AYI NEDJIMI Consultants

Gestion des tiers et supply chain : évaluer les risques

Catégorie : Consulting Lecture : 8 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Évaluez les risques cyber de votre supply chain. Méthodologie TPRM complète avec due diligence, monitoring continu et conformité NIS 2 et DORA.

Résumé exécutif

La gestion des risques liés aux tiers et à la supply chain numérique est devenue une priorité stratégique absolue pour les organisations confrontées à la multiplication des attaques exploitant les interconnexions avec les fournisseurs, prestataires et partenaires commerciaux. Ce guide détaille les méthodologies d'évaluation des risques tiers, les processus de due diligence cybersécurité à intégrer dans le cycle de vie des relations fournisseurs, les exigences réglementaires de NIS 2 et DORA en matière de supervision de la chaîne d'approvisionnement, et les outils pratiques permettant de structurer un programme de gestion des risques tiers mature, évolutif et démontrablement auditable par les autorités de contrôle européennes et les organismes de certification ISO 27001, en s'appuyant sur des retours d'expérience terrain issus de missions d'accompagnement auprès d'organisations de toutes tailles confrontées à la complexité croissante de leur écosystème numérique.

Les attaques par la supply chain numérique ont connu une croissance exponentielle ces dernières années, transformant radicalement l'approche de la cybersécurité organisationnelle qui ne peut plus se limiter à sécuriser le périmètre interne de l'entreprise. L'attaque SolarWinds de 2020, la compromission de Kaseya en 2021 et les vulnérabilités critiques dans des composants open source comme Log4Shell ont démontré de manière spectaculaire que la **surface d'attaque réelle** d'une organisation s'étend bien au-delà de ses propres systèmes d'information pour englober l'ensemble de son écosystème numérique. Les régulateurs européens ont pleinement intégré cette réalité dans la directive NIS 2, qui impose aux entités essentielles et importantes de prendre en compte les risques liés à la chaîne d'approvisionnement dans leurs mesures de gestion des risques cyber. Le règlement *DORA* va plus loin en exigeant des institutions financières une supervision active et continue de leurs prestataires de services TIC critiques. Face à cette convergence entre menace croissante et exigence réglementaire, la mise en place d'un programme structuré de **gestion des risques tiers** n'est plus une option mais une nécessité stratégique pour toute organisation responsable soucieuse de protéger ses actifs numériques et de maintenir la confiance de ses parties prenantes dans un écosystème numérique de plus en plus interdépendant et vulnérable aux effets de cascade.

Pourquoi la supply chain est-elle le maillon faible de la cybersécurité ?

La supply chain numérique représente un vecteur d'attaque privilégié pour les acteurs malveillants sophistiqués car elle offre un effet de levier considérable : compromettre un seul fournisseur stratégique peut ouvrir simultanément les portes de centaines ou milliers d'organisations clientes. Les attaquants étatiques et les groupes cybercriminels organisés l'ont parfaitement compris et investissent massivement dans le développement de techniques d'attaque ciblant spécifiquement la chaîne d'approvisionnement logicielle et de services.

Les risques liés aux tiers se manifestent sous plusieurs formes complémentaires. Le risque de **compromission directe** survient lorsqu'un attaquant utilise les accès du fournisseur pour pénétrer dans le système d'information du client. Le risque de **compromission logicielle** concerne l'injection de code malveillant dans les mises à jour ou les composants fournis. Le risque de **fuite de données** résulte d'une sécurité insuffisante chez un sous-traitant traitant des données sensibles du client. Le risque de **dépendance critique** expose l'organisation à une interruption d'activité en cas de défaillance d'un fournisseur unique sans alternative disponible, comme analysé dans notre guide sur la conformité NIS 2.

Combien de vos fournisseurs disposent d'un accès VPN permanent à votre réseau interne, et quand avez-vous pour la dernière fois vérifié que ces accès sont toujours légitimes et correctement segmentés ?

Mon avis : La gestion des risques tiers est le domaine où l'écart entre les intentions affichées et la réalité opérationnelle est le plus flagrant. La plupart des organisations envoient un questionnaire de sécurité à leurs fournisseurs lors de la contractualisation, puis ne vérifient plus jamais rien jusqu'au renouvellement du contrat trois ans plus tard. Un programme de gestion des risques tiers mature exige un monitoring continu et des audits périodiques, pas un simple exercice déclaratif ponctuel.

Comment évaluer les risques cybersécurité de vos fournisseurs ?

L'évaluation des risques cybersécurité des fournisseurs suit un processus structuré en quatre étapes. La première consiste à **classifier les fournisseurs** selon leur criticité pour l'organisation, en croisant le niveau d'accès aux données et systèmes, la criticité du service fourni pour les processus métier et la substituabilité du fournisseur. Cette classification détermine le niveau de diligence approprié : un fournisseur critique nécessite une évaluation approfondie, tandis qu'un fournisseur non critique peut être couvert par des contrôles allégés.

La deuxième étape consiste à collecter les informations de sécurité via des **questionnaires de sécurité** standardisés (SIG, CAIQ, questionnaire ANSSI) complétés par des éléments factuels : certifications détenues (ISO 27001, SOC 2), résultats de tests d'intrusion récents, politiques de sécurité et plans de continuité. La troisième étape évalue les réponses et attribue un score de risque. La quatrième étape définit les mesures de traitement : exigences contractuelles

renforcées, clauses d'audit, mesures de segmentation réseau pour les accès tiers ou recherche d'un fournisseur alternatif. Ce processus s'aligne avec la gestion des vulnérabilités de votre périmètre étendu.

Quelles exigences contractuelles imposer aux tiers ?

Le cadre contractuel constitue le levier principal pour maîtriser les risques liés aux tiers. Les clauses de cybersécurité à intégrer systématiquement dans les contrats fournisseurs couvrent les **obligations de sécurité** (respect d'un référentiel minimum, chiffrement des données, gestion des accès, journalisation), les **obligations de notification** (alerte en cas d'incident de sécurité affectant les données ou services du client dans un délai défini), les **droits d'audit** (possibilité pour le client ou un tiers mandaté de vérifier la conformité aux engagements de sécurité) et les **clauses de réversibilité** (conditions de récupération des données et de transfert du service en fin de contrat).

Pour les fournisseurs traitant des données personnelles, les clauses doivent également couvrir les exigences de l'article 28 du RGPD relatives aux sous-traitants : objet et durée du traitement, nature et finalité, types de données et catégories de personnes concernées, obligations et droits du responsable de traitement. Le **Data Processing Agreement** (DPA) doit être annexé au contrat principal et mis à jour lors de chaque évolution du périmètre de traitement. Les exigences contractuelles doivent être proportionnées à la classification de criticité du fournisseur et alignées avec la conformité RGPD.

Niveau de criticité	Due diligence requise	Fréquence de réévaluation	Clauses contractuelles
Critique (accès données sensibles)	Évaluation approfondie + audit sur site	Annuelle	SLA sécurité, audit, notification 24h
Important (accès SI partiel)	Questionnaire détaillé + preuves	Bisannuelle	Référentiel sécurité, notification 72h
Standard (service non critique)	Questionnaire simplifié	Triennale	Clauses de base, confidentialité
Faible (pas d'accès données/SI)	Déclaration de conformité	Au renouvellement	Confidentialité standard

L'attaque SolarWinds révélée en décembre 2020 reste le cas d'école majeur en matière de risque supply chain numérique. Le groupe APT Cozy Bear, attribué aux services de renseignement russes, a compromis le processus de build de la plateforme Orion de SolarWinds pour injecter une backdoor dans les mises à jour distribuées à plus de 18 000 organisations clientes, incluant des agences gouvernementales américaines et des entreprises du Fortune 500. Les organisations qui exigeaient contractuellement de SolarWinds la fourniture de rapports SOC 2 Type II et qui vérifiaient activement les indicateurs de compromission issus de leur plateforme de threat intelligence ont détecté l'anomalie significativement plus rapidement que celles reposant uniquement sur la confiance contractuelle.

Comment mettre en place un monitoring continu des tiers ?

Le monitoring continu des risques tiers complète les évaluations périodiques en fournissant une visibilité en temps quasi réel sur l'évolution de la posture de sécurité des fournisseurs. Les plateformes de **security rating** comme BitSight, SecurityScorecard ou RiskRecon évaluent en continu la surface d'attaque externe des fournisseurs en analysant les vulnérabilités exposées, les configurations DNS, les certificats SSL, les fuites de données et les indicateurs de compromission sur le dark web.

Ces outils fournissent un score de sécurité actualisé quotidiennement qui permet de détecter rapidement une dégradation de la posture de sécurité d'un fournisseur critique et de déclencher les actions appropriées (alerte, demande de clarification, audit extraordinaire, plan de sortie). Le monitoring continu doit être intégré dans les processus du SOC pour corréler les alertes de security rating avec les événements de sécurité détectés sur les flux réseau des fournisseurs. La combinaison évaluation périodique approfondie et monitoring continu automatisé constitue le standard de maturité attendu par les régulateurs NIS 2 et DORA.

Faut-il un programme dédié de gestion des risques tiers ?

La mise en place d'un programme dédié de gestion des risques tiers, souvent désigné sous l'acronyme *TPRM* (Third-Party Risk Management), est indispensable dès lors que l'organisation dépend de plus d'une dizaine de fournisseurs ayant accès à ses données ou systèmes. Le programme TPRM définit la politique de gestion des risques tiers, les processus d'évaluation et de suivi, les rôles et responsabilités, les outils utilisés et les indicateurs de performance du programme. Il est piloté par un responsable dédié rattaché au RSSI ou à la direction des risques.

Le programme couvre l'ensemble du cycle de vie de la relation fournisseur : due diligence pré-contractuelle, intégration sécurisée des accès (onboarding), monitoring continu pendant l'exécution du contrat, réévaluation périodique et désengagement sécurisé (offboarding) avec révocation de tous les accès et récupération des données. Les KPIs du programme incluent le taux de couverture des fournisseurs critiques évalués, le délai moyen de traitement des écarts identifiés, le score moyen de sécurité des fournisseurs et le nombre d'incidents liés aux tiers, en lien avec le log management. Les recommandations de l'ANSSI sur l'externalisation et de l'ENISA sur la supply chain security fournissent des cadres méthodologiques complémentaires.

Comment gérer l'offboarding sécurisé des fournisseurs ?

La fin de la relation contractuelle avec un fournisseur est une phase critique souvent négligée qui expose l'organisation à des risques significatifs si elle n'est pas gérée de manière structurée et documentée. Le processus d'offboarding sécurisé doit couvrir la révocation immédiate et vérifiée de tous les accès du fournisseur aux systèmes d'information de l'organisation, la récupération complète des données confiées au prestataire dans un format exploitable et documenté, la confirmation de la destruction effective des données chez le fournisseur conformément aux obligations contractuelles et réglementaires, et la clôture formelle de tous les comptes techniques et applicatifs utilisés dans le cadre de la prestation.

Le plan d'offboarding doit être préparé dès la phase contractuelle et testé régulièrement, particulièrement pour les fournisseurs critiques dont la substitution nécessite une période de transition significative. La réversibilité effective des données et des services doit être vérifiée par des tests périodiques pendant la durée du contrat, et non découverte lors de la fin de la relation. Les clauses contractuelles doivent prévoir explicitement les modalités de transition, les délais de restitution des données et les pénalités en cas de non-respect des engagements de réversibilité par le fournisseur sortant.

Sources et références : ANSSI · CERT-FR

Quel rôle pour l'intelligence artificielle dans la gestion des risques tiers ?

Les technologies d'intelligence artificielle et d'apprentissage automatique transforment progressivement la gestion des risques tiers en automatisant les tâches de collecte, d'analyse et de surveillance qui nécessitaient auparavant un effort humain considérable et souvent insuffisant pour couvrir l'ensemble de l'écosystème fournisseurs. Les plateformes de TPRM de nouvelle génération intègrent des capacités d'analyse automatique des questionnaires de sécurité par traitement du langage naturel, de corrélation des données de security rating avec les informations contractuelles et de détection précoce des signaux faibles annonciateurs d'une dégradation de la posture de sécurité d'un fournisseur.

Ces outils permettent également d'automatiser la classification des fournisseurs en fonction de leur profil de risque, de générer des rapports d'évaluation structurés à partir de données hétérogènes et de prioriser les actions de remédiation en fonction de l'exposition réelle de l'organisation. Cependant, l'intelligence artificielle ne remplace pas le jugement humain pour les décisions critiques de gestion des risques tiers, notamment l'évaluation de la fiabilité d'un fournisseur stratégique, la négociation des clauses contractuelles de sécurité ou la décision de maintenir ou de rompre une relation fournisseur présentant un niveau de risque élevé persistant malgré les demandes de remédiation.

À retenir : La gestion des risques tiers exige une approche structurée couvrant tout le cycle de vie fournisseur : classification par criticité, due diligence proportionnée, exigences contractuelles robustes, monitoring continu et réévaluation périodique. Les réglementations NIS 2 et DORA imposent désormais une supervision active de la chaîne d'approvisionnement numérique. Investissez dans des outils de security rating pour compléter les questionnaires déclaratifs par des données objectives et actualisées.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr