board of cyber

CESIN

OBSERVATOIRE TPRM 2025

Le risque cyber lié aux fournisseurs

Face à la montée des risques cyber, les entreprises centralisent la gestion du risque fournisseur et aspirent à une mutualisation de la notation

3e ÉDITION

Sommaire

OBSERVATOIRE TPRM 2025
Le risque cyber lié aux fournisseurs

Introduction

Cette troisième édition de l'Observatoire du risque cyber lié aux fournisseurs, menée par Board of Cyber en partenariat avec le CESIN, s'appuie sur les réponses de plus de **170 entreprises** de toutes tailles et de tous secteurs d'activités.

Elle donne la parole à celles et ceux qui sont en première ligne face à la complexité croissante des écosystèmes numériques et de la menace cyber : RSSI, DSI, CTO, directeurs conformité. Leurs témoignages, recueillis pendant l'été 2025, sont essentiels. **Ils éclairent directement l'évolution du paysage cyber et la montée en puissance d'un risque tiers désormais reconnu comme stratégique**.

Leurs témoignages révèlent une maturité en nette progression : la prise de conscience de l'importance du TPRM (*Third Party Risk Management*) est désormais généralisée. Une étape importante est franchie. Pour autant, la consolidation de cette maturité nécessite encore de lever des freins persistants. Cette édition 2025 explore les approches les plus prometteuses pour rendre la gestion du risque plus efficace, continue et partagée.

En remerciant les décideurs qui ont contribué à cette étude, le CESIN et Board of Cyber réaffirment leur ambition commune : **accompagner la montée en maturité des organisations françaises et européennes et promouvoir une approche collective, mesurée et durable du risque cyber fournisseurs.**

ÉDITORIAL

Face à l'ampleur du risque, un changement de méthode s'impose

Quand un nouveau risque émerge dans l'environnement des entreprises, deux étapes s'enchaînent naturellement : d'abord, en mesurer l'ampleur ; ensuite, définir les moyens d'y répondre.

Concernant le risque cyber lié aux fournisseurs, la première étape est désormais derrière nous et prise en compte par le management. La transformation digitale, en s'accélérant, a considérablement élargi la surface d'attaque des organisations. Par ailleurs, l'uniformisation des logiciels offre aux cyberattaquants un terrain d'action démultiplié. Résultat : **le risque cyber fournisseur est devenu un risque systémique**. Les régulateurs, eux, l'ont bien compris et s'attaquent au sujet via des dispositifs comme DORA ou NIS2.

Nous entrons maintenant dans le vif du sujet : sécuriser les fournisseurs, quels que soient leur taille, leur secteur ou les services qu'ils rendent. Deux questions stratégiques s'imposent. Premièrement, les externalisations opérées ces dernières années, pour se recentrer sur le « cœur de métier », sont-elles encore pertinentes ? Deuxièmement, comment piloter efficacement la cybersécurité de centaines, voire de milliers de fournisseurs qui composent aujourd'hui la supply chain des grandes entreprises ?

Une chose est sûre : **il est temps de rationaliser les méthodes de gestion du risque cyber fournisseur.** Cette nouvelle édition de l'Observatoire TPRM révèle une forte attente des entreprises en matière de mutualisation et d'automatisation. Face à l'ampleur du défi, l'urgence d'agir n'est plus à démontrer.

Frank VAN CAENEGEM
Administrateur du CESIN, RSSI EMEA de Schneider Electric

Alain BOUILLÉ
Délégué général du CESIN

OBSERVATOIRE TPRM 2025
Le risque cyber lié aux fournisseurs

ÉDITORIAL

Le calme avant la tempête ?

Cette nouvelle édition de l'Observatoire des risques cyber fournisseurs, réalisée par Board of Cyber en collaboration avec le CESIN, confirme que les entreprises ont franchi un cap : elles tendent à reconnaître de plus en plus clairement le risque cyber fournisseurs comme **un enjeu stratégique de gouvernance et de résilience.**

Les attaques fréquentes, en 2025, ont encore souligné le risque lié aux tiers, l'interdépendance des entreprises avec leur écosystème et l'impact financier de ces attaques. En revanche, le décalage de l'application de NIS2 en France a retardé le passage à l'échelle de l'évaluation des fournisseurs pour de nombreuses organisations.

Les réponses recueillies dans cette édition révèlent une dynamique encourageante : l**a cybersécurité fournisseurs n'est plus un sujet périphérique**, elle s'impose désormais comme un enjeu stratégique de gouvernance et un levier structurant de la confiance numérique. Mais la route reste longue. Charge de travail chronophage, hétérogénéité de maturité des fournisseurs, complexité de les engager, manque de ressources… L'enjeu, désormais, n'est plus de convaincre, mais de trouver la bonne réponse pour industrialiser. Deux thématiques sont mises en avant pour faire face à cet enjeu : la mutualisation de l'évaluation des fournisseurs, plébiscitée par 80 % des participants et la demande d'automatisation nécessaire pour éviter la charge stérile du remplissage de questionnaire par les fournisseurs.

C'est à ce prix que les entreprises parviendront à transformer la prise de conscience en véritable culture du risque partagé, fondée sur des évaluations continues, standardisées et reconnues.

Ce mouvement collectif, que Board of Cyber accompagne depuis plusieurs années, s'inscrit au cœur d'une ambition au service de l'écosystème : **rendre la mesure du risque cyber fournisseurs plus simple, plus lisible et plus fiable** pour toutes les organisations.

Luc DECLERCK
Directeur général de Board of Cyber

1

La régulation, moteur de maturité

La prise de conscience continue de progresser, portée par la pression réglementaire et la volonté des organisations de mieux maîtriser un risque désormais stratégique.

OBSERVATOIRE TPRM 2025
Le risque cyber lié aux fournisseurs

Comme en 2024, plus de 80 % des organisations interrogées (81,8 %) considèrent le risque fournisseur comme « important » ou « très important », un constat partagé par tous les secteurs d'activité, y compris les acteurs publics. Cette perception homogène témoigne d'une évolution culturelle : la dépendance numérique est désormais reconnue comme un facteur majeur de résilience.

Et les réglementations contribuent directement à cette prise de conscience. Seules 16 % des entreprises interrogées ne sont, pour l'instant, concernées par aucun texte. Le ruissellement des exigences de sécurité vers les fournisseurs – NIS2, DORA, CRA – a déjà commencé, imposant progressivement à l'ensemble des fournisseurs IT des standards de sécurité et des audits réguliers, avec des niveaux de responsabilités accrus.

L'étude montre que huit entreprises sur dix évoluent dans un cadre réglementaire renforcé : 63 % mentionnent la directive NIS2, 36 % l'AI Act et 32 % le cadre DORA. Pour 55 % des répondants, toutefois, cet environnement réglementaire ne modifie pas encore leur approche du risque fournisseurs ou partenaires.

Ce constat interroge : s'agit-il d'un manque de moyens, d'un déficit d'outillage, d'une clarté encore insuffisante des exigences ou du fait que les pénalités prévues par les textes ne sont pas encore pleinement effectives ? Quoi qu'il en soit, la régulation semble agir moins comme un levier opérationnel immédiat que comme un **cadre structurant à moyen terme**, incitant les organisations à formaliser leurs pratiques et à renforcer la coopération avec leurs partenaires.

Cette évolution se traduit déjà dans les modes de gouvernance : 60 % des entreprises centralisent désormais la gestion du risque fournisseurs au niveau du siège, contre 55 % en 2024 (tandis que 32 % optent pour une gestion hybride et 12 % pour une approche décentralisée). Cette tendance à la centralisation confirme que la conformité réglementaire devient un **vecteur d'intégration** et un **moteur d'unification** de la gestion du risque cyber au sein des organisations.

À RETENIR

81,8 %

des organisations interrogées considèrent le risque fournisseur comme « important » ou « très important ».

2

Les RSSI en première ligne, les Comex à la table

Sous l'effet conjugué de la pression réglementaire et de la montée des enjeux cyber, la gestion du risque fournisseurs devient un exercice collectif, désormais suivi jusqu'au Comex.

Dans 87 % des entreprises, la fonction RSSI groupe est la plus impliquée dans la gestion du risque fournisseurs/partenaires devant la direction des achats (60 %), la direction juridique (60 %), le RSSI de la business unit (44 %), le risk manager et le responsable conformité (30 %).

L'implication de la direction juridique connaît une progression spectaculaire : 11 % en 2024, contre 60 % aujourd'hui. Cette évolution s'explique en grande partie par l'extension du champ réglementaire : 90 % des entreprises qui associent la direction juridique à ce pilotage sont en effet soumises à une réglementation cyber.

Près d'une entreprise sur deux (48 %) applique, en outre, un processus différencié pour ses fournisseurs IT, signe que la maturité se renforce là où les enjeux de dépendance technologique sont les plus critiques.

La dynamique s'étend également aux directions générales et aux comités exécutifs. Dans 54 % des entreprises, le risque cyber fournisseurs fait désormais l'objet d'un suivi au plus haut niveau – proportion qui atteint 80 % parmi celles qui le jugent important ou très important (contre 76 % en 2024).

À RETENIR

60 %

des entreprises impliquent aujourd'hui la direction juridique dans la gestion du risque fournisseurs. Un chiffre en forte hausse : elles étaient 11 % en 2024.

À RETENIR

54 %

des entreprises assurent un suivi du risque cyber fournisseurs au plus haut niveau (directions générales et Comex).

Ce mouvement est très marqué dans la banque et l'assurance, où la supervision du risque fournisseurs par le Comex concerne plus de 82 % des organisations. Dans les grandes entreprises, cette implication atteint un cas sur deux.

L'ensemble de ces données traduit une **évolution structurelle :** la gestion du risque fournisseurs n'est plus un domaine purement opérationnel, mais un sujet de **gouvernance partagée**, où convergent désormais les logiques de sécurité, de conformité et de performance.

Cette gouvernance élargie montre une maturité accrue, mais révèle aussi ses limites : si le risque fournisseurs est désormais reconnu comme stratégique, il reste souvent sous-évalué dans son suivi opérationnel.

3

Un risque reconnu mais encore sous-surveillé

Malgré une conscience accrue du risque tiers, la majorité des entreprises continuent d'évaluer un nombre restreint de fournisseurs, faute de ressources suffisantes ou par choix de priorisation.

OBSERVATOIRE TPRM 2025
Le risque cyber lié aux fournisseurs

Pour la moitié des entreprises, le nombre de fournisseurs effectivement évalués reste inférieur à vingt. Même parmi les grands comptes – dont près de 90 % considèrent le risque fournisseurs comme important ou très important – seuls 55 % procèdent à l'évaluation de plus de cinquante fournisseurs par an.

On aurait pu s'attendre à un périmètre plus large, couvrant plusieurs centaines, voire milliers de partenaires, mais les contraintes opérationnelles demeurent fortes.

Deux hypothèses qui se superposent certainement pour de nombreuses sociétés :

➜ D'une part, les **coûts de certaines méthodes d'évaluation** restent élevés et limitent la fréquence ou la profondeur des contrôles.

➜ D'autre part, la mise en œuvre d'un *tiering* (priorisation des évaluations sur les fournisseurs critiques) permet de concentrer les efforts sur un périmètre plus restreint mais jugé stratégique.

À RETENIR

55 %

seulement des grands comptes procèdent à l'évaluation de plus de cinquante fournisseurs par an.

À RETENIR

68 %

des entreprises ont désormais érigé la classification des risques comme norme, contre 60 % en 2024.

L'étude montre aussi que 63 % des sociétés au total évaluent moins de cinquante fournisseurs. C'est donc une problématique transverse à tous les secteurs et toutes les tailles d'organisation.

L'Observatoire révèle également que la classification des risques est désormais la norme pour 68 % des entreprises, contre 60 % en 2024. Cette classification est définie selon la criticité du service ou du produit délivré par le fournisseur (69 %, contre 57,4 % en 2024), de son niveau d'intégration dans le système d'information de l'entreprise (67 %, contre 51,4 % en 2024), de l'accès à des données personnelles (62 %, contre 48 % en 2024) ou stratégiques (58 %, contre 44,5 % en 2024).

Ces chiffres confirment une évolution méthodologique notable : les entreprises structurent davantage leur approche du risque fournisseurs, mais la **profondeur de la surveillance** reste encore limitée au regard de l'ampleur des interdépendances numériques.

4

Une multiplicité de dispositifs d'analyse du risque

Face à la complexité croissante de leurs chaînes d'approvisionnement, les entreprises recourent à une grande variété d'outils pour évaluer le risque cyber de leurs fournisseurs. Mais aucune méthode ne s'impose encore comme référence commune.

OBSERVATOIRE TPRM 2025
Le risque cyber lié aux fournisseurs

L'Observatoire TPRM 2025 montre à nouveau que les entreprises mobilisent des outils de nature différente pour évaluer le risque cyber fournisseurs. Selon les réponses apportées par les entreprises, les dispositifs les plus utilisés en 2025 sont :

- Le Plan d'Assurance Sécurité (75 %), en augmentation par rapport au précèdent Observatoire (66,3 %) ;
- Le questionnaire auto-déclaratif (60 %), moins utilisé qu'en 2024 (66,3 %) ;
- La certification ISO SOC 2 (55 %) ;
- Le questionnaire avec dépôt de preuve (40 %) ;
- La notation cyber (34 %, contre 29,7 % en 2024) ;
- Test d'intrusion (30 %) ;
- Audit GRC (29 %) ;
- CTI (fuite de données, incidents, récents, rançongiciels...) (20 %).

Si l'appétence pour les PAS et les questionnaires de sécurité reste élevée, ces dispositifs demeurent difficilement industrialisables dans leur forme actuelle.

À l'inverse, le recours aux certifications s'impose progressivement comme une voie de mutualisation crédible, soutenue par l'émergence de cadres européens tels que le schéma EUCC. Cette dynamique reste toutefois limitée pour les fournisseurs considérés comme critiques. Elle illustre une tension récurrente : les démarches de conformité se multiplient, mais leur reconnaissance mutuelle demeure partielle, ce qui ne valorise pas toujours les efforts significatifs consentis par les fournisseurs.

La fréquence des évaluations tend également à s'homogénéiser. Un tiers des entreprises interrogées déclarent aujourd'hui évaluer leurs fournisseurs une fois par an, contre 48 % en 2024. 19 % d'entre elles procèdent à une évaluation tous les deux ans et une proportion équivalente tous les trois ans (contre, respectivement, 13 % et 30 % en 2024). Enfin, 35 % des entreprises n'ont pas encore défini de rythme d'évaluation précis.

Ces résultats traduisent une **volonté de structuration**, mais aussi une **recherche** d'équilibre entre exhaustivité, coûts et charge opérationnelle. Ils confirment, qu'à défaut de cadre commun, les entreprises construisent encore leurs propres modèles d'évaluation, selon leurs contraintes et leur niveau de maturité.

À RETENIR

35 %

des entreprises interrogées n'ont pas encore défini un rythme précis d'évaluation des risques cyber fournisseurs.

5

Les principales difficultés

Le manque de ressources et la difficulté à engager les fournisseurs demeurent les deux principaux obstacles à une gestion efficace du risque cyber tiers selon les répondants.

OBSERVATOIRE TPRM 2025
Le risque cyber lié aux fournisseurs

Interrogées sur les difficultés qu'elles ont rencontrées, les entreprises citent :

➜ **Le manque de ressources humaines et financières** (68 %), taux en léger recul par rapport à 2024 (73 %), signe que certaines ont accru leurs moyens, sans combler les besoins ;

➜ **La complexité d'engager partenaires et fournisseurs** (64 %), une contrainte particulièrement marquée pour les grands acteurs du cloud international, souvent réticents à se soumettre à des évaluations externes ;

➜ **L'incapacité de certains fournisseurs à atteindre le niveau de sécurité** demandé (52 %), en légère hausse par rapport à 2024 (48,5 %) ;

➜ La difficulté d'embarquer les métiers (43 %) ;

➜ Le passage à l'échelle (41 %) ;

➜ L'absence de mutualisation des audits ou de plateforme commune d'évaluation (31 %).

Ces limites traduisent une tension récurrente entre l'ambition de maîtrise du risque et la capacité opérationnelle à le gérer au quotidien.

Pour **neuf entreprises sur dix, le contrat demeure l'outil principal de pilotage du risque fournisseurs**. Les clauses de sécurité constituent le premier levier de responsabilisation des partenaires. Mais d'autres pratiques se développent en parallèle :

➜ 55 % des entreprises exigent des certifications à leurs fournisseurs ;

➜ 43 % organisent un suivi périodique et ont créé un comité de pilotage ;

➜ 40 % ont mis en place un plan d'action partagé ;

➜ 25 % mettent à disposition la notation cyber réalisée ;

➜ 15 % recourent à des actions de sensibilisation et de partage des bonnes pratiques.

À noter que **37 % des entreprises prévoient de mettre en place des vérifications sur le suivi des partenaires de leurs partenaires**, illustrant une volonté de mieux maîtriser les chaînes d'interdépendance.

Ces données montrent que la contractualisation reste la pierre angulaire de la relation de confiance clients-fournisseurs. Mais la diversité des exigences et des interprétations limite encore la comparabilité et la reconnaissance mutuelle des démarches. Comme le souligne le RSSI d'un grand groupe de services énergétiques : « *La certification ISO 27001, bien qu'elle constitue un cadre reconnu, présente parfois des interprétations variables et ne garantit pas toujours un niveau homogène de sécurité. Une certification basée sur des critères clairs, précis et audités de manière rigoureuse offrirait une fiabilité bien supérieure.* »

Cela rejoint une tendance émergente : la recherche de référentiels partagés, pour fluidifier les évaluations et renforcer la confiance dans les chaînes d'approvisionnement numériques.

6

Vers une approche collective du risque cyber fournisseurs

La majorité des entreprises souhaitent alléger la charge d'évaluation, en s'appuyant sur des démarches communes fondées sur la confiance, la standardisation et la reconnaissance mutuelle des certifications.

OBSERVATOIRE TPRM 2025
Le risque cyber lié aux fournisseurs

Pour rendre l'appréciation du risque cyber fournisseurs plus pertinente et plus efficace, les entreprises ouvrent une piste de réflexion nouvelle : **la mutualisation. 80 % d'entre elles seraient prêtes à mutualiser l'évaluation des fournisseurs.**

Trois conditions dominantes structurent le consensus :
1. **Un référentiel reconnu et transparent**, garantissant la qualité et la comparabilité des évaluations ;
2. **Une mutualisation limitée à un périmètre homogène** (secteur, taille, niveau de maturité) ;
3. **Un cadre de confiance institutionnel, reposant sur des acteurs légitimes :** la majorité des entreprises favorables à la mutualisation posent la condition qu'elle soit réalisée par une société du même secteur (55 %), un membre du CESIN (45 %), une entreprise de taille équivalente (29 %) ou tout autre label (22 %).

Les aspects méthodologiques apparaissent comme des prérequis implicites, mais moins souvent exprimés. C'est la preuve que la priorité des RSSI est d'abord la fiabilité et la légitimité de la source.

Cette tendance à la mutualisation se confirme : 85 % des répondants se disent prêts à adapter la profondeur des contrôles selon la criticité du fournisseur, tandis que 77 % privilégient l'appui sur des certifications reconnues (ISO, SOC 2) pour éviter l'envoi systématique de questionnaires de sécurité.

Les témoignages recueillis traduisent **une volonté partagée de rationaliser les pratiques, tout en préservant un niveau d'exigence élevé** : *« Oui à la mutualisation de l'évaluation de fournisseurs, par une société du même secteur ou une entreprise de taille équivalente »,* estime le RSSI d'un grand groupe de services énergétiques. *« À condition de garantir un niveau d'exigence homogène et une transparence totale sur la méthodologie utilisée. Il est essentiel de valider en amont le cadre d'évaluation, les critères appliqués et le processus de décision, afin d'assurer la fiabilité et la comparabilité des résultats. »*

De son côté, le RSSI d'un grand groupe du BTP s'affirme favorable à la mutualisation *« notamment au niveau de la collecte des éléments de preuves. Cependant, cela n'est applicable qu'à la condition d'une revue locale en interne par l'équipe cyber. Nous n'avons pas tous la même sensibilité ni les mêmes exigences et le contexte de notre entreprise est important dans l'évaluation. »*

En filigrane, cette recherche de convergence esquisse les contours d'un écosystème de confiance interentreprises, où la mesure du risque cyber s'appuie sur des standards partagés et des évaluations réutilisables. Ce mouvement, déjà amorcé en France au sein du CESIN, s'inscrit dans une perspective plus large : celle d'une mutualisation européenne du risque fournisseurs, fondée sur la transparence, la comparabilité et la confiance.

7

Et s'il existait une baguette magique ?

L'Observatoire a demandé aux répondants de suggérer des actions ou des outils qui faciliteraient radicalement la gestion du risque fournisseurs, comme s'ils disposaient d'une baguette magique.

OBSERVATOIRE TPRM 2025
Le risque cyber lié aux fournisseurs

Les réponses font émerger un diagnostic partagé : la gestion du risque fournisseurs reste un processus chronophage, manuel et fragmenté, trop dépendant de la réactivité et de la bonne volonté des tiers. Mais derrière cette frustration se dessine une aspiration claire : celle d'un modèle plus collectif, plus automatisé et plus responsabilisant.

Le premier souhait, exprimé par près de la moitié des répondants, concerne l'implication accrue des fournisseurs eux-mêmes. Beaucoup regrettent le manque de réactivité, la qualité inégale des réponses et une faible appropriation des enjeux de sécurité par les prestataires.

Vient ensuite **une forte demande d'automatisation et d'outillage** : plateformes mutualisées, notation cyber… Les RSSI aspirent à des processus plus fluides, capables de suivre l'évolution des risques en continu plutôt que par campagnes annuelles. Cette réponse est fortement corrélée à la demande d'une augmentation de moyens humains et financiers.

De nombreux répondants appellent également à des approches standardisées et certifiantes fondées sur des labels tels qu'ISO 27001 ou SOC 2, ainsi que sur des modèles de mutualisation permettant de partager les évaluations entre pairs, notamment au sein de communautés comme le CESIN.

Ces pistes convergent vers un écosystème de confiance ouvert : des contrôles plus précis, réutilisables et une transparence qui ne crée pas de barrières à l'entrée ni ne freine l'innovation. Elles révèlent aussi une maturité croissante dans la vision du risque tiers : les entreprises ne remettent plus en cause la nécessité de l'évaluer, mais veulent désormais **l'industrialiser, le simplifier et l'inscrire dans une logique collective**.

Ce mouvement annonce une transformation profonde de la gouvernance cyber : la confiance ne se décrète plus, elle se mesure, se partage et s'alimente en continu.

LE MOT CLÉ

Confiance

Toutes les pistes convergent vers un écosystème de confiance ouvert : des contrôles plus précis, réutilisables, et une transparence qui ne crée pas de barrières à l'entrée, ni ne freine l'innovation.

Verbatims

« Il faut créer une cartographie dynamique de l'écosystème fournisseurs, un inventaire en temps réel de tous les prestataires, partenaires, fournisseurs, sous-traitants avec leurs connexions aux systèmes critiques et leur exposition réelle, notamment pour adresser le risque Shadow IT. Ainsi que des clauses contractuelles standardisées non négociables telles que le droit d'audit.

Le RSSI d'un grand **groupe du BTP**

« Je créerais un système unique où toutes les sociétés sont auditées et les résultats disponibles sur demande, pour avoir un seul questionnaire/audit par an. »

Le RSSI d'une **ETI de l'industrie manufacturière**

« Je rêve de questionnaires complétés automatiquement, sans interprétations ni reformulations pour embellir les réponses. »

Le RSSI d'une **ETI de services informatiques**

« Cela fait dix ans que la communauté RSSI perd une bonne partie de sa capacité à remplir ou à faire remplir des questionnaires qui ne servent à rien, sauf à se donner bonne conscience. Trop peu d'acteurs ont la capacité de réaliser des contrôles sur place ou sur pièces. Pour l'écrasante majorité des autres, la mutualisation est la seule alternative. À condition de faire preuve de pragmatisme et d'ouverture d'esprit : qui sont mes fournisseurs vraiment importants, quelles sont les mesures critiques que je souhaite qu'ils mettent en œuvre, comment puis-je contrôler cette mise en œuvre de façon probante ? Stop au bullshit… »

Le RSSI d'un grand **groupe agroalimentaire**

OBSERVATOIRE TPRM 2025
Le risque cyber lié aux fournisseurs

Disposer d'un « Cyberscore » (comme le Nutriscore) de toutes les entreprises ayant des activités en Europe, basé sur un référentiel d'évaluation unique et une plateforme pour connaître le niveau des entreprises.

Le RSSI d'une **ETI de services énergétiques**

« Je créerais une norme universelle de confiance (NUC), à laquelle tous les fournisseurs devraient se conformer avant de pouvoir établir un partenariat ? Cette norme ne se limiterait pas à des certifications complexes et couteuses. Elle reposerait sur une évaluation en continu et en temps réel de la posture de sécurité de chaque fournisseur. Ma baguette magique permettrait de visualiser un tableau de bord unique montrant le niveau de risque de tous les partenaires en un clin d'œil. Ce tableau de bord intègrerait des données dynamiques sur les vulnérabilités, les incidents récents et la conformité aux meilleures pratiques garantissant une transparence totale et immédiate. »

Le RSSI d'une **PME de services informatiques**

Mettre en œuvre un organisme de confiance qui valide la conformité des tiers, afin d'éviter de se référer aux partenaires/fournisseurs à chaque fois. Une autorité de référence sous contrôle serait une bonne façon de construire de la confiance, en plus des certifications, qui ne sont pas non plus ultra fiables.

Le directeur cybersécurité et conformité d'un grand **groupe de services informatiques**

Ils ont répondu à l'enquête

(liste non exhaustive)

OBSERVATOIRE TPRM 2025
Le risque cyber lié aux fournisseurs

CESIN

CESIN.FR

À PROPOS DU CESIN

Le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) est une association loi 1901, créée en juillet 2012, avec des objectifs de professionnalisation et de promotion de la cybersécurité. Lieu d'échanges, de partage de connaissances et d'expériences, le CESIN permet la coopération entre experts de la sécurité de l'information et du numérique, ainsi qu'entre ces experts et les pouvoirs publics. Il participe à des démarches nationales et est force de proposition sur des textes réglementaires, guides et autres référentiels. Le CESIN compte parmi ses membres plusieurs organismes et institutions, comme l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), Gendarmerie Nationale, Commandement Cyber, Commission Nationale de l'Informatique et des Libertés (CNIL), Gimelec, Préfecture de Police, Police Judiciaire, Cybermalveillance.gouv.fr, ministère de la Justice, ministère de l'Intérieur. Le CESIN compte plus de 1 200 membres issus de tous secteurs d'activité, industries, ministères et entreprises, dont CAC40 et SBF120.

board of cyber

BOARDOFCYBER.IO

À PROPOS DE BOARD OF CYBER

Scale-up française fondée en 2022, Board of Cyber est spécialisée dans la gestion du risque cyber. Ses solutions SaaS totalement automatisées permettent à ses clients d'évaluer, piloter et améliorer en continu la performance cyber de leur organisation et de leur écosystème. Avec ses 40 collaborateurs, Board of Cyber accompagne plus de 500 clients. Sa mission est de contribuer à créer autour des organisations un écosystème de confiance.

boardofcyber.io

contact@boardofcyber.io

7, avenue de la Cristallerie, 92310 Sèvres

Contact Presse :
pierre-edouard.builly@lesroismages.fr

cesin.fr

contact@cesin.fr

115, rue Saint-Dominique, 75007 Paris

Contact Presse :
vloquet@alx-communication.com