OSSIR × formind

Sécuriser ma chaîne de sous-traitants

À l'attention de **l'OSSIR**

TPRM - Des risques cyber forts et croissants …

Hausse des attaques impliquant des tiers

- En 2025, 30 % des violations de données ont impliqué un tiers *(vs 15% année -1, source Verizon DBIR 2025)*
- 98% des organisations ont au moins un fournisseur ayant subi une violation depuis 2 ans
- 41% des ransomware ont exploité une compomission de tiers *(Security Scorecard)*

Mauvaise connaissance de la conformité cyber des Tiers

- Pas de recensement
- Tiers sensibles non identifiés
- NDA et clauses de sécurité pas toujours pertinentes / appliquées / contrôlées
- Processus achats/ ISP non systématiquement utilisés
- Utilisation de shadow IT/ shadow AI
- Peu de visibilité sur les Tiers de Tiers
- Stock de Tiers rarement traités *(focus new - renew)*

Certains Tiers sont 'critiques'

- Risque de **fuite d'informations** stratégiques via le Tiers, le tiers de tiers, …
- Risque **d'intrusion**, de rebond sur mon SI
- Risque de **coupures de service**, de **perte** de données
- Risque de **dépendance**, de **souveraineté**, …
- Risque de **fraude** , d'altération de données critiques, de qualité de données

Absence ou faiblesse de contrôle des tiers

- Multiplication de questionnaires non adaptés
- Scans de surface éclairant 20% du problème
- Besoin d'audits réels du Top 10 – sur le bon périmètre
- Approche classique TPRM êu pertinente sur les 'gros' et 'tout petits'
- ….

Exigences réglementaires structurantes

TPRM – L'état de l'art

1. Cadre TPRM validé et opposable

- Le cadre doit être formalisé (politique TPRM ou § PSSI), validé et rendu **opposable**
- Il décrit les **responsabilités** de chacun, les **règles** de gestion et les points de **contrôle**
- Son application est contrôlée, dans un cadre d'amélioration permanente
- Les parties prenantes sont informées - formées

2. Identification / inventaire des Tiers

- Les prestataires et fournisseurs sont identifiés *(cf. achats / compta / …)*
- Ne pas viser l'exhaustivité, commencer par catégoriser …
- Les autres Tiers *(partenaires, JV, clients, …)* sont à 'catégoriser'

3. Classification des Tiers

- Recensement des Tiers & indicateur de criticité – cible DIC
- Analyse sur le build et idéalement sur le stock
- Les Tiers '**critiques**' sont adressés en priorité

4. Les tiers sont juridiquement engagés

- NDA généralisés & idéalement centralisés
- Clausiers types de sécurité à établir, par type de Tiers & par criticité
- Mise en œuvre avec les achats et les métiers (build & stock)
- Mécanismes de pénalités
- Focus sur les « petits & gros »

5. Plans d'Assurance sécurité (PAS)

- Créer un modèle de PAS IT et Métier + PAS Partenaire
- Préciser les obligations de moyens et les indicateurs & points de contrôle associés
- Le dérouler sur les Tiers critiques et sensibles – responsabilités à préciser
- Les contrôler régulièrement *(cf. point 6)*

6. Revues régulières de sécurité

- Comité sécurité & interlocuteur(s) sécurité
- Indicateurs adaptés (incidents, maintien des engagements dont certification, vulnérabilités, entrainement, …)
- Suivi des non-conformités / sous le seuil / pénalités

7. Auto-évaluation des Tiers

- Questionnaires ?
- Analyses régulières des surfaces d'attaques
- Mise en place d'une solution externalisée TPRM

8. Audit des Tiers les plus sensibles

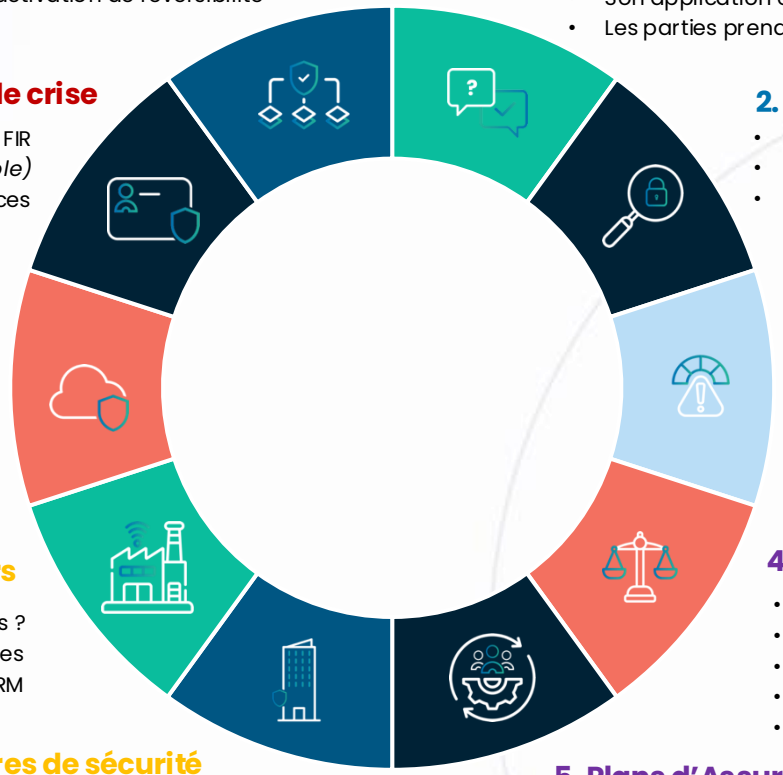
Clauses d'audit dans les contrats
Audits réguliers des prestataires les plus critiques
Gestion & suivi des recos / preuves

9. Gestion de crise

Procédure d'alerte et d'intervention – FIR
Exigence de tests de crise réguliers *(périmètre sensible)*
Implication des fournisseurs essentiels dans ces exercices

10. Switch des prestations non sécurisées

Clauses de sortie & réversibilité dans les contrats
Process de sortie & activation de réversibilité



Gouvernance **Identification** **Engagement & contractualisation** **Sécurisation & évaluation** **Détection & réaction**

Fournisseurs et prestataires IT (extrait)

Catégories	Sous-catégories	Principaux acteurs	Criticité Cyber max *				Accès SI	RTO	RPO	Commentaires
			Dispo	Intégrité Fraude	Confidentialité	Autre				
Infrastructure	Matériel & stockage	• Dell EMC, NetApp • HPE • Veeam (sauvegardes)								
	Infogérant - Hosting	• Cap Gemini • Atos								
	Services fondamentaux	• Microsoft AD • DNS, DHCP, NTP, VPN, …								
	Cloud	• Azure • AWS • OVHcloud								
	Sécurité	• Palo Alto, Crowdstrike, Splunk, … • Identité Okta • MFA & PKI								
	Collaboration	• Exchange • Teams, Slack • Cisco								
Applications	Services Infra	• IT SM : Service Now • VMWare • Atlassian								
	Logiciels SaaS	• CRM : Salesforce • ERP : SAP, Oracle • Docusign								
	Développement externe	• Sopra • …								
	Maintenance logicielle	• …								
…	…									

* *Impact de la défaillance du service du Tiers*

1 – Impact faible	*2 Impact significatif*	*3 Impact potentiellement majeur*

TPRM – L'approche progressive

Tiers 'Critiques' – 5%

Caractéristiques:
- Le fournisseur est critique pour l'activité ou l'entreprise
- Il dispose d'accès étendus au SI ou héberge des données critiques
- Les enjeux réglementaires, contractuels ou d'image sont élevés

Contrôles réalisés :
- Comités de sécurité renforcés
- Audit organisationnel complet (gouvernance, processus SSI, gestion des risques)
- Audit technique approfondi basé sur des preuves détaillées

Tiers 'Sensibles' – 20%

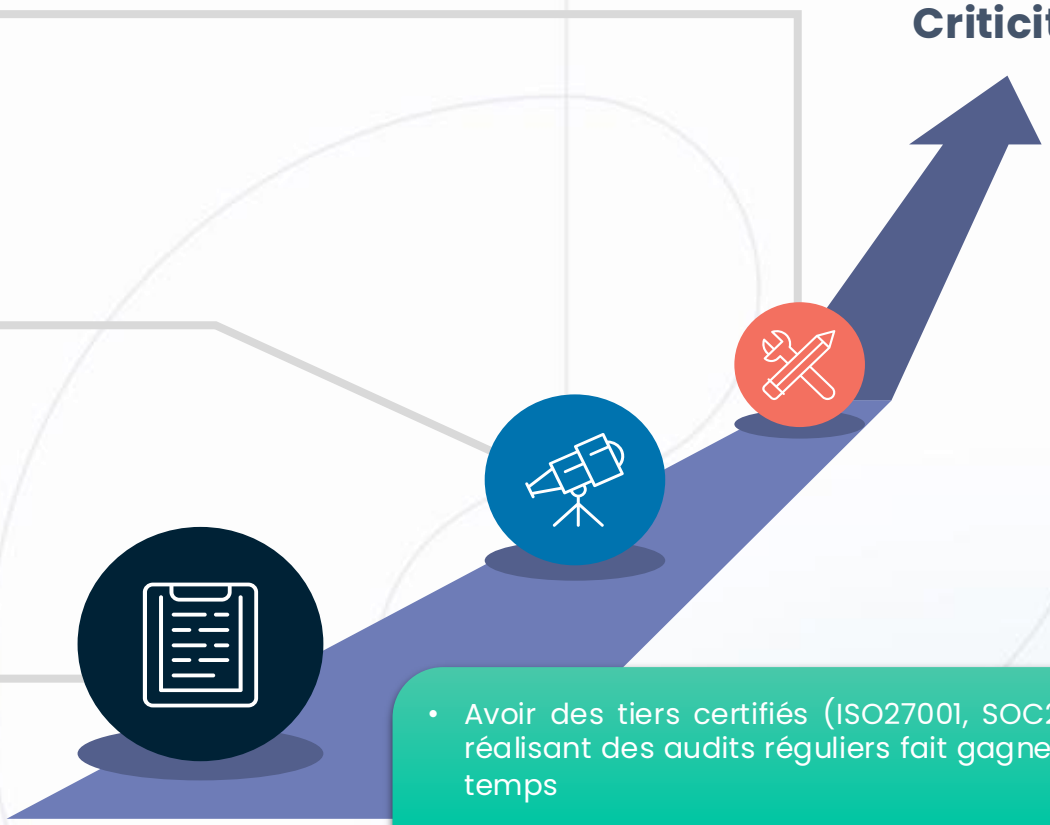
Caractéristiques:
- Le fournisseur a un accès à mon SI et/ ou traite des données sensibles
- Le scoring du contrôle de 1er niveau fait apparaître des signaux de risque
- Le service a un impact métier modéré à fort

Contrôles réalisés:
- Tous les contrôles de l'audit simplifié
- Analyse documentaire ciblée (politiques, procédures, attestations)
- Demande et revue de preuves (indicateurs, extraits d'outils, rapports)
- Entretiens ciblés avec les parties prenantes clés

Tiers 'Standards' – 75%

Caractéristiques:
- Le fournisseur présente un risque a priori limité
- Le service rendu n'implique pas d'accès sensible à mon SI

Contrôles réalisés:
- Évaluation automatisée du score de risque (outil de security rating / EASM)
- Envoi d'un questionnaire d'auto-évaluation & Analyse des réponses
- Attribution d'un premier niveau de risque
- Formulation de recommandations génériques



- Avoir des tiers certifiés (ISO27001, SOC2, …) réalisant des audits réguliers fait gagner du temps
- Une démarche outillée permet d'automatiser une grande partie de ces activités d'audits

Eléments de politique TPRM

1. Introduction

1. Objectifs
   - Cadrer les relations entre le Groupe et les tiers avec lesquels il échange des données (…)
   - *Identifier les responsabilités de chacun*
   - Préciser le cadre d'identification et de suivi des risques liés aux tiers
   - Edicter les principes et règles applicables
   - Dessiner les mesures de contrôle et d'amélioration permanente
2. Domaine d'application :
   - *Cadre de relation contractuelle avec un tiers : fournisseurs, partenaires, cotraitant, JV*
   - Politique applicable aux Acheteurs, équipes sécurité, équipes SI dont chefs de projet et SDM, Direction métiers susceptibles de réaliser des commandes et partenariats…
3. Principaux documents associés
   - Clauses contractuelles de sécurité
   - Plan d'Assurance Sécurité
   - NDA
   - Chartes 'usage du SI & administrateurs)
   - …

2. Responsabilités

1. Acheteurs
   - *Appliquer les contrats types incluant les clauses de sécurité*
   - *S'appuyer sur les équipes métiers et cyber pour toute négociation / dérogation de ces clauses*
2. Equipes sécurité
   - *Proposer les outils d'engagement des Tiers à la Cyber : Modèles types de plan d'assurance sécurité (PAS) adaptés par type de Tiers, clauses de cyber, procédures de contrôle*
   - *Venir en appui des équipes Achats ou métiers pour les Tiers sensibles ou critiques si le cadre ne peut s'appliquer*
3. Directions métiers
   - *Identifier les Tiers sensibles et critiques relevant de sa responsabilité – notamment ceux avec lesquels des données classifiées (secret ou confidentiel) sont partagées*
4. Commanditaire – Managers métiers
   - *Analyser le risque lié aux Tiers avec lesquels il a ou vise une relation contractuelle (build & stock)*
   - *Appliquer le processus TPRM en renseignant le PAS pour les Tiers sensibles et critiques*
   - *Faire appel aux équipes Achats et Cyber selon besoins*
5. Filière Juridique
   - *Rédige & valide les clauses de sécurité pour les Tiers (fournisseurs, partenaires, JV, …)*
6. Direction de l'audit : intègre la sécurité des Tiers dans son programma d'audit ?
7. Fournisseurs - Partenaires - JV
   - *Respectent les engagements de sécurité et remontent tout incident*

3. Principes

1. Le niveau de sécurité assuré par les Tiers sur le SI et les informations du Groupe XXX Construction doit être au moins équivalent à celui assuré en interne
2. Approche par les risques : les exigences sont proportionnées au niveau de risque encouru
3. Les obligations de sécurité avec les tiers sont rendues opposables, à la fois en obligation de résultat (cf. NDA et clauses contractuelles) et en obligation de moyens (PAS)

4. Règles

1. Un **NDA** est signé avec tous les tiers **avant** échange d'informations confidentielles ou secrètes
2. Les Tiers avec lesquels des informations sensibles sont échangées sont identifiés / **classifiés**
3. Les **clausiers** de sécurité sont intégrés et négociés selon besoins dans tout achat sensible, métier et IT, ainsi que dans les partenariats et JV
   Les exigences applicables aux Tiers s'appliquent également à leurs éventuels sous-traitants susceptibles d'accéder aux informations de XXX Construction
4. Le **PAS** (Plan d'Assurance Sécurité) est obligatoire et opposable pour toute contractualisation avec un Tiers sensibles
   Ce PAS, cosigné des parties, précise notamment les engagements de résultats et de moyens, ainsi que les points de contrôle / indicateurs envisagés
5. A l'issu d'un contrat, la phase de réversibilité doit permettre de supprimer l'ensemble des données sensibles de XXX Construction sur le SI du Tiers et d'en mettre les preuves à disposition

5. Contrôles

1. Des **revues de sécurité** / comité sécurité sont régulièrement menées, a minima annuellement, pour tout Tiers sensible ou critique (revue des engagements du PAS), en particulier pour suivre :
   - Le suivi des événements de sécurité (incidents, failles, manquements)
   - Le suivi des éventuelles dérogations
   - Les résultats des contrôles réalisés (revues d'habilitations, tests d'intrusion, …)
2. Des contrôles sont opérés sur le parc de Tiers sensibles
   Un processus de 'self assesment' peut être requis.
   De même, un processus de scans de vulnérabilités externes peut être mis en place (à discuter)

Merci

Hervé MORIZOT

Co-CEO

06 70 45 77 58

Herve.morizot@formind.fr

www.formind.fr

formind

Security for business performance