

Septembre 2026

Risque Cyber Fournisseurs : Comment disposer de parcours d'évaluation complets ?

Découvrez les 3 niveaux d'évaluation cyber de vos fournisseurs et testez votre maturité avec les 8 questions essentielles.



SOMMAIRE

5 *AVANT PROPOS*

6 *INTRODUCTION*

Le fournisseur, nouveau maillon faible du risque cyber

- 6 Une menace systémique en forte croissance
- 7 Les angles d'exposition des tiers
- 8 Le défi des équipes : évaluer à grande échelle

9 *PARTIE 1*

Le cadre réglementaire : ce que la loi impose désormais

- 9 NIS2 : l'obligation de surveiller ses tiers
- 10 DORA : la résilience opérationnelle dans le secteur financier
- 10 ISO 27001 : le référentiel de maturité de référence
- 11 Synthèse des exigences réglementaires
- 12 Ce que cela change pour les équipes RSSI et les Directions Achats



13 **PARTIE 2**

Cartographier pour prioriser : les fondations du programme

- 13 Tous les fournisseurs ne se valent pas
- 15 Construire sa matrice de criticité
- 15 Les questions à se poser avant d'évaluer
- 15 Segmenter son panel : une étape souvent négligée

16 **PARTIE 3**

Les 3 niveaux d'évaluation du risque cyber fournisseur

- 17 Niveau 1 : Questionnaires et collecte documentaire
- 20 Niveau 2 : Score de risque cyber basé sur l'analyse de surface (Board of Cyber)

PAROLE D'EXPERT

- 23 Board of Cyber : Une vision concrète et continue du risque cyber, de l'entreprise à son écosystème

- 28 Niveau 3 : Analyse humaine et service managé (Galink)

PAROLE D'EXPERT

- 30 Galink : L'évaluation cyber de vos fournisseurs, opérée par des experts, lisible par vos équipes achats



40 PARTIE 4

Aprovall Manager : la plateforme qui orchestre les 3 niveaux

40 Le problème de l'éclatement des outils

41 Aprovall Manager, la plateforme unique de TPRM

42 Les bénéfices concrets

43 Témoignage client (CISO, Groupe Énergie & Services)

44 PARTIE 5

Mettre en œuvre : guide de démarrage en 5 étapes

44 Étapes 1–3 : Cartographier, Qualifier, Scorer

45 Étapes 4–5 : Auditer, Piloter

46 CONCLUSION

De la conformité subie à la maîtrise du risque

47 ANNEXES

47 Glossaire

48 Tableau récapitulatif des 3 niveaux

48 Checklist : Suis-je prêt à lancer mon programme ?



AVANT-PROPOS

La cybersécurité ne s'arrête plus aux frontières de l'entreprise. Avec la généralisation de l'externalisation, de l'interconnexion des systèmes et du recours massif aux prestataires, la surface d'exposition d'une organisation dépasse largement son périmètre direct. Un fournisseur mal sécurisé suffit aujourd'hui à ouvrir une brèche dans les systèmes les plus robustes.

Face à cette réalité, évaluer le risque cyber de ses fournisseurs est devenu un impératif stratégique, autant qu'une obligation réglementaire croissante. NIS2, DORA, ISO 27001 : les cadres normatifs convergent vers une même exigence : démontrer que les risques liés aux tiers sont identifiés, mesurés et gérés.

Pourtant, de nombreuses organisations continuent de s'appuyer sur des approches parcellaires : un questionnaire envoyé une fois par an, des documents collectés sans centralisation, des scores de risque non actualisés. L'enjeu n'est plus de simplement cocher des cases, mais de construire un véritable parcours d'évaluation, structuré, continu et actionnable.

Ce livre blanc propose une grille de lecture en **trois niveaux complémentaires : de la collecte documentaire à l'analyse de surface automatisée, jusqu'à l'expertise humaine pour les fournisseurs les plus critiques**. Il s'adresse aux RSSI, aux équipes Achats et à toute organisation souhaitant professionnaliser sa gestion des risques cyber tiers. Ces trois niveaux sont soutenus par le **partenaire stratégique Board of Cyber** et par **Galink**.

INTRODUCTION

Le fournisseur, nouveau maillon faible du risque cyber.

Une menace systémique en forte croissance

Les attaques par rebond, où un acteur malveillant exploite la relation de confiance entre une organisation et ses prestataires, représentent désormais l'un des vecteurs d'intrusion les plus utilisés. En compromettant un fournisseur disposant d'accès privilégiés ou de connexions directes aux systèmes d'information de ses clients, les attaquants contournent les défenses périmétriques traditionnelles.

Les exemples se multiplient dans tous les secteurs : compromission d'un prestataire de maintenance industrielle pour atteindre une infrastructure critique, exfiltration de données via un sous-traitant logistique, ransomware propagé depuis un outil de gestion partagé. Le fournisseur est devenu une cible en lui-même, précisément parce qu'il est un point d'entrée vers des systèmes plus importants.

Entre **50%** et **60%**

des PME victimes d'une cyberattaque finissent par fermer dans les 18 mois suivant l'incident.
(Orange Cyberdefense)

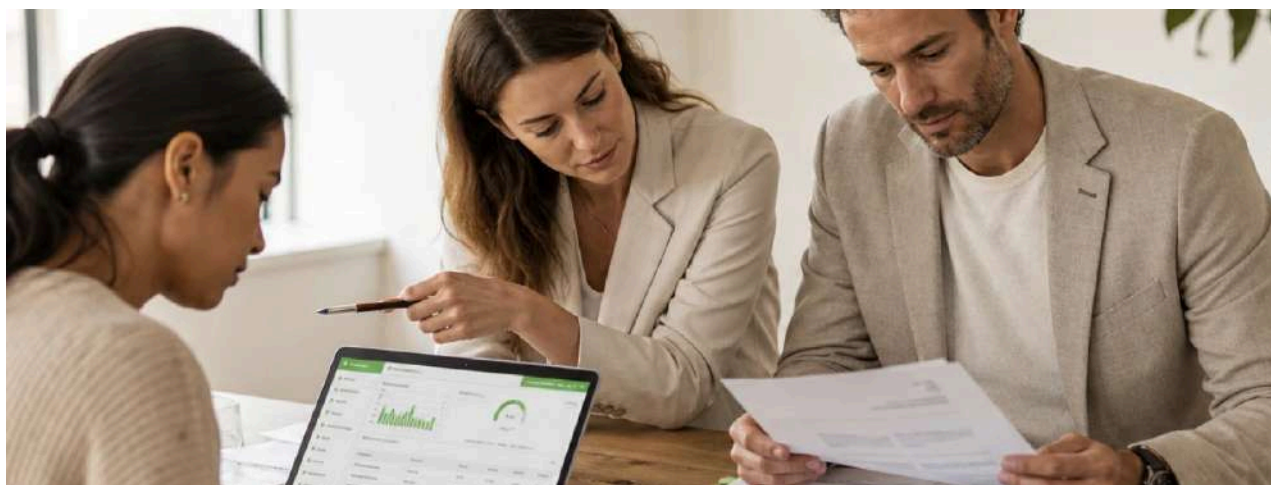


Les angles d'exposition des tiers

Le risque cyber lié aux fournisseurs se manifeste sous plusieurs formes, souvent cumulatives :

- ✓ **Accès directs aux systèmes d'information** : VPN, accès distants, interconnexions applicatives
- ✓ **Données partagées** : documents contractuels, bases de données clients, informations financières
- ✓ **Dépendances opérationnelles** : fournisseurs dont l'interruption entraîne un arrêt de production
- ✓ **Mauvaises configurations visibles de l'extérieur** : serveurs exposés, certificats expirés, vulnérabilités non patchées

Chacun de ces angles requiert une méthode d'évaluation adaptée. C'est précisément ce que proposent les trois niveaux d'évaluation présentés dans ce livre blanc.



Le défi des équipes : évaluer à grande échelle

La majorité des grandes entreprises et ETI travaillent avec des dizaines, voire des centaines de fournisseurs actifs. Évaluer chacun d'entre eux avec la même rigueur est impossible sans une approche structurée. Le premier enjeu est donc la priorisation : **tous les fournisseurs ne présentent pas le même niveau de risque, et toutes les évaluations ne justifient pas le même investissement.**

Le second enjeu est la continuité : une évaluation réalisée une fois par an ne reflète pas la réalité d'un risque cyber qui évolue quotidiennement. La posture de sécurité d'un fournisseur peut se dégrader en quelques jours suite à une vulnérabilité non corrigée ou à un incident non déclaré.

Ce document propose un cadre pour répondre à ces deux défis : segmenter pour prioriser, et combiner des méthodes complémentaires pour couvrir l'ensemble du spectre du risque.



PARTIE 1

Le cadre réglementaire : ce que la loi impose désormais

La gestion des risques tiers n'est plus seulement une bonne pratique : elle est désormais inscrite dans plusieurs cadres réglementaires contraignants. Comprendre ces exigences est le point de départ de tout programme d'évaluation sérieux.

1 | NIS2 : l'obligation de surveiller ses tiers

La directive européenne NIS2, entrée en vigueur en janvier 2023 et dont la transposition dans le droit des États membres est en cours, élargit considérablement le périmètre des organisations soumises à des obligations de cybersécurité. Elle concerne les entités essentielles et importantes dans des secteurs critiques : énergie, transport, santé, eau, infrastructure numérique, secteur public et plus encore.

L'une des évolutions majeures de NIS2 par rapport à sa version précédente est l'inclusion explicite de la gestion des risques liés à la chaîne d'approvisionnement. Les organisations concernées doivent désormais :

- Évaluer les risques cyber de leurs fournisseurs et prestataires de services
- Imposer des exigences de sécurité contractuelles à leurs tiers
- Mettre en place des mécanismes de surveillance continue
- Documenter leurs démarches d'évaluation pour pouvoir les justifier auprès des autorités compétentes

NIS2 place ainsi la responsabilité de l'organisation donneur d'ordre sur la posture de sécurité de ses fournisseurs. Un incident chez un prestataire non surveillé peut engager la responsabilité de l'entité cliente.

2 | DORA : la résilience opérationnelle dans le secteur financier

Le règlement européen DORA (Digital Operational Resilience Act), applicable depuis janvier 2025, s'adresse au secteur financier : banques, assurances, gestionnaires d'actifs, infrastructures de marché, mais aussi leurs prestataires de services TIC.

DORA introduit des exigences particulièrement strictes sur la gestion des risques liés aux tiers :

- Tenue d'un registre exhaustif des prestataires de services TIC, avec distinction des prestataires critiques
- Évaluation approfondie des risques de concentration (dépendance à un prestataire unique)
- Contractualisation renforcée incluant des clauses d'audit, de continuité et de sortie
- Tests de résilience opérationnelle intégrant les prestataires critiques

Pour les organisations financières, les niveaux 1, 2 et 3 d'évaluation décrits dans ce livre blanc correspondent précisément aux différentes couches d'exigences de DORA, selon la criticité du prestataire.

3 | ISO 27001 : le référentiel de maturité de référence

La norme ISO 27001 reste le référentiel international le plus reconnu en matière de management de la sécurité de l'information. Dans sa version 2022, elle consacre un contrôle spécifique (A.5.19 à A.5.22) à la sécurité des relations avec les fournisseurs.

Pour les organisations certifiées ou en démarche de certification, ISO 27001 implique de :

- Définir des politiques de sécurité pour les relations avec les fournisseurs
- Traiter les risques liés à l'accès des fournisseurs aux actifs informationnels
- Surveiller et réviser régulièrement les prestations des fournisseurs
- Gérer les changements chez les fournisseurs dans une logique de continuité

La certification d'un fournisseur à ISO 27001 constitue un signal positif, mais ne dispense pas d'une évaluation complémentaire : le périmètre certifié peut être limité, et la certification ne garantit pas l'absence de vulnérabilités techniques actives.

4 | Synthèse des exigences réglementaires

Réglementation	Obligation principale tiers	Niveau d'évaluation requis
NIS2	Gestion des risques liés aux prestataires essentiels	Niveaux 1 + 2 minimum
DORA	Registre des prestataires IT critiques, tests de résilience	Niveaux 1 + 2 + 3 pour les prestataires critiques
ISO 27001	Évaluation des risques tiers, annexe A.15	Niveau 1 minimum, niveau 2 recommandé

5 | Ce que cela change pour les équipes RSSI et les Directions Achats

Ces réglementations convergent vers une même exigence : passer d'une conformité déclarative à une conformité vérifiable et documentée.

Le RSSI n'est plus seulement garant de la sécurité interne : il devient responsable de la posture cyber de l'ensemble de l'écosystème tiers.

Cette évolution implique une collaboration renforcée avec les équipes Achats, qui restent en première ligne dans la relation contractuelle avec les fournisseurs. Intégrer les critères cyber dans les processus d'achat, dès la qualification d'un fournisseur, lors des renouvellements, à chaque évolution de périmètre, est devenu une nécessité opérationnelle autant que réglementaire.



PARTIE 2

Cartographier pour prioriser : les fondations du programme

Avant de déployer des méthodes d'évaluation, toute organisation doit disposer d'une vision claire de son panel fournisseurs. Sans cartographie, il est impossible de prioriser les efforts et d'allouer les ressources au bon endroit.

1 | Tous les fournisseurs ne se valent pas

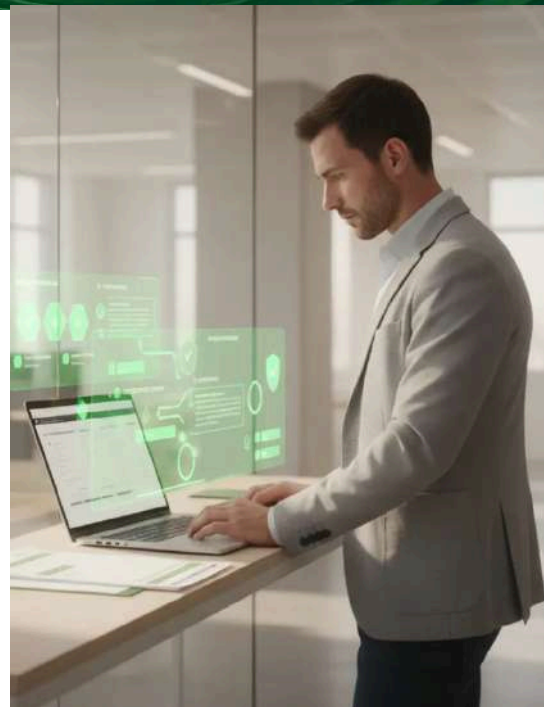
Le risque inhérent d'un fournisseur dépend de plusieurs facteurs combinés :

- Le type d'accès accordé : accès distant au SI, connexion VPN, accès à des données sensibles, hébergement d'applications critiques
- La nature des données échangées : données personnelles, données financières, propriété intellectuelle, données de production
- Le niveau de dépendance opérationnelle : quelle est la conséquence d'une interruption de ce fournisseur sur l'activité ?
- Le secteur d'activité du fournisseur : certains secteurs présentent des risques de compromission plus élevés

La combinaison de ces critères permet de positionner chaque fournisseur sur une échelle de criticité allant de faible (fournisseur sans accès SI et sans données sensibles) à critique (prestataire IT avec accès direct aux systèmes de production).

2 | Construire sa matrice de criticité

Une matrice de criticité fournisseurs croise deux axes : l'impact potentiel d'un incident chez ce fournisseur (sur les données, les opérations, la réputation) et le niveau d'exposition actuel (accès accordés, données partagées, intégrations en place).



Cette matrice permet d'identifier quatre segments :

- **Fournisseurs critiques** : impact élevé + exposition élevée → priorité d'évaluation maximale, niveaux 1 + 2 + 3
- **Fournisseurs à surveiller** : impact élevé + exposition limitée → niveaux 1 + 2, réévaluation régulière
- **Fournisseurs à qualifier** : impact limité + exposition élevée → niveau 1 + score de surface ponctuel
- **Fournisseurs standard** : impact limité + exposition limitée → niveau 1 simplifié



3 | Les questions à se poser avant d'évaluer

Avant de lancer un programme d'évaluation, trois questions structurantes méritent d'être traitées :

- 1 Quels fournisseurs ont accès à mes systèmes ou à mes données sensibles ? Cette liste doit être tenue à jour, car les accès évoluent constamment.
- 2 Quelles réglementations s'appliquent à mon secteur et à mon périmètre ? NIS2, DORA, ISO 27001 n'imposent pas les mêmes niveaux d'exigence ni les mêmes délais.
- 3 Quelle profondeur d'analyse pour quel segment de fournisseurs ? La réponse conditionne directement le choix des méthodes d'évaluation et le budget à mobiliser.

4 | Segmenter son panel : une étape souvent négligée

La segmentation du panel fournisseurs est souvent traitée comme une formalité administrative alors qu'elle constitue le socle de tout programme TPRM efficace. Sans segmentation, les ressources d'évaluation sont dispersées uniformément sur l'ensemble du panel, au détriment des fournisseurs qui méritent le plus d'attention.

Une segmentation efficace repose sur des critères objectifs : **type de prestation, niveau d'accès, données traitées**, et doit être revue à chaque évolution significative du périmètre : nouvelle prestation, extension des accès, changement de prestataire.

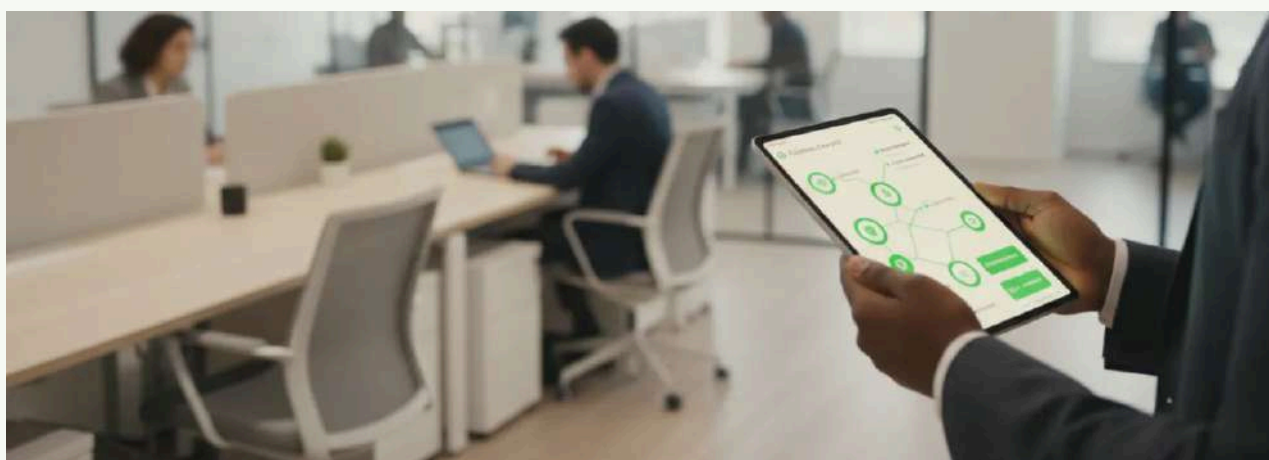
PARTIE 3

Les 3 niveaux d'évaluation du risque cyber fournisseur.

L'évaluation du risque cyber fournisseur ne peut pas se réduire à une seule méthode. Chaque approche a ses forces et ses limites. La robustesse d'un programme TPRM repose sur la combinaison de trois niveaux complémentaires, déployés selon la criticité des fournisseurs concernés.

Ces trois niveaux fonctionnent comme un entonnoir : large et systématique au niveau 1, ciblé et objectif au niveau 2, approfondi et contextuel au niveau 3.

Niveau	Approche	Couverture	Profondeur	Idéal pour
1	Questionnaires & documents	Large	Déclarative	Tout le panel
2	Score de surface (Board of Cyber)	Ciblée	Technique / objective	Fournisseurs à risque modéré à élevé
3	Analyse humaine managée (Galink)	Restreinte	Experte / contextuelle	Fournisseurs critiques



1 | Niveau 1 : Questionnaires et collecte documentaire

Le principe

Le niveau 1 est le point d'entrée universel de tout programme d'évaluation cyber fournisseurs. Il repose sur une évaluation déclarative structurée : l'organisation adresse à ses fournisseurs des questionnaires portant sur leurs pratiques de sécurité, et collecte des documents justificatifs attestant de leur niveau de conformité.

Ce que l'on évalue

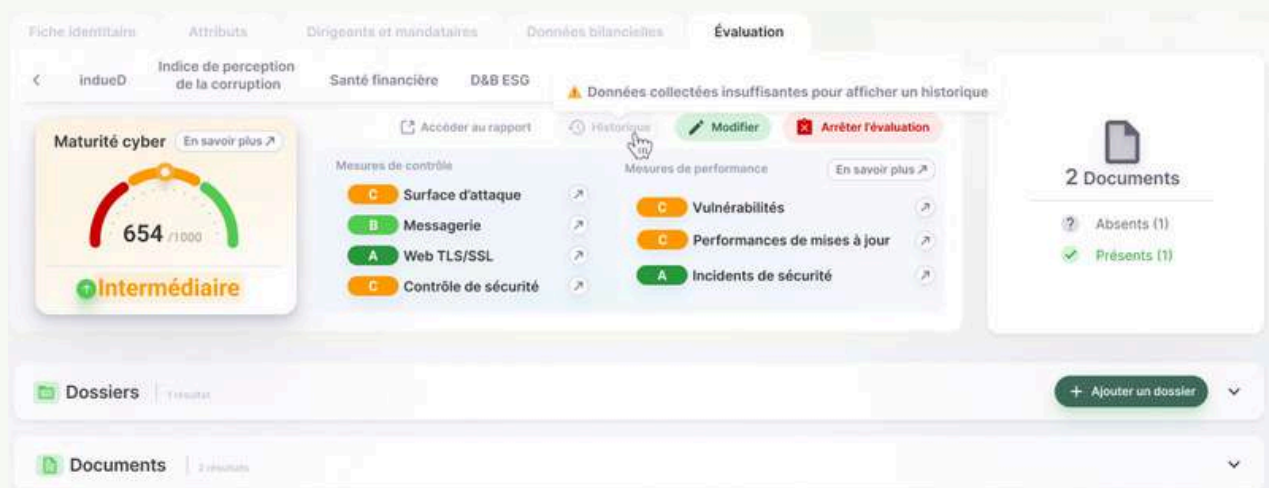
Les questionnaires de niveau 1 couvrent généralement les domaines suivants :

- ✓ **Gouvernance de la sécurité** : existence d'une politique de sécurité, désignation d'un responsable SSI, sensibilisation des équipes
- ✓ **Gestion des accès** : contrôle des accès logiques, gestion des identités et des droits, politique de mots de passe
- ✓ **Sécurité des infrastructures** : gestion des correctifs, protection des postes de travail, sécurité des réseaux
- ✓ **Gestion des incidents** : existence d'un plan de réponse, délais de notification, retours d'expérience
- ✓ **Continuité et résilience** : plans de continuité d'activité, sauvegardes, tests de reprise

La collecte documentaire complète ces questionnaires : certifications en cours de validité (ISO 27001, SOC 2, HDS...), rapports d'audit récents, attestations de conformité réglementaire.

Les référentiels mobilisables

Plusieurs référentiels peuvent servir de base à la construction des questionnaires de niveau 1 : le NIST Cybersecurity Framework, les CIS Controls, le questionnaire VSA du BSIMM, ou des questionnaires sectoriels spécifiques (SWIFT, PCI DSS...). AprovaLL propose des questionnaires préconfigurés alignés sur ces référentiels, adaptables aux exigences propres de chaque organisation.



Analyse intelligente des documents et des preuves

L'IA analyse automatiquement les documents et justificatifs collectés auprès des tiers. Elle contrôle les pièces, identifie les informations pertinentes et peut déclencher leur validation, leur invalidation ou leur intégration dans les processus d'évaluation AprovaLL. Cette automatisation fiabilise le contrôle des preuves tout en réduisant les traitements manuels.

Un questionnaire standard fondé sur l'ISO 27001

Le questionnaire Cyber Risque standard d'AprovaLL s'appuie sur les principaux domaines de contrôle de l'ISO 27001 et couvre les dimensions essentielles du risque cyber. Dynamique, il adapte les questions à la typologie du tiers et à ses réponses précédentes. Le standard peut également être personnalisé afin d'affiner l'évaluation et de générer les indicateurs de risque cyber propres à chaque organisation.

Des campagnes Cyber Risque pilotées par la cartographie des risques

Les campagnes d'évaluation sont déclenchées en fonction de la cartographie des risques et du niveau d'exposition de chaque tiers. Cette approche permet d'adapter la profondeur des contrôles, les questionnaires et les preuves demandées aux enjeux réellement identifiés, afin de concentrer les efforts sur les tiers les plus critiques.

Des plans d'actions pour piloter la remédiation

Lorsqu'un risque, une non-conformité ou une faiblesse est identifié, Aprovall permet de mettre en place des plans d'actions adaptés. Les mesures correctives peuvent être attribuées, suivies et documentées afin de piloter la remédiation et de mesurer dans le temps l'amélioration du niveau de maîtrise du risque cyber.

Des données de référence sur les certifications ISO 27001

Aprovall enrichit l'évaluation grâce à des sources de données permettant d'identifier et de contrôler les certifications ISO 27001 des tiers. Ces informations externes viennent compléter les questionnaires et les preuves collectées pour renforcer la fiabilité de l'évaluation cyber.

Aprovall en pratique

Aprovall automatise l'envoi des questionnaires, les relances et la collecte des documents justificatifs via Aprovall Portal. Les fournisseurs accèdent gratuitement au portail pour répondre aux demandes. L'ensemble des réponses et documents est centralisé, tracé et mis à disposition des équipes Achats et Cybersécurité pour une prise de décision rapide.

2 | Niveau 2 : Score de risque cyber basé sur l'analyse de surface (Board of Cyber)

Le principe

Le niveau 2 introduit une approche radicalement différente : objective, non intrusive et continue. Plutôt que de demander au fournisseur de déclarer sa posture de sécurité, on l'observe directement depuis l'extérieur, en analysant les signaux visibles sur Internet sans aucun accès aux systèmes internes.

Cette technique, appelée analyse de la surface d'attaque externe (ou EASM, External Attack Surface Management), permet d'évaluer en temps réel ce qu'un attaquant pourrait découvrir et exploiter depuis l'extérieur.



Ce que l'on mesure

L'analyse de surface couvre plusieurs dimensions techniques :

- ✓ **Surface d'attaque** : inventaire des actifs exposés sur Internet, ports ouverts, services accessibles
- ✓ **Messagerie** : configuration des serveurs mail, protection anti-phishing (SPF, DKIM, DMARC)
- ✓ **Web et TLS/SSL** : qualité des certificats, protocoles supportés, configuration HTTPS
- ✓ **Contrôle de sécurité** : présence d'une politique de divulgation des vulnérabilités, en-têtes HTTP de sécurité
- ✓ **Vulnérabilités connues** : corrélation avec les bases de données CVE pour identifier des versions logicielles vulnérables exposées
- ✓ **Incidents de sécurité** : présence dans des bases de données de compromissions ou de fuites de données

La logique du score dynamique

Ces données sont agrégées en un score de risque mis à jour quotidiennement. Contrairement à un questionnaire qui photographie une situation à un instant T, le score de surface reflète l'état réel de l'exposition à tout moment. Une dégradation soudaine du score, suite à l'apparition d'une nouvelle vulnérabilité ou d'une configuration défaillante, déclenche une alerte permettant d'agir avant qu'un incident ne survienne.

Board of Cyber, partenaire stratégique d'Aprovall, est un acteur français spécialisé dans cette approche. Son moteur d'analyse permet d'obtenir un score structuré et actionnable pour l'ensemble du panel fournisseurs, indépendamment de toute déclaration du fournisseur lui-même.

Comment utiliser le score pour prioriser ?

Le score de surface est particulièrement utile pour qualifier rapidement un grand nombre de fournisseurs et identifier ceux qui méritent une investigation approfondie (niveau 3). Un fournisseur affichant un score dégradé malgré un questionnaire favorable est un signal d'alerte à traiter en priorité.

Les limites du niveau 2

L'analyse de surface ne couvre que ce qui est visible de l'extérieur. Elle ne renseigne pas sur les pratiques internes, la gouvernance de la sécurité, la gestion des accès humains, ou les risques liés aux comportements des équipes. Un fournisseur peut présenter une surface externe bien configurée tout en ayant des pratiques internes défaillantes. C'est pourquoi le niveau 2 se combine toujours avec le niveau 1 et, pour les fournisseurs critiques, avec le niveau 3.





PAROLE D'EXPERT

Une vision concrète et continue du risque cyber, de l'entreprise à son écosystème



Évaluer des centaines de fournisseurs, sans questionnaires

Chaque organisation est à la fois cliente de ses fournisseurs et fournisseur de ses propres clients. Les mêmes exigences circulent donc dans les deux sens, et les mêmes preuves sont redemandées en boucle.

L'évaluation des tiers doit évoluer : passer d'un modèle lourd, discontinu et fondé sur des sollicitations répétées à une approche mutualisée, automatisée et continue.

Les fournisseurs, prestataires, partenaires et filiales exposent l'entreprise à un risque cyber. Dans un contexte de menaces accrues et d'exigences réglementaires renforcées, notamment avec NIS2 et DORA, évaluer un écosystème de centaines ou milliers de tiers par questionnaires, relances et analyses manuelles n'est plus envisageable.

La nouvelle solution TPCRM de Board of Cyber permet d'évaluer l'ensemble du portefeuille de tiers de manière automatisée, continue et homogène, sans campagnes de questionnaires. Elle associe deux approches complémentaires :



Un score fondé sur l'analyse documentaire

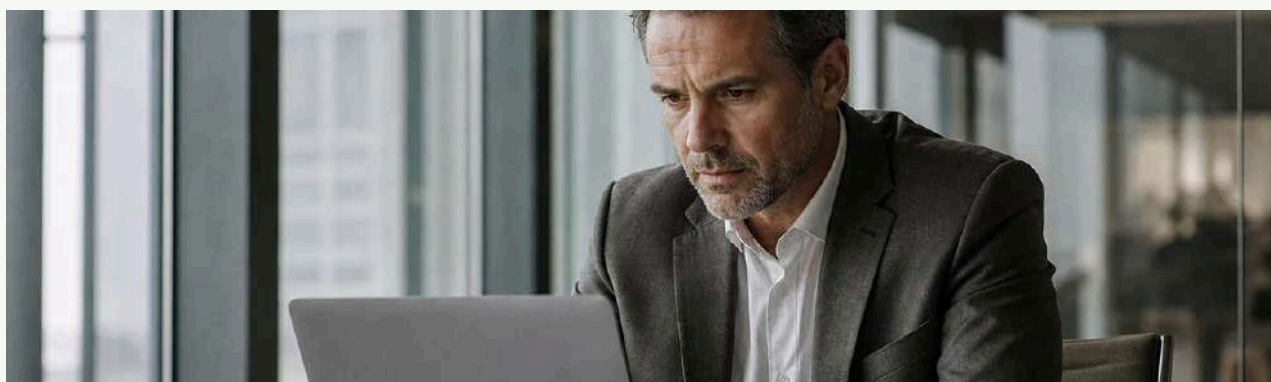
calculé automatiquement par IA à partir des documents et preuves de sécurité fournis par chaque tiers (politiques de sécurité, rapports d'audit, plans d'assurance sécurité, attestations, etc.) au regard d'un référentiel de plus de 300 points de contrôle.



Security Rating

qui complète cette évaluation par une analyse continue de la surface d'exposition externe de chaque fournisseur, afin d'identifier les signaux de risque et les évolutions de sa posture cyber.

Ce référentiel partagé entre organisations s'enrichit progressivement des preuves déposées par les acteurs eux-mêmes. Cet écosystème permet d'évaluer plus largement au-delà de ses fournisseurs critiques, en profitant des évaluations déjà demandées par d'autres pour un maximum de vélocité.



Cette approche étend la visibilité au-delà des seuls fournisseurs critiques, tout en supprimant les démarches administratives liées aux questionnaires. Déposée une seule fois, la documentation est analysée automatiquement : chaque client en tire sa propre note selon le niveau d'exigence qu'il juge pertinent, avec l'accord du fournisseur.



Cette approche permet de :

- ✓ **Gagner du temps** : supprimer les relances, la collecte d'informations et les analyses manuelles liées aux questionnaires
- ✓ **Prouver plutôt que déclarer** : fonder l'évaluation des tiers sur des preuves documentaires
- ✓ **Appliquer le bon niveau d'exigence** : définir les exigences de cybersécurité selon la criticité du tiers, la relation et le service consommé
- ✓ **Identifier les priorités** : détecter plus rapidement les écarts, dépendances et risques de concentration
- ✓ **Faire progresser l'écosystème** : définir et suivre des plans de remédiation avec les fournisseurs afin d'élever durablement le niveau de sécurité de tous
- ✓ **Piloter et décider** : fournir aux équipes opérationnelles et aux directions une vision consolidée des risques

Compléter l'analyse documentaire par la vision externe

Le **Security Rating** apporte une lecture continue et non intrusive de la surface d'attaque externe, sans agent ni déploiement. Appliqué aux tiers comme à l'entreprise elle-même, il aide à identifier les actifs exposés, les signaux de risque et les écarts à analyser.



Il permet notamment de :

- ✓ Obtenir rapidement une vision de l'exposition externe d'un fournisseur
- ✓ Détecter les tiers nécessitant une attention prioritaire
- ✓ Suivre l'évolution de leur posture cyber dans le temps
- ✓ Mesurer l'effet des actions de remédiation
- ✓ Fournir au Comex des indicateurs clairs pour mieux appréhender les enjeux cyber et orienter les décisions

Dans le cadre de la collaboration avec Aprovall, Security Rating fournit un **premier niveau d'évaluation automatisé et non intrusif de l'exposition externe de l'ensemble des fournisseurs**. Les organisations disposent ainsi d'une vision continue des signaux de risque de leur écosystème, sans solliciter les tiers.

Gérer les exceptions et piloter les remédiations

Tous les fournisseurs ne nécessitent pas le même niveau de suivi. Un tiers critique, une exigence contractuelle particulière ou un écart identifié peut justifier une demande de preuve complémentaire, un questionnaire ciblé ou un plan d'action formalisé.

Trust HQ centralise ces situations : campagnes ciblées, échanges avec les fournisseurs, plans de remédiation, relances et traçabilité des décisions. Les équipes RSSI, GRC et achats disposent d'un espace commun pour suivre les actions correctrices et piloter les relations les plus sensibles.

L'objectif n'est pas de multiplier les contrôles, mais de concentrer les efforts sur les cas qui le nécessitent et de mettre en place un dialogue utile avec les fournisseurs.

Renforcer les environnements critiques

Board of Cyber étend cette approche aux environnements les plus sensibles de l'entreprise.

AD Rating évalue la sécurité de l'Active Directory afin d'identifier les configurations, droits et pratiques à corriger en priorité.

365 Rating analyse la posture de sécurité Microsoft 365 et met en évidence les écarts pouvant affecter les comptes, les données, la messagerie et les espaces de collaboration.

Faire du risque cyber un levier de décision

Board of Cyber transforme une gestion dispersée du risque cyber en un pilotage continu, factuel et priorisé.

AprovaLL en pratique

Board of Cyber est intégré nativement dans la plateforme AprovaLL. Le score de risque cyber est affiché directement sur la fiche de chaque fournisseur, avec un historique de l'évolution et des alertes automatiques en cas de dégradation. Les équipes disposent ainsi d'une vision objective et quotidiennement actualisée, sans aucune action manuelle.

3 | Niveau 3 : Analyse humaine et service managé (Galink)

Le principe

Le niveau 3 mobilise une expertise humaine approfondie pour les fournisseurs les plus critiques, ceux pour lesquels un incident aurait un impact majeur sur les opérations, les données ou la réputation de l'organisation. Il s'agit d'aller au-delà des données et des déclarations pour comprendre la réalité opérationnelle de la posture de sécurité d'un fournisseur.



Ce que l'on analyse

L'analyse de niveau 3 combine plusieurs approches :

- ✓ **Examen approfondi de la documentation technique et contractuelle :**
politiques de sécurité, architecture réseau, procédures de gestion des incidents, plans de continuité
- ✓ **Entretiens avec les équipes techniques et dirigeantes du fournisseur :**
compréhension de la gouvernance, des investissements en sécurité, de la culture cyber
- ✓ **Évaluation de la posture de sécurité globale :** cohérence entre les déclarations, les documents et les observations techniques
- ✓ **Identification des risques contextuels :** dépendances cachées, sous-traitants du fournisseur, risques liés aux personnes clés
- ✓ **Production d'un plan de remédiation :** recommandations hiérarchisées et suivi de leur mise en œuvre

Quand activer le niveau 3

Le niveau 3 est pertinent pour les fournisseurs présentant une combinaison de critères de criticité élevés :

- Accès directs aux systèmes d'information (VPN, API, hébergement d'applications)
- Traitement de données sensibles ou personnelles en grande quantité
- Dépendance opérationnelle forte (arrêt de la production en cas d'incident chez ce fournisseur)
- Fournisseurs soumis à des exigences DORA (prestataires de services TIC critiques)
- Fournisseurs présentant un score de surface dégradé (détecté au niveau 2)



PAROLE D'EXPERT

Galink & Aprovall : l'évaluation cyber de vos fournisseurs, opérée par des experts, lisible par vos équipes achats



Galink, expert de l'évaluation cyber des fournisseurs

Galink est le leader européen du TPCRM cyber (gestion du risque cyber fournisseur). Ses analystes opèrent depuis la France plusieurs milliers d'évaluations cyber par an, sur la base de preuves et selon les référentiels reconnus NIST et ISO 27001, continuellement mis à jour au rythme des évolutions réglementaires (DORA, NIS2, CRA, AI Act).

Cette expertise fait autorité dans l'écosystème : les experts Galink s'impliquent dans l'associatif cyber en Europe, et Galink organise le Vendor Cyber Risk Summit, le rendez-vous annuel de référence de la filière.

La confiance est au cœur de son modèle : Galink est certifié ISO 27001.

Le défi : le réglementaire impose une gestion active du risque cyber fournisseur

43%

des attaques visant les grands groupes transitent aujourd'hui par un fournisseur.

La menace, d'abord : 43 % des attaques visant les grands groupes transitent aujourd'hui par un fournisseur. Mais si le sujet est devenu incontournable, c'est aussi parce que le cadre réglementaire européen a changé de nature. Il ne s'agit plus de recommandations : trois textes majeurs imposent désormais une obligation de résultat sur la chaîne d'approvisionnement.

DORA impose aux entités financières un encadrement strict du risque lié à leurs prestataires IT : évaluation avant contractualisation, clauses obligatoires, suivi tout au long de la relation.

NIS2 étend à des milliers d'entités essentielles et importantes l'obligation de sécuriser leur chaîne d'approvisionnement, avec des sanctions substantielles et une responsabilité directe des dirigeants.

Le CRA (Cyber Resilience Act) prolonge cette logique aux produits comportant des éléments numériques, en exigeant une maîtrise de la sécurité sur l'ensemble de la chaîne de valeur.

Le point commun de ces textes : ils n'exigent pas une case cochée une fois, mais une gestion active, documentée et continue du risque cyber fournisseur, évaluer avant de contracter, tracer les preuves, suivre la remédiation, réévaluer dans le temps. En cas d'incident ou de contrôle, c'est cette documentation qui sera demandée.

Or, cette responsabilité échoit largement aux Directions Achats dont c'est devenu le deuxième risque prioritaire souvent sans les moyens adaptés :

- **Un processus chronophage** : évaluer sérieusement un seul fournisseur peut prendre jusqu'à 20 heures, dont plus de 90 % consacrées à relancer et collecter l'information plutôt qu'à analyser le risque.
- **Des équipes non équipées** : les acheteurs ne sont pas des experts cyber. Les questionnaires manuels prennent des semaines et produisent des résultats techniques, difficilement exploitables pour prendre une décision.
- **Des fournisseurs sur-sollicités** : chaque donneur d'ordre envoie son propre questionnaire, au détriment de la relation commerciale.



Quel niveau d'évaluation pour quel fournisseur ?

Toutes les évaluations cyber ne se valent pas et toutes ne sont pas nécessaires pour tous les fournisseurs. La bonne pratique consiste à adapter le niveau d'évaluation à la criticité du fournisseur. Trois niveaux se dégagent :

Criticité	Type d'évaluation	Ce que ça apporte	Ce que ça ne couvre pas
Faible	Scoring externe analyse automatique de la surface d'attaque visible (domaines, IP, vulnérabilités exposées) Questionnaire déclaratif sur les pratiques de sécurité, sans vérification	Déploiement immédiat et à grande échelle, sollicitation nulle ou minime du fournisseur, première vision de la maturité	Vision uniquement externe ou déclarative.
Modérée à Elevée	Questionnaire avec preuves Questionnaire accompagné de preuves documentaires (politiques de sécurité, rapports de pentest, certifications ISO, SOC 2...) analysées par un expert	Vision fiable de la maturité réelle, détection des non-conformités effectives, alignement NIS2, DORA, ISO 27001	Lourd à opérer sans expertise interne dédiée pour analyser les preuves
Critique	Audit sur site / Pentest / Red team pour les prestataires les plus sensibles	Niveau de garantie maximal, détection des risques non visibles autrement	Option très coûteuse, chronophage et requiert l'accord du fournisseur

Pour la grande majorité des fournisseurs à enjeu, du niveau modéré au niveau critique, le questionnaire avec preuves constitue le socle de l'évaluation : c'est le niveau exigé par les régulateurs, et le seul qui distingue les pratiques réelles des déclarations. Mais il suppose d'analyser des politiques de sécurité, des rapports de pentest, des certifications... un travail d'expert que la plupart des équipes achats ne peuvent pas absorber.

C'est précisément ce verrou que lève le partenariat entre AprovaLL et Galink.

Intégrer Galink Assessment dans le processus AprovaLL

AprovaLL et Galink ont noué un partenariat permettant de déclencher Galink Assessment, l'évaluation cyber avec preuves 100 % managée par les analystes Galink, directement depuis AprovaLL.

Lorsqu'un besoin d'évaluation cyber est identifié sur un tiers :

1

Étape 1

Vous déclenchez l'évaluation en un clic depuis AprovaLL.

2

Étape 2

Galink prend en charge l'intégralité du processus : invitation du fournisseur, relances, collecte des preuves, analyse. Un interlocuteur dédié accompagne le fournisseur de l'invitation jusqu'au rendu, sans aucun coût pour ce dernier.

3

Étape 3

Les analystes Galink évaluent la maturité cyber du fournisseur sur la base des preuves fournies, avec un double scoring selon les référentiels NIST et ISO 27001.

4

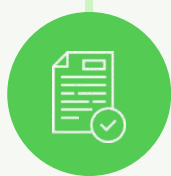
Étape 4

Vous récupérez un rapport complet, prêt à être présenté en comité.

Le délai médian observé, du lancement au livrable, est de 9 jours ouvrés. Le fournisseur reçoit quant à lui sa scorecard, qu'il peut valoriser auprès de son écosystème. Un processus conçu pour être accepté, comme en témoigne une satisfaction fournisseur moyenne de 8,8/10.

Un rapport exploitable, sans expertise cyber requise

C'est la conviction qui a guidé la conception du livrable Galink : **un résultat doit pouvoir être lu, compris et utilisé par un acheteur, un juriste ou un dirigeant, pas seulement par un RSSI.**



Chaque évaluation produit un rapport structuré qui donne, dès la première page, tout ce qu'il faut pour décider :

- ✓ **Un score global sur 100** et un niveau de maturité en clair : Insuffisant, Basic, Moderate, Advanced ou Mature.
- ✓ **Un commentaire d'analyste rédigé** : une synthèse en langage courant des points forts et des signaux d'alerte, qui donne le contexte derrière le chiffre.
- ✓ **Une décomposition par domaine de sécurité** (protection des données, continuité d'activité, gestion des tiers...), selon les référentiels NIST et ISO 27001.
- ✓ **Un plan de remédiation priorisé**, directement actionnable avec le fournisseur.

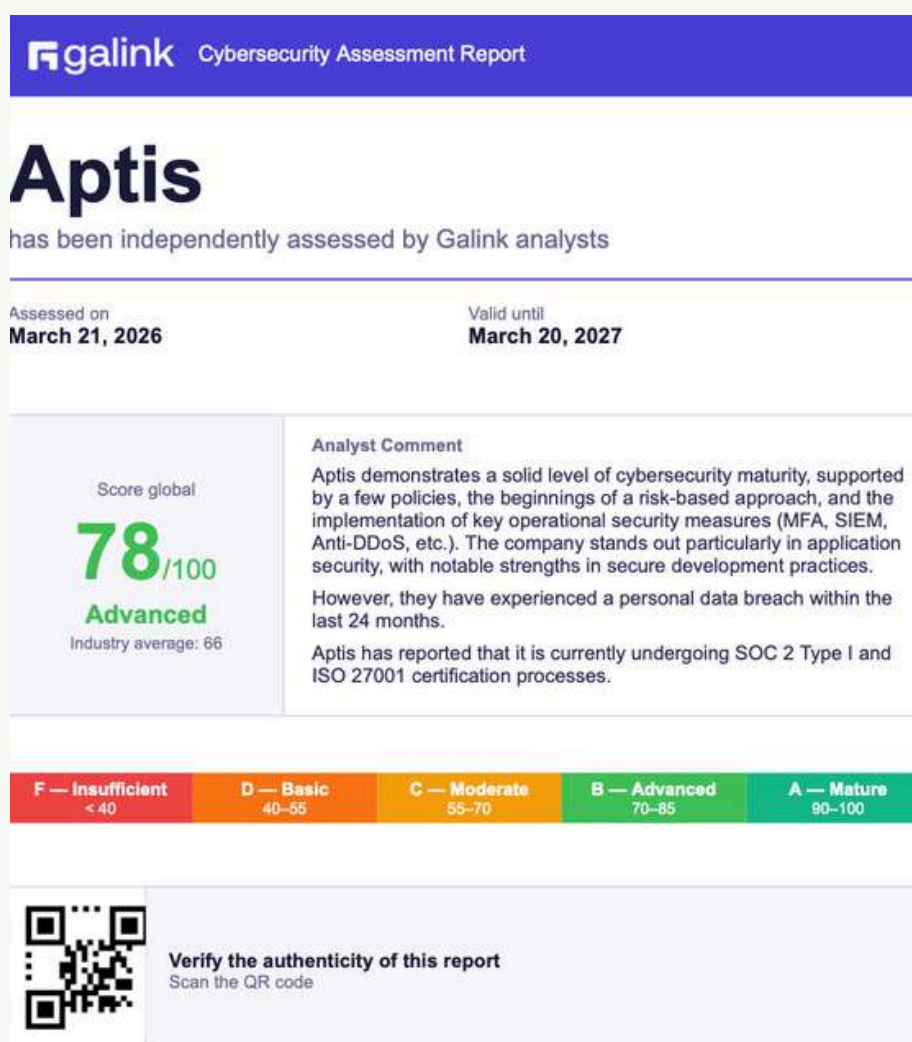
Le mode d'action est tout aussi simple : il suffit de définir un score minimum par niveau de criticité, et le tri se fait en un coup d'œil. Par exemple :

Fournisseur critique : score minimum requis de **80/100**

Fournisseur non critique : score minimum requis de **60/100**

Au-dessus du seuil, le fournisseur est validé ; en dessous, le plan de remédiation fourni avec le rapport sert de base d'échange pour corriger les points bloquants. Pas de grille d'analyse complexe, pas d'arbitrage technique : une règle simple, applicable par n'importe quel acheteur.

En cas d'audit ou de contrôle réglementaire (DORA, NIS2), le rapport constitue par ailleurs une preuve formalisée, tracée et auditable : questionnaire structuré, preuves collectées, scoring référencé.



Exemple de première page du rapport

Un levier tout au long du cycle fournisseur

Intégrée au processus AprovaLL, l'évaluation Galink s'active aux moments clés de la relation fournisseur : lors d'un appel d'offres sur des solutions IT, SaaS ou cloud ; à la contractualisation avec un fournisseur critique ; dans le cadre d'une campagne d'audit du panel ; ou au renouvellement d'un contrat arrivant à échéance.

Conclusion

Avec ce partenariat, AprovaLL et Galink proposent une réponse complète et clé en main au défi de l'évaluation cyber des fournisseurs : AprovaLL orchestre le cycle fournisseur et offre une vision 360° du panel, Galink apporte l'expertise cyber et opère les évaluations de bout en bout.

Les directions achats gagnent du temps et de la clarté : elles répondent aux exigences réglementaires et sécurisent leur chaîne d'approvisionnement, sans mobiliser d'expertise cyber interne. Plus vite. Plus clair. Plus sûr.



Les niveaux d'évaluation Cyber Fournisseur

Adapter le niveau d'évaluation à la criticité du fournisseur

Criticité	Type d'évaluation	En quoi ça consiste ?	Avantages	Limites
Faible	Scoring extérieur	- Analyse automatique de la surface d'attaque externe - Aucune information demandée au fournisseur - Domaines, IP, certificats, vulnérabilités exposées	- Aucune action du fournisseur requise - Déploiement immédiat et à grande échelle	- Vision uniquement externe - Rien sur la prestation ou l'interne de l'entreprise : ex où sont stockées les données ?
Faible	Questionnaire déclaratif	- Questionnaire sur les pratiques de sécurité du fournisseur - Couvre : accès, chiffrement, incidents, RGPD... - Réponses non vérifiées par des preuves	- Première vision de la maturité - Simple à déployer à grande échelle	- Engagement fournisseur faible - Aucune vérification des réponses
Modéré / Élevé	Questionnaire preuves	- Questionnaire accompagné de preuves documentaires - Politiques de sécurité, rapports de pentest, certifications (ISO, SOC 2...) - Analyse experte des documents fournis	- Vision fiable de la maturité réelle - Détection des non-conformités effectives - Alignement NIS2, DORA, ISO 27001	- Lourd sans expertise interne dédiée - Nécessite des ressources pour analyser les preuves
Critique	Audit sur site/ Pentest	- Audit approfondi directement chez le fournisseur - Intégrable dans vos exercices de pentest - Réservé aux prestataires critiques	- Niveau de garantie maximal - Détection des risques non visibles autrement	- Coûteux et chronophage - Requiert l'accord du fournisseur

La valeur ajoutée de l'expertise humaine

Le niveau 3 apporte ce que les outils ne peuvent pas offrir : la compréhension du contexte, la capacité à détecter des incohérences entre le discours et la réalité, et la formulation de recommandations adaptées à la situation spécifique du fournisseur. Un expert humain peut identifier un risque lié à une décision organisationnelle ou à une dépendance non documentée que ni un questionnaire ni une analyse de surface ne révéleraient.

Galink, partenaire d'AprovaLL, propose ce service managé d'analyse experte. Les résultats sont centralisés dans la plateforme AprovaLL pour une vision unifiée de la posture de chaque fournisseur.

Les limites du niveau 3

Le niveau 3 est une approche chronophage et coûteuse, qui justifie un périmètre restreint de fournisseurs à enjeux élevés. Il ne peut pas être déployé systématiquement sur l'ensemble d'un panel. C'est précisément pour cela qu'il s'inscrit dans une logique d'entonnoir : les niveaux 1 et 2 permettent d'identifier les fournisseurs qui méritent cet investissement.

AprovaLL en pratique

AprovaLL orchestre le déclenchement des analyses de niveau 3 depuis la plateforme, en lien avec les équipes Galink. Les résultats, recommandations et plans de remédiation sont centralisés dans la fiche fournisseur, aux côtés des données déclaratives et du score de surface, pour une vision 360° complète.



PARTIE 4

AprovaLL Manager : la plateforme qui orchestre les 3 niveaux

Disposer de méthodes d'évaluation complémentaires ne suffit pas si les données restent dispersées dans des outils différents, des tableurs et des boîtes mail. L'efficacité d'un programme TPRM repose sur la capacité à centraliser, corréler et actionner l'ensemble des informations disponibles sur chaque fournisseur.

1 | Le problème de l'éclatement des outils

La plupart des organisations qui gèrent le risque cyber tiers se heurtent au même obstacle : les données sont fragmentées. Les questionnaires sont gérés dans un outil, les documents dans un autre, les scores de risque dans un troisième. Les équipes Achats et Cybersécurité n'ont pas accès aux mêmes informations et ne parlent pas le même langage.

Cette fragmentation a des conséquences directes :

- Impossibilité d'avoir une vision consolidée de la posture cyber de l'ensemble du panel
- Prise de décision sur des données obsolètes ou incomplètes
- Temps excessif consacré à la coordination et à la consolidation manuelle
- Difficulté à justifier sa démarche face aux auditeurs et aux régulateurs

2 | AprovaLL Manager ; la plateforme unique de TPRM.

AprovaLL est une plateforme TPRM (Third Party Risk Management) conçue pour centraliser et orchestrer l'ensemble du parcours d'évaluation des fournisseurs, tous domaines de risque confondus, dont le risque cyber.

Sur le domaine Cyber, AprovaLL permet de :

- ✓ **Gérer la collecte automatisée** des questionnaires et documents (niveau 1) via AprovaLL Portal
- ✓ **Afficher et suivre le score de risque cyber quotidien** issu de Board of Cyber (niveau 2)
- ✓ **Centraliser les résultats** des analyses expertes Galink (niveau 3)
- ✓ **Corréler ces trois sources d'information** sur une fiche fournisseur unique
- ✓ **Générer des alertes automatiques** en cas de dégradation du score ou de non-conformité documentaire
- ✓ **Piloter la conformité** aux référentiels ISO 27001, NIS2 et DORA via des tableaux de bord dédiés

3 | Les bénéfices concrets



Gain de temps opérationnel

L'automatisation de la collecte documentaire, des relances fournisseurs et de la mise à jour des scores réduit considérablement le temps consacré aux tâches à faible valeur ajoutée. Les équipes peuvent se concentrer sur l'analyse et la décision plutôt que sur la logistique de collecte.



Fiabilité et objectivité des données

En combinant données déclaratives et score de surface objectif, AprovaLL offre une vision plus juste de la réalité que chaque méthode prise isolément. Le score Board of Cyber, mis à jour quotidiennement, garantit que les données disponibles reflètent l'état actuel et non une photographie vieille de plusieurs mois.



Conformité documentée

La traçabilité des évaluations, des historiques de scores et des plans de remédiation constitue un dossier de conformité exploitable directement pour les audits ISO 27001, les contrôles NIS2 ou les exigences DORA. AprovaLL facilite la démonstration de la démarche auprès des régulateurs et des partenaires.



Collaboration Achats & Cybersécurité

AprovaLL est conçu pour être utilisé conjointement par les équipes Achats et Cybersécurité. Les deux fonctions accèdent aux mêmes données, dans un environnement partagé qui favorise l'alignement des décisions stratégiques.



Grâce à AprovaLL, nous avons enfin une vision claire et consolidée de la posture cybersécurité de nos fournisseurs.

L'automatisation des évaluations a simplifié nos audits ISO 27001 et NIS2, tout en nous faisant gagner un temps précieux. Aujourd'hui, nous priorisons les actions sur les partenaires les plus critiques grâce à des données actualisées, et la collaboration avec les achats est désormais fluide et alignée.



CISO, Groupe Énergie & Services

PARTIE 5

Mettre en œuvre : guide de démarrage en 5 étapes

Construire un programme d'évaluation cyber fournisseurs peut sembler complexe. Voici un chemin de mise en œuvre structuré, applicable quelle que soit la taille de l'organisation et le niveau de maturité de départ.

1

Étape 1 | Cartographier

Commencer par constituer un inventaire exhaustif du panel fournisseurs actif : qui sont-ils, quelles prestations fournissent-ils, quels accès leur ont été accordés, quelles données traitent-ils ? Cette cartographie est le socle de tout ce qui suit.

Livrable attendu : une liste segmentée de fournisseurs avec leur niveau de criticité cyber (faible / modéré / élevé / critique).

2

Étape 2 | Qualifier

Déployer les questionnaires de niveau 1 sur l'ensemble du panel, avec une profondeur adaptée à chaque segment. Collecter les documents justificatifs (certifications, audits, politiques de sécurité). Automatiser les relances pour garantir un taux de réponse élevé.

Livrable attendu : un dossier documentaire complet pour chaque fournisseur, avec un statut de conformité déclarative.

3

Étape 3 | Scorer

Activer l'analyse de surface sur les fournisseurs à risque modéré à élevé. Intégrer les scores dans le tableau de bord de pilotage. Identifier les fournisseurs présentant un écart significatif entre leur déclaration (niveau 1) et leur score technique (niveau 2) : ce sont les premiers candidats au niveau 3.

Livrable attendu : un score de risque objectif et actualisé pour les fournisseurs prioritaires, avec alertes configurées.

4

Étape 4 | Auditer

Déclencher une analyse experte de niveau 3 sur les fournisseurs critiques identifiés. Structurer la démarche avec des entretiens, une revue documentaire approfondie et la production d'un plan de remédiation. Suivre l'avancement des actions correctives.

Livrable attendu : un rapport d'analyse expert avec recommandations priorisées et plan de remédiation suivi.

5

Étape 5 | Piloter

Centraliser l'ensemble des données sur une plateforme unique. Mettre en place un cycle de réévaluation : annuel pour les fournisseurs standard, semestriel pour les fournisseurs à risque élevé, continu (score de surface) pour les fournisseurs critiques. Partager le tableau de bord avec les équipes Achats pour intégrer les critères cyber dans les décisions d'achat.

Livrable attendu : un programme TPRM cyber opérationnel, avec des cycles d'évaluation définis, des indicateurs de pilotage et une collaboration Achats-Cybersécurité formalisée.

AprovaLL en pratique

Ces cinq étapes sont directement supportées par la plateforme AprovaLL, qui couvre l'ensemble du cycle de vie de l'évaluation fournisseurs : de la cartographie initiale au pilotage continu, en passant par l'orchestration des trois niveaux d'évaluation.

CONCLUSION

De la conformité subie à la maîtrise du risque

Le risque cyber fournisseurs n'est plus une problématique périphérique. Il est au cœur des préoccupations des RSSI, des directions Achats et des comités de direction, sous la pression conjuguée des incidents réels, des obligations réglementaires et des exigences croissantes des clients et partenaires.

Les organisations qui s'en sortent le mieux ne sont pas celles qui cochent le plus de cases dans un questionnaire annuel. Ce sont celles qui ont su construire un parcours d'évaluation structuré, combinant plusieurs niveaux d'analyse complémentaires, et piloté en continu plutôt que par à-coups.

Les trois niveaux présentés dans ce livre blanc : collecte documentaire, analyse de surface, expertise humaine, constituent un cadre robuste et proportionné, applicable quelle que soit la taille de l'organisation. Leur efficacité repose sur leur complémentarité : chaque niveau comble les angles morts du précédent.

La technologie joue un rôle essentiel dans cette démarche : automatiser la collecte, centraliser les données, corréler les sources, alerter en temps réel. Mais elle ne remplace pas le jugement humain pour les fournisseurs les plus critiques, ni la collaboration entre les équipes pour ancrer le risque cyber dans les décisions d'achat.

Évaluer ses fournisseurs n'est plus un exercice de conformité : c'est un avantage compétitif pour les organisations qui en font une pratique durable.

ANNEXES

A. Glossaire

DORA (Digital Operational Resilience Act)

Règlement européen applicable au secteur financier depuis janvier 2025, imposant des exigences strictes de résilience opérationnelle numérique, dont la gestion des risques liés aux prestataires TIC.

EASM (External Attack Surface Management)

Pratique consistant à identifier et analyser les actifs numériques d'une organisation (ou de ses fournisseurs) visibles depuis l'extérieur, afin d'évaluer leur exposition aux cyberattaques.

ISO 27001

Norme internationale de management de la sécurité de l'information. Sa version 2022 intègre des contrôles spécifiques sur la gestion des risques liés aux fournisseurs (A.5.19 à A.5.22).

NIS2 (Network and Information Security 2)

Directive européenne de 2023 renforçant les obligations de cybersécurité pour les entités essentielles et importantes, incluant la gestion des risques liés à la chaîne d'approvisionnement.

Score de surface

Indicateur synthétique calculé à partir de l'analyse de la surface d'attaque externe d'une organisation, reflétant son niveau d'exposition aux cybermenaces visible depuis Internet.

TPRM (Third Party Risk Management)

Ensemble des processus et outils permettant à une organisation d'identifier, évaluer, surveiller et gérer les risques liés à ses fournisseurs, prestataires et partenaires.

B. Tableau récapitulatif des 3 niveaux

Niveau	Approche	Couverture	Profondeur	Idéal pour
1	Questionnaires & documents	Large	Déclarative	Tout le panel
2	Score de surface (Board of Cyber)	Ciblée	Technique / objective	Fournisseurs à risque modéré à élevé
3	Analyse humaine managée (Galink)	Restreinte	Experte / contextuelle	Fournisseurs critiques

C. Checklist : Suis-je prêt à lancer mon programme ?



- ☐ J'ai cartographié l'ensemble de mon panel fournisseurs
- ☐ J'ai segmenté mes fournisseurs par niveau de criticité (accès SI, données sensibles, dépendance opérationnelle)
- ☐ J'ai identifié les réglementations applicables à mon secteur et mon périmètre (NIS2, DORA, ISO 27001...)
- ☐ J'ai mis en place un dispositif de collecte documentaire automatisé (questionnaires, certifications)
- ☐ J'ai activé une analyse de surface sur mes fournisseurs à risque modéré à élevé
- ☐ J'ai lancé une analyse experte pour mes fournisseurs à accès critique
- ☐ Je dispose d'un tableau de bord consolidé pour piloter l'ensemble des évaluations
- ☐ Mes équipes Achats et Cybersécurité partagent les mêmes données et critères de décision

AprovaLL

AprovaLL est un leader européen des logiciels de gestion des risques et de conformité des tiers (TPRM).

Grâce à sa plateforme AprovaLL Third Party Manager, ses clients bénéficient de l'ensemble des évaluations et des informations nécessaires tout le long du cycle de vie des relations avec leurs tiers, assurant leur conformité, la protection de leurs actifs et de leur réputation dans un environnement de plus en plus complexe et contraignant.

Pour en savoir plus,
visitez www.aprovaLL.com



Nos engagements

