**, les **nouveaux enjeux** de sécurité de l'information correctement.



Les programmes de sécurité de l'info sont **insuffisants** pour rencontrer les besoins de l'entreprise.



Le **budget** sécurité est souvent inadapté.



La sécurité a évolué avec des contraintes réglementaires – **l'information à protéger est partout**.



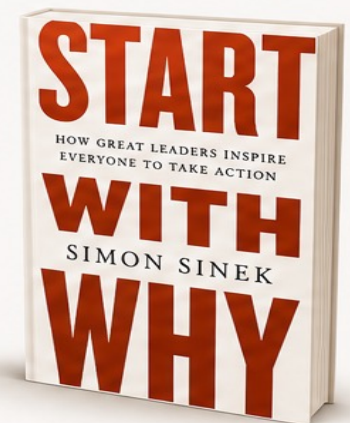
Et en plus on doit protéger **la vie privée**.



Dans certains cas les **SM** sont **Accountable** pour **IS Gouvernance**.



On doit **créer de la valeur** pour les actionnaires et les parties prenantes.



OBJECTIF : ALIGNER LA SÉCURITÉ DE L'INFORMATION AVEC LA STRATÉGIE DE L'ENTREPRISE POUR RÉDUIRE LES RISQUES, ASSURER LA CONFORMITÉ ET CRÉER DE LA VALEUR DURABLE.

INFORMATION SECURITY (IS) : NOTRE RÔLE

IS s'assure que l'info au centre est bien protégée par le **CIA**

ON A BESOIN DE CONTRÔLES...

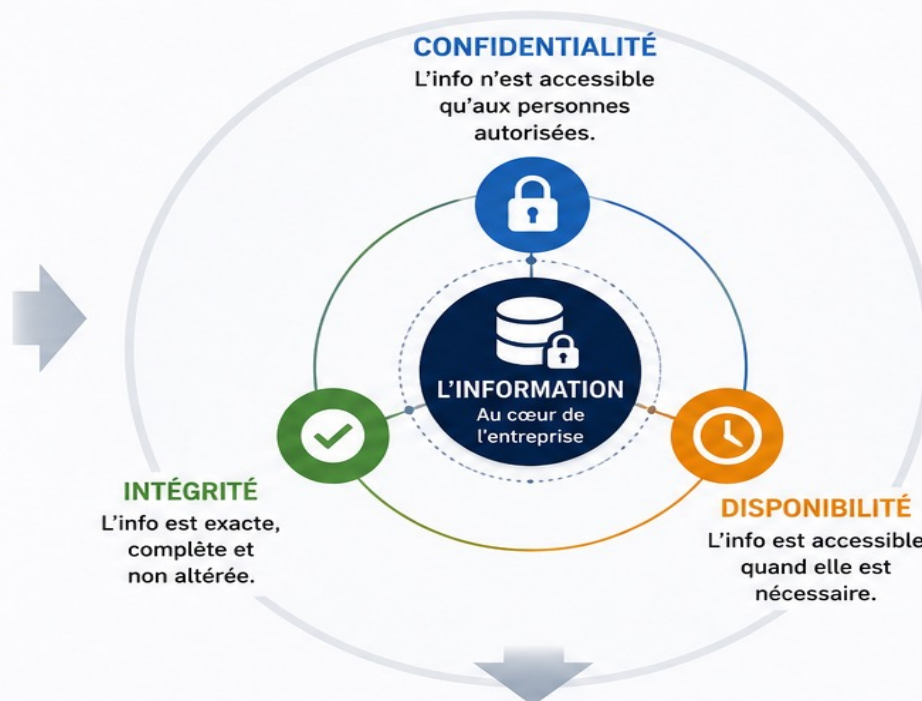
 **Préventifs**
Empêcher les incidents

 **Détectifs**
Détecter rapidement

 **Correctifs**
Limiter l'impact

 **Récupératifs**
Rétablir les services

 **Administratifs**
Gouverner et piloter



RISQUE

 **MENACE** ×  **VULNÉRABILITÉ** ×  **IMPACT**

 **MENACE**
Un événement potentiel qui pourrait exploiter une vulnérabilité.

 **VULNÉRABILITÉ**
Une faiblesse qui pourrait être exploitée par une menace.

 **IMPACT**
Les conséquences si la menace exploite la vulnérabilité.

 **Notre objectif : réduire le risque à un niveau accepté par l'entreprise.**

BESOIN DE PPPPT

 **PEOPLE**

- Sensibilisation
- Compétences
- Responsabilités

 **PROCESS**

- Gestion des risques
- Gestion des incidents
- Gestion des changements
- Continuité d'activité

 **POLICY**

- Politique de sécurité
- Standards
- Règles et exigences

 **PROCEDURES**

- Procédures opérationnelles
- Instructions de travail
- Bonnes pratiques

 **TECHNOLOGY**

- Contrôles techniques
- Outils de sécurité
- Architectures sécurisées



OBJECTIF FINAL : PROTÉGER L'INFORMATION POUR ASSURER LA CONFIANCE, LA CONFORMITÉ ET LA CRÉATION DE VALEUR POUR L'ENTREPRISE ET SES PARTIES PRENANTES.

ON ME DIT SOUVENT :
LA SÉCURITÉ EST UN FREIN.



SANS FREIN

VOUS ROULEZ À **300**
SI IL N'Y A PAS DE FREIN ?



- ✗ PERTE DE CONTRÔLE
- ✗ ACCIDENT
- ✗ ARRÊT BRUTAL
- ✗ DÉGÂTS IMPORTANTS
- ✗ MISE HORS ROUTE



SANS FREIN,
JE ROULE PAS À **120** SUR L'AUTOROUTE.



AVEC DES FREINS

DONC ON MET DES FREINS
POUR ALLER **PLUS VITE** !



- ✓ CONTRÔLE
- ✓ SÉCURITÉ
- ✓ CONFIANCE
- ✓ PERFORMANCE
- ✓ OBJECTIFS ATTEINTS

OBJECTIF
ARRIVER PLUS LOIN
PLUS VITE



LA SÉCURITÉ N'EST PAS UN FREIN,
C'EST CE QUI NOUS PERMET D'ALLER PLUS VITE
ET D'ATTEINDRE NOTRE DESTINATION EN TOUTE SÉCURITÉ.





Qui transporte le plus de personnes à l'heure ?

CONCLUSIONS



**L'AGILITÉ PERMET
D'ALLER PLUS VITE**



**LA SÉCURITÉ PERMET
D'ALLER PLUS LOIN**



**LES ORGANISATIONS
QUI RÉUSSIRONT DEMAIN
SERONT CAPABLES
DE FAIRE LES DEUX**



ALLER PLUS VITE
RÉAGIR, INNOVER, LIVRER
RAPIDEMENT



ALLER PLUS LOIN
RÉSILIANCE, CONFIANCE,
DURABILITÉ, CONFORMITÉ



L'AGILITÉ DOIT DEVENIR L'ALLIÉE DE LA SÉCURITÉ
(surtout dans les entreprises avec peu de gouvernance)



COLLABORATION
ÉQUIPES ALIGNÉES



PROCESSUS
INTÉGRÉS DÈS LE DÉPART
(SECURITY BY DESIGN)



CONTRÔLES SIMPLES
ET ADAPTÉS
(PROPORTIONNÉS)



VISIBILITÉ
ET FEEDBACK
CONTINU



LIVRER VITE
SANS PERDRE
LE CONTRÔLE



RÉSULTAT :
PLUS DE VALEUR,
MOINS DE RISQUES,
PLUS DE CONFIANCE



**FAIRE VITE, FAIRE BIEN, ET ALLER LOIN.
C'EST CELA, LA PERFORMANCE DURABLE.**



Q&A



<https://compliancewithoutcoma.com>

<https://www.linkedin.com/in/fabricedepaepe/>

<https://www.youtube.com/@compliancewithoutcoma>

<https://www.instagram.com/compliancewithoutcoma/>

<https://www.tiktok.com/@compliancewithoutcoma>