FICHE DE RÉVISION

Module : Gestion des Prestataires et Conformité

Formation : Pilotage et Animation de la Cybersécurité

🤝 1. Gestion des Prestataires et Sous-traitants

> **Objectif :** Identifier les obligations et les risques liés à la sous-traitance

▸ Cadre réglementaire de la sous-traitance

Texte	Article clé	Obligation pour le donneur d'ordre
RGPD	Art. 28 — Contrat de sous-traitance	Formaliser un DPA (Data Processing Agreement), vérifier que le ST offre des garanties suffisantes, auditer
NIS2	Art. 21 — Sécurité de la chaîne d'approvisionnement	Évaluer les risques liés aux fournisseurs TIC, imposer des exigences de sécurité contractuelles
DORA	Art. 28-44 — Risques liés aux tiers TIC	Registre des contrats TIC, clauses obligatoires, surveillance des PTCI (prestataires tiers critiques)
ISO 27001	Annexe A — A.5.19 à A.5.22	Politique de sécurité fournisseurs, exigences dans les accords, suivi et revue des services
LPM / RGS	Qualification ANSSI	Recourir à des prestataires qualifiés PRIS, PDIS, hébergeurs SecNumCloud pour les OIV/OSE

▸ Typologies de prestataires et niveau de risque associé

Type de prestataire	Exemples	Risque cyber principal	Niveau de risque
Hébergeur / Cloud IaaS	AWS, Azure, OVH, Scaleway	Défaillance, compromission de l'infrastructure, localisation des données	🔴 Élevé
Éditeur SaaS	Salesforce, Microsoft 365, SAP	Fuite de données, indisponibilité, dépendance fournisseur (vendor lock-in)	🔴 Élevé
ESN / Infogérance	Prestataire infogérance IT, TMA applicative	Accès privilégiés, rebond d'attaque, exfiltration via VPN partagé	🔴 Élevé
Prestataire de sécurité	SOC externe, pentest, MSSP	Accès aux données sensibles, qualité des livrables, dépendance	🟠 Moyen-élevé
Fournisseur de matériel	Constructeurs hardware, IoT	Firmware malveillant, backdoors, composants contrefaits	🟠 Moyen
Prestataire de maintenance	Techniciens sur site, hotline	Accès physique, ingénierie sociale, accès non supervisé	🟠 Moyen

Éditeur de logiciel	Développeur d'applications métier	Supply chain attack, vulnérabilités non patchées, dépendances tierces	🟡 Modéré

▸ Processus de qualification et de sélection d'un prestataire

#	Étape	Actions concrètes
1	Cartographie et inventaire	Lister tous les prestataires accédant au SI, aux données ou aux locaux ; les classifier par criticité
2	Évaluation initiale (due diligence)	Questionnaire sécurité, vérification des certifications (ISO 27001, SecNumCloud, HDS), analyse financière
3	Analyse des risques spécifiques	Évaluer la sensibilité des données traitées, les accès accordés, la dépendance opérationnelle
4	Contractualisation	Intégrer les clauses de sécurité (DPA, SLA, audit, notification incidents) avant toute collaboration
5	Surveillance continue	Revues périodiques, suivi des SLA, alertes CVE sur les solutions du prestataire, threat intelligence
6	Évaluation annuelle	Questionnaire de réévaluation, audit si criticité élevée, revue des incidents de l'année
7	Gestion de la fin de contrat	Plan de réversibilité, récupération des données, révocation des accès, destruction sécurisée

▸ Matrice de criticité prestataire (exemple de critères de scoring)

Critère d'évaluation	Pondération	Questions de scoring
Sensibilité des données traitées	30 %	Données personnelles sensibles ? Données financières ? Secrets industriels ?
Niveau d'accès au SI	25 %	Accès physique ? Accès réseau ? Comptes privilégiés ? Accès en production ?
Dépendance opérationnelle	20 %	Interruption possible en cas de défaillance ? Single point of failure ?
Maturité sécurité du prestataire	15 %	Certifications ISO 27001 ? SOC 2 ? Politique de sécurité documentée ?
Exposition géographique	10 %	Sous-traitance hors UE ? Pays à risque ? Juridiction applicable ?

📝 2. Clauses Contractuelles de Sécurité

> **Objectif :** Rédiger des clauses types et analyser un contrat fournisseur

▸ Architecture contractuelle de la relation prestataire

La sécurité doit être intégrée à chaque niveau de la relation contractuelle, depuis l'appel d'offres jusqu'à la fin de contrat. Les documents contractuels se complètent et ne se substituent pas.

Document	Rôle	Contenu sécurité clé

Contrat principal / MSA	Cadre juridique général de la relation	Engagement de confidentialité, droit d'audit, responsabilités générales
DPA (Data Processing Agreement)	Contrat de sous-traitance RGPD (Art. 28)	Finalités, durée, nature des données, mesures de sécurité, sous-sous-traitance
SLA (Service Level Agreement)	Niveau de service et disponibilité	RTO/RPO, taux de disponibilité, délai de notification incident, pénalités
NDA (Non-Disclosure Agreement)	Confidentialité des informations échangées	Périmètre de confidentialité, durée, sanctions, restitution des documents
Politique de sécurité fournisseur (PSF)	Exigences de sécurité à respecter	Liste des règles à appliquer : chiffrement, MFA, gestion des accès, audit logs
Plan d'Assurance Sécurité (PAS)	Engagement du prestataire sur ses mesures	Détail des mesures mises en oeuvre, référencement des certifications

▸ Catalogue de clauses contractuelles de sécurité types

Clause	Obligatoire ?	Contenu et formulation type
Confidentialité	Oui (RGPD + usage)	Le prestataire s'engage à maintenir la stricte confidentialité de toutes les informations, données et documents auxquels il a accès dans le cadre du contrat, y compris après sa cessation.
Mesures de sécurité minimales	Oui (RGPD Art. 32)	Le prestataire met en oeuvre les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque (chiffrement, MFA, gestion des correctifs, journalisation).
Notification d'incident	Oui (RGPD/NIS2)	Le prestataire notifie le client de tout incident de sécurité affectant les données ou services couverts dans un délai de 24 heures après détection, avec un rapport complet sous 72 heures.
Droit d'audit	Oui (RGPD Art. 28)	Le client se réserve le droit de mener ou de faire mener, par un tiers indépendant, des audits de sécurité auprès du prestataire, sur préavis raisonnable (15 jours ouvrés), aux frais du client.
Gestion des accès et habilitations	Oui	Le prestataire applique le principe du moindre privilège. Les comptes d'accès sont nominatifs, tracés, et révoqués immédiatement en cas de départ ou de fin de mission.
Sous-sous-traitance	Oui (RGPD Art. 28.2)	Le prestataire ne peut recourir à un sous-traitant supplémentaire sans l'accord préalable écrit du client. Il reste responsable de sa conformité aux mêmes exigences de sécurité.
Localisation des données	Recommandé	Les données du client sont hébergées et traitées exclusivement dans l'Union Européenne / sur des infrastructures certifiées SecNumCloud, sauf autorisation expresse du client.
Réversibilité et portabilité	Recommandé	En fin de contrat, le prestataire remet l'intégralité des données au client dans un format ouvert et interopérable, dans un délai de 30 jours, et procède à la destruction certifiée des copies.
Pénalités de non-conformité	Recommandé	Tout manquement aux exigences de sécurité constaté lors d'un audit ou d'un incident expose le prestataire à des pénalités contractuelles définies en Annexe X, sans préjudice des recours légaux.

SLA de sécurité	Recommandé	Le prestataire garantit un taux de disponibilité de XX % et un délai maximal de résolution des incidents de sécurité critiques de YY heures. Tout dépassement donne lieu à des crédits de service.

▸ Grille d'analyse d'un contrat fournisseur — Points de vigilance

Point à vérifier	Statut	Questions à se poser
Clause de confidentialité	✅ / ❌	Couvre-t-elle toutes les catégories de données ? Est-elle opposable après la fin du contrat ?
DPA conforme RGPD Art. 28	✅ / ❌	Toutes les mentions obligatoires sont-elles présentes ? Les sous-traitants sont-ils listés ?
Droit d'audit explicite	✅ / ❌	Le délai de préavis est-il raisonnable ? Les frais sont-ils précisés ? L'accès aux logs est-il garanti ?
Délai de notification incident	✅ / ❌	Le délai est-il inférieur à 24h ? Les canaux de notification sont-ils définis ?
Localisation des données	✅ / ❌	Les données restent-elles dans l'UE ? Les transferts hors UE sont-ils encadrés (CCT, BCR) ?
Réversibilité / sortie de contrat	✅ / ❌	Le format de restitution est-il ouvert ? La destruction est-elle certifiée ? Quel est le délai ?
Limitation de responsabilité	✅ / ❌	Le plafond de responsabilité est-il cohérent avec la valeur des données traitées ?
Loi applicable et juridiction	✅ / ❌	La loi française / européenne est-elle applicable ? La juridiction compétente est-elle identifiée ?

🔍 3. Pilotage des Audits et Évaluations

> **Objectif :** Construire un plan d'audit interne / externe

▸ Définition et objectifs des audits de sécurité

Un audit de sécurité est une évaluation formelle et documentée de la conformité, de l'efficacité et du niveau de maturité des mesures de sécurité d'un système, d'un prestataire ou d'une organisation.

Type d'audit	Objectif principal	Qui réalise ?
Audit interne	Vérifier l'application de la PSSI et des procédures internes, préparer la certification	Équipe audit interne, RSSI, référents sécurité
Audit externe / de certification	Obtenir ou renouveler une certification (ISO 27001, HDS, SecNumCloud)	Organisme certificateur accrédité (AFNOR, BSI, Bureau Veritas…)
Audit prestataire / fournisseur	Vérifier le respect des clauses contractuelles et des exigences de sécurité	RSSI + équipe sécurité du client, éventuellement tiers auditeur
Pentest (test d'intrusion)	Identifier les vulnérabilités exploitables depuis l'extérieur ou l'intérieur	Prestataire qualifié PASSI (ANSSI), ethical hacker

Audit de code / applicatif	Détecter les vulnérabilités dans le code source (SAST) ou en exécution (DAST)	Développeurs sécurité, prestataire spécialisé
Audit de configuration	Vérifier les durcissements (hardening) des systèmes, équipements réseau, cloud	Équipe sécurité opérationnelle, outil automatisé (CIS-CAT, Nessus)

▸ Construire un plan d'audit annuel

#	Étape	Contenu et livrables
1	Définition du périmètre	Identifier les entités, systèmes et processus à auditer ; prioriser selon la criticité et les résultats N-1
2	Sélection des référentiels	Choisir les normes et cadres de contrôle : ISO 27001, RGPD, NIS2, DORA, PSSI interne, CIS Controls
3	Planification calendaire	Établir le calendrier sur 12 mois : fréquence par type d'audit, ressources mobilisées, budget
4	Préparation des questionnaires	Préparer les grilles de contrôle, les demandes de preuves (logs, procédures, attestations, certifications)
5	Réalisation de l'audit	Entretiens, revue documentaire, tests techniques, observations sur site
6	Rapport d'audit	Documenter les constats, les écarts, les risques associés, les recommandations priorisées (critique / majeur / mineur)
7	Plan d'action corrective (PAC)	Pour chaque écart : action corrective, responsable, délai, ressources, indicateur de clôture
8	Suivi et vérification	Vérifier la mise en oeuvre des actions correctives ; clôturer ou escalader les écarts non traités

▸ Qualification des écarts — Grille de criticité

Niveau	Définition	Délai de correction	Exemple
🔴 Critique	Non-conformité majeure exposant à un risque élevé immédiat	< 15 jours / immédiat	Absence de MFA sur les comptes admin, données sensibles non chiffrées
🟠 Majeur	Non-conformité significative réduisant l'efficacité des contrôles	30 à 60 jours	Patch management non documenté, logs non conservés 1 an
🟡 Mineur	Écart limité, contrôle partiellement en place ou documentation incomplète	90 à 180 jours	Charte informatique non signée par tous, procédure non mise à jour
🔵 Observation	Bonne pratique à améliorer, risque négligeable	Prochaine revue annuelle	Formation sécurité non formalisée, absence d'indicateur sur un process

▸ Exemple de structure de plan d'audit prestataire

Prestataire	Type d'audit	Fréquence	Prochaine date	Référentiel / Périmètre
Hébergeur Cloud	Audit documentaire + questionnaire	Annuel	T1 N+1	ISO 27001, SecNumCloud, localisation données
ESN infogérance	Audit sur site + test d'accès	Annuel	T2 N+1	PSSI, gestion des accès, habilitations, logs
Éditeur SaaS critique	Revue documentaire (SOC 2, ISO 27001)	Annuel	T2 N+1	Certification, DPA, notification incidents
Prestataire de maintenance	Vérification des accès et traçabilité	Semestriel	T1 N+1	Gestion des comptes, journaux, habilitations
Sous-traitant de données RH	Audit DPA + sécurité des traitements	Annuel	T3 N+1	RGPD Art. 28, minimisation, durée conservation

⚠️ 4. Gestion des Incidents Contractuels

> **Objectif :** Gérer les non-conformités, plans d'action, sanctions

▸ Définition et types d'incidents contractuels

Un incident contractuel est tout manquement d'un prestataire à ses obligations définies dans le contrat ou dans les documents annexes (PSSI, DPA, SLA, PAS). Il se distingue de l'incident de sécurité au sens technique, même si les deux peuvent être liés.

Type d'incident contractuel	Exemples concrets	Conséquence potentielle
Violation de confidentialité	Fuite de données client vers un tiers non autorisé, accès non justifié aux données	Résiliation, dommages-intérêts, notification CNIL, sanctions RGPD
Non-respect des SLA	Indisponibilité du service au-delà du RTO contractuel, délai de résolution dépassé	Pénalités financières, crédits de service, résiliation si récidive
Défaut de notification	Incident non signalé dans le délai contractuel (ex : > 24h)	Mise en demeure, pénalité, risque de sanction réglementaire solidaire
Non-conformité aux exigences sécurité	Absence de MFA, patch non appliqué, non-respect de la PSSI fournisseur	Plan de remédiation exigé, audit imposé, suspension d'accès
Sous-traitance non autorisée	Recours à un sous-traitant supplémentaire sans accord préalable	Résiliation pour faute, engagement de la responsabilité civile
Incident de sécurité imputable	Cyberattaque via un accès prestataire (rebond VPN, compromission compte admin)	Responsabilité civile, résiliation, déclaration aux autorités

▸ Processus de gestion d'un incident contractuel

#	Phase	Actions et responsables
1	Détection et qualification	Identifier et documenter le manquement (logs, alertes SLA, rapport d'audit) ; qualifier sa gravité (critique / majeur / mineur)
2	Notification formelle	Adresser un courrier de mise en demeure au prestataire avec description précise des faits, référence contractuelle et délai de réponse
3	Analyse des causes	Demander au prestataire une analyse de cause racine (RCA — Root Cause Analysis) sous délai défini contractuellement
4	Plan d'action correctif (PAC)	Co-construire ou valider le plan de remédiation : actions, responsables, jalons, preuves de correction attendues
5	Suivi et vérification	Contrôler la mise en oeuvre du PAC aux jalons fixés ; effectuer un audit de vérification si nécessaire
6	Application des sanctions	Si le PAC n'est pas respecté : appliquer les pénalités prévues, suspendre les accès ou initier la procédure de résiliation
7	Clôture et capitalisation	Documenter l'incident, mettre à jour la cartographie des risques fournisseurs, réviser les clauses contractuelles si nécessaire

▸ Gradation des sanctions contractuelles

Niveau de sanction	Mécanisme	Conditions de déclenchement
1. Avertissement formel	Lettre de mise en demeure sans pénalité financière immédiate	Premier manquement, non-conformité mineure ou écart isolé
2. Pénalités financières	Déduction du montant contractuellement prévu sur la prochaine facture	SLA non respecté, délai de notification dépassé, non-conformité récurrente
3. Audit imposé aux frais du prestataire	Audit de sécurité diligenté par le client, coût à charge du prestataire	Incident de sécurité significatif, défaut de notification, suspicion de non-conformité grave
4. Suspension d'accès	Révocation temporaire des accès au SI jusqu'à remédiation prouvée	Risque immédiat pour le SI ou les données, compromission détectée
5. Résiliation pour faute	Fin anticipée du contrat sans indemnité à verser au prestataire	Violation grave et répétée, refus de remédier, mise en danger avéré des données

▸ Documentation et traçabilité

- Conserver tous les échanges écrits liés à l'incident (emails, courriers, PV de réunion)
- Horodater chaque action du processus de gestion de l'incident
- Enregistrer dans un registre des incidents contractuels (prestataire, date, type, gravité, statut PAC)
- Informer les parties prenantes internes concernées : DG, DPO, Direction Juridique, DSI
- Notifier les autorités si l'incident contractuel entraîne une violation de données (CNIL sous 72h, ANSSI si OIV/OSE)

5. Veille Réglementaire et Conformité Continue

Objectif : Mettre à jour la conformité selon NIS2, RGPD, ISO 27001

Pourquoi la conformité est un processus continu ?

La conformité n'est pas un état figé mais un processus d'amélioration continue. Les réglementations évoluent, les technologies changent, les menaces se renouvellent et l'organisation se transforme. Une conformité obtenue ne garantit pas une conformité maintenue.

Déclencheur de mise à jour	Impact sur la conformité
Nouvelle réglementation ou révision	NIS2, DORA, CRA, actes délégués RGPD : nouvelles obligations à intégrer dans les processus et contrats
Évolution de l'organisation	Fusion-acquisition, nouveau métier, ouverture à un nouveau marché : réévaluation du périmètre SMSI et des risques
Incident de sécurité significatif	Révision des mesures défaillantes, mise à jour de la PSSI, révision des clauses contractuelles
Résultats d'audit défavorables	Plan d'action corrective, mise à jour des procédures, formation des équipes
Évolution technologique majeure	Migration Cloud, déploiement IA, nouveaux usages IoT : évaluation de l'impact sur la surface d'attaque
Menaces émergentes	Nouvelle technique d'attaque, CVE critique, alerte CERT-FR : mise à jour des mesures de protection

Cycle de conformité continue — Le modèle PDCA appliqué

Phase	Activité	Actions concrètes
PLAN	Veille & diagnostic	Surveiller les évolutions réglementaires (RGPD, NIS2, DORA), cartographier les écarts, mettre à jour la cartographie des risques
DO	Mise en oeuvre	Mettre à jour les politiques, procédures et contrats ; déployer les nouvelles mesures de sécurité ; former les équipes
CHECK	Contrôle & mesure	Audits internes, revue des indicateurs de conformité, tests de restauration, campagnes de phishing simulé
ACT	Amélioration	Traiter les non-conformités, mettre à jour le registre des risques, présenter le bilan à la direction, réviser la PSSI

Tableau de veille réglementaire — Sources et rythme de consultation

Source	Type de contenu	Fréquence	URL / Abonnement
ANSSI	Alertes, bulletins de sécurité, référentiels, guides	Hebdomadaire	ssi.gouv.fr — flux RSS
CERT-FR	Avis de vulnérabilité, alertes incidents, IoC	Quotidien	cert.ssi.gouv.fr — alertes email
CNIL	Délibérations, recommandations, mises en demeure	Mensuel	cnil.fr — newsletter

EUR-Lex / JOUE	Règlements, directives, actes délégués UE	Mensuel	eur-lex.europa.eu
ENISA	Rapports de menaces, guidelines NIS2, DORA	Trimestriel	enisa.europa.eu
NVD / CVE	Base de vulnérabilités, scores CVSS, patches	Quotidien	nvd.nist.gov — flux RSS CVE
ISO / AFNOR	Nouvelles normes, révisions (27001:2022, 27005:2022)	Annuel	iso.org — bulletins AFNOR

▸ Checklist de mise à jour de la conformité — NIS2, RGPD, ISO 27001

Action de conformité	Réglementation	Description et fréquence
Mettre à jour le registre des traitements	RGPD	Réviser les finalités, bases légales, durées de conservation — annuellement ou à chaque nouveau traitement
Réviser et re-signer les DPA	RGPD / NIS2	Mettre à jour les clauses si changement de sous-traitant ou nouvelle obligation réglementaire
Conduire une nouvelle AIPD si besoin	RGPD	Si nouveau traitement à risque élevé ou modification substantielle d'un traitement existant
Mettre à jour la Déclaration d'Applicabilité (DdA)	ISO 27001	Après chaque révision du périmètre SMSI ou modification des risques — annuellement
Réévaluer les risques fournisseurs	NIS2 / DORA	Suite à un incident, un changement de prestataire ou une alerte sectorielle — annuellement
Former les dirigeants à la cybersécurité	NIS2	Formation obligatoire et documentée des membres de la direction sur les risques cyber
Tester le PCA/PRA	ISO 27001 / DORA	Exercices de simulation annuels avec documentation des résultats et des axes d'amélioration
Mettre à jour les clauses contractuelles	NIS2 / DORA / RGPD	À chaque renouvellement de contrat ou nouvelle réglementation applicable aux prestataires
Renouveler la certification ISO 27001	ISO 27001	Audit de surveillance annuel + recertification tous les 3 ans auprès de l'organisme accrédité
Notifier l'autorité compétente	NIS2 / RGPD	En cas d'incident significatif : ANSSI (NIS2 / LPM) et CNIL (RGPD) dans les délais réglementaires

📌 Mémo Récapitulatif — À Retenir

🤝 Prestataires	📝 Clauses	🔍 Audits	⚠️ Incidents	📡 Conformité
• Art. 28 RGPD = DPA obligatoire • 7 étapes : inventaire → fin de contrat • Criticité : données + accès + dépendance	• 6 documents : MSA, DPA, SLA, NDA, PSF, PAS • 10 clauses types (confidentialité → pénalités) • Notification incident < 24h	• 6 types d'audit (interne, externe, pentest…) • 8 étapes du plan d'audit (périmètre → clôture)	• 7 phases de gestion (détection → clôture) • 5 niveaux de sanction (avertissement → résiliation)	• Conformité = cycle PDCA continu • 6 déclencheurs de mise à jour • Veille : CERT-FR (quotidien),

• Qualification ANSSI : PRIS, PDIS, SecNumCloud • Réversibilité prévue dès le contrat	dans le contrat • Droit d'audit = clause non négociable • Localisation données UE à exiger	• 4 niveaux : critique / majeur / mineur / obs. • Critique → correction < 15 jours • PASSI = qualification ANSSI pour les pentests	• RCA exigée du prestataire sous délai • Traçabilité : registre incidents contractuels • Violation données → CNIL 72h + ANSSI si OIV	CNIL (mensuel) • DdA ISO 27001 révisée annuellement • NIS2 : formation dirigeants obligatoire