FICHE DE RÉVISION

Module : Mise en Oeuvre d'Actions de Contrôle

Formation : Pilotage et Animation de la Cybersécurité

1. Plan de Traitement et Priorisation des Actions

> **Objectif :** Élaborer un plan de maîtrise adapté aux risques identifiés

Du risque à l'action — La logique du plan de traitement

Le Plan de Traitement des Risques (PTR) est le document opérationnel qui formalise, pour chaque risque retenu, l'option de traitement choisie, les mesures à mettre en oeuvre, les responsables, les délais et les ressources nécessaires. Il constitue le lien entre l'analyse des risques et les actions concrètes de sécurité.

Étape amont	Lien avec le plan de traitement
Cartographie des risques	Fournit la liste priorisée des risques (rouge → vert) et les scores V × I à partir desquels les actions sont définies
Option de traitement choisie	Pour chaque risque : Réduire / Accepter / Transférer / Éviter — choix qui détermine la nature des actions à mener
Déclaration d'Applicabilité (ISO 27001)	Référence les mesures de l'Annexe A applicables pour chaque risque à réduire
Appétit au risque de la direction	Définit le seuil en dessous duquel un risque peut être accepté sans mesure corrective

Structure type d'un Plan de Traitement des Risques (PTR)

ID	Risque / Scénario	Option retenue	Mesure(s) à mettre en oeuvre	Responsable	Délai cible	Statut
SCN-042	Ransomware via phishing admin	🔽 Réduire	MFA sur tous comptes admin, segmentation réseau, sensibilisation ciblée	RSSI + DSI	J+30	🟡 En cours
SCN-015	Fuite données via API exposée	🔽 Réduire	Audit des API, déploiement WAF, tests de pénétration	DSI + Dev	J+45	🔴 Non démarré
SCN-008	Indisponibilité datacenter	🔄 Transférer + Réduire	Assurance cyber souscrite, PCA revu, sauvegardes hors-site testées	RSSI + DG	J+60	🟡 En cours
SCN-031	Vol de poste en télétravail	🔽 Réduire	Chiffrement intégral	DSI	J+90	🟡 En cours

			(BitLocker), MDM déployé, politique BYOD révisée			
SCN-019	Panne équipement non critique	✅ Accepter	Risque documenté et validé par la direction — surveillance trimestrielle	RSSI	N/A	🟢 Accepté

▸ Critères de priorisation des actions de traitement

Critère	Description	Exemple d'arbitrage
Niveau de risque (V × I)	Les risques en zone critique (rouge) sont traités en priorité absolue, avant tout autre arbitrage	SCN-042 (score 12) traité avant SCN-031 (score 8)
Impact réglementaire	Tout risque entraînant une violation RGPD, NIS2 ou LPM est traité prioritairement quelle que soit son ampleur financière	Fuite de données personnelles → priorité absolue
Facilité et rapidité de mise en oeuvre	Une mesure rapide à fort impact de réduction est priorisée (quick win) sur une mesure longue à effet équivalent	Activer le MFA en 2 jours vs. segmentation réseau en 3 mois
Coût proportionné à l'impact	Le coût de la mesure doit être inférieur à la valeur de l'actif protégé et au coût potentiel de l'incident	Patch d'un serveur critique : 2h d'astreinte vs. millions de rançon
Dépendances entre actions	Certaines mesures sont préalables à d'autres (ex. : inventaire des actifs avant audit de configuration)	Déployer l'EDR avant d'activer la détection comportementale du SIEM
Exposition dans le temps	Un risque dont la vraisemblance augmente (CVE activement exploitée, alerte CERT-FR) remonte en priorité	CVE critique publiée → remontée immédiate dans le PTR

▸ Les quick wins sécurité — Actions à fort impact et faible coût

Action (Quick Win)	Impact sur les risques	Délai typique	Coût estimé
Activer le MFA sur tous les comptes	Réduit de 99 % le risque de compromission par credential stuffing	1 à 5 jours	Faible à nul (inclus dans M365, Google)
Appliquer les patches critiques (CVSS ≥ 9)	Supprime les vecteurs d'attaque les plus exploités	24 à 72h	Faible (astreinte technique)
Activer le chiffrement des postes (BitLocker/FileVault)	Élimine le risque de vol de données en cas de perte ou vol de matériel	1 semaine	Nul (natif Windows/macOS)

Mettre en place la règle de sauvegarde 3-2-1	Réduit drastiquement l'impact d'un ransomware ou d'une panne	2 à 4 semaines	Modéré (stockage externe)
Désactiver les comptes inactifs et les droits orphelins	Réduit la surface d'attaque interne et les mouvements latéraux	1 semaine	Nul (revue manuelle ou script)
Déployer SPF, DKIM et DMARC sur les domaines de messagerie	Réduit fortement l'usurpation d'identité par email (phishing, spoofing)	2 à 5 jours	Nul (configuration DNS)

▸ Gouvernance du PTR — Rôles et instances

Acteur / Instance	Rôle dans le PTR	Fréquence d'intervention
RSSI	Pilote du PTR : définit les actions, suit les avancements, escalade les blocages, rapporte à la direction	Continu — revue hebdomadaire des actions en cours
Direction Générale	Valide les risques résiduels acceptés, arbitre les budgets et les priorités entre projets concurrents	Trimestriel — revue du PTR et des risques résiduels
DSI / Équipes IT	Met en oeuvre les mesures techniques, remonte les blocages opérationnels, fournit les preuves de correction	Hebdomadaire — avancement des chantiers techniques
Directions métier	Valident les impacts sur leurs processus, participent aux tests de continuité, remontent les besoins de sécurité	Mensuel — revue des risques par périmètre métier
Comité de pilotage sécurité (COPIL)	Instance de gouvernance : arbitre, valide les priorités, suit les indicateurs, escalade à la DG si nécessaire	Mensuel ou trimestriel — tableau de bord PTR

2. Pilotage et Indicateurs de Suivi

Objectif : Mettre en place des KPI et tableaux de bord sécurité

▸ Taxonomie des indicateurs de sécurité

Type	Définition	Mesure	Exemples
KRI — Key Risk Indicator	Mesure le niveau d'exposition au risque en amont d'un incident	Lagging / Leading	Nb de CVE critiques non patchées, nb comptes sans MFA
KPI — Key Performance Indicator	Mesure la performance des processus de sécurité mis en oeuvre	Performance	Délai moyen de patch, taux de conformité PSSI, % EDR déployé

KCI — Key Control Indicator	Vérifie qu'un contrôle de sécurité est en place et fonctionne	Contrôle	% comptes avec MFA actif, couverture antivirus, logs conservés
Métriques opérationnelles SOC	Données techniques temps réel pour le pilotage opérationnel quotidien	Opérationnel	MTTD (détection), MTTR (résolution), volume alertes SIEM

▸ Catalogue complet de KPIs — Par domaine de contrôle

Domaine	Indicateur	Cible	Fréquence	Type
Gestion des vulnérabilités	% CVE critiques (CVSS ≥ 9) corrigées dans les délais	> 95 %	Mensuel	KPI
Gestion des vulnérabilités	Délai moyen de correction CVE critiques (MTTM)	< 72 h	Mensuel	KPI
Gestion des vulnérabilités	Nb de vulnérabilités critiques non corrigées > 30 jours	= 0	Hebdo	KRI
Contrôle des accès	% comptes utilisateurs avec MFA activé	> 99 %	Mensuel	KCI
Contrôle des accès	Nb comptes inactifs (> 90 jours) non désactivés	= 0	Mensuel	KCI
Contrôle des accès	Nb comptes à droits excessifs identifiés	Tendance ↓	Trimestriel	KRI
Gestion des incidents	Nb d'incidents de sécurité critiques sur la période	Tendance ↓	Mensuel	KRI
Gestion des incidents	Délai moyen de détection — MTTD	< 24 h	Mensuel	KPI
Gestion des incidents	Délai moyen de résolution — MTTR (incidents critiques)	< 4 h	Mensuel	KPI
Sensibilisation	Taux de clic sur campagnes de phishing simulé	< 5 %	Trimestriel	KPI
Sensibilisation	Taux de complétion formations sécurité obligatoires	> 90 %	Annuel	KPI
Conformité PSSI	% de conformité à la PSSI (audit interne)	> 80 %	Annuel	KCI
Conformité PSSI	Nb d'écarts critiques sans plan d'action documenté	= 0	Trimestriel	KCI
Continuité et sauvegardes	% de restaurations de sauvegardes testées avec succès	100 %	Semestriel	KCI
Continuité et sauvegardes	Taux de disponibilité des services SI critiques	> 99,9 %	Mensuel	KPI
Plan de traitement (PTR)	% actions PTR réalisées dans les délais	> 85 %	Mensuel	KPI
Plan de traitement (PTR)	Nb de risques critiques sans mesure de traitement active	= 0	Mensuel	KRI

▸ Structure du tableau de bord sécurité — Niveaux de lecture

Niveau	Audience	Contenu et format
Tableau de bord Stratégique	Direction Générale, COMEX	1 page : synthèse RAG (Rouge/Ambre/Vert), 3-5 KPIs clés, faits marquants du mois, décisions à prendre — fréquence : mensuelle ou trimestrielle
Tableau de bord Tactique	COPIL sécurité, DSI, DPO	5-10 pages : avancement PTR, KPIs par domaine (graphiques), écarts de conformité, incidents en cours, alertes réglementaires — fréquence : mensuelle
Tableau de bord Opérationnel	Équipe sécurité, SOC, RSSI	Temps réel ou quotidien : alertes SIEM, tickets incidents ouverts, scan de vulnérabilités, logs de connexion — via plateforme SOC ou SIEM

▸ Contenu type du tableau de bord stratégique mensuel

§	Rubrique	Contenu recommandé
1	Synthèse exécutive (RAG)	Niveau de risque global : 🟢 Maîtrisé / 🟡 Vigilance / 🔴 Critique — 2 lignes d'explication
2	Faits marquants sécurité	Incidents significatifs, alertes CERT-FR impactantes, vulnérabilités critiques publiées
3	3 à 5 KPIs clés	Graphiques simples avec tendance N vs N-1 : ex. MTTD, % MFA, taux conformité PTR
4	Avancement du PTR	Tableau RAG des chantiers sécurité : statut (vert/orange/rouge), jalons atteints, blocages
5	Conformité réglementaire	Statut RGPD, NIS2, ISO 27001 : actions en cours, échéances, risques de sanction
6	Décisions à prendre	Arbitrages budgétaires, validations de risques résiduels, choix stratégiques à soumettre à la DG

▸ Principes d'un reporting efficace

- Adapter le niveau de détail à l'audience : 1 page RAG pour la DG, détail opérationnel pour le SOC
- Visualiser plutôt que chiffrer : jauges, graphiques tendance, codes couleur RAG — pas de tableaux de chiffres bruts
- Contextualiser les données : comparer à N-1, au benchmark sectoriel, aux objectifs fixés en début d'année
- Relier les indicateurs aux enjeux métier : traduire un MTTD de 36h en impact opérationnel compréhensible par un DG
- Déboucher sur des décisions : chaque reporting doit proposer des arbitrages ou des validations, pas seulement informer
- Garantir la régularité : un reporting irrégulier perd en crédibilité — fixer et respecter un calendrier annuel fixe

🔍 3. Contrôles et Audits Internes de Sécurité

> **Objectif :** Appliquer les principes de contrôle et d'audit

▸ Distinction entre contrôle et audit

Dimension	Contrôle de sécurité	Audit de sécurité

Définition	Vérification régulière et ciblée qu'une mesure ou une règle est bien appliquée	Évaluation formelle et indépendante d'un périmètre de sécurité par rapport à un référentiel
Fréquence	Continue, régulière (quotidien à mensuel)	Périodique et planifiée (semestriel, annuel)
Indépendance	Réalisé par les équipes internes (RSSI, DSI)	Nécessite une indépendance : auditeur interne ou externe distinct des opérationnels
Livrables	Dashboard, alerte, ticket, note interne	Rapport d'audit, liste d'écarts qualifiés, plan d'action correctif (PAC)
Exemples	Revue des logs de connexion, scan de vulnérabilités hebdo, vérification des sauvegardes	Audit ISO 27001, audit de conformité PSSI, audit prestataire, pentest

▸ Les types de contrôles de sécurité

Nature du contrôle	Objectif	Exemples
Contrôles préventifs	Empêcher un incident de se produire	MFA, chiffrement, politique de mots de passe, formation, liste blanche applicative
Contrôles détectifs	Identifier qu'un incident est en cours ou s'est produit	SIEM, IDS, analyse des logs, alerte sur comportement anormal (UEBA)
Contrôles correctifs	Limiter les dommages et restaurer l'état nominal après un incident	PCA, restauration de sauvegarde, patch d'urgence, isolation d'un système compromis
Contrôles dissuasifs	Décourager les comportements non autorisés par la visibilité des mesures	Charte informatique avec sanctions, journalisation affichée, caméras de surveillance
Contrôles compensatoires	Pallier une mesure primaire impossible à mettre en oeuvre	Surveillance renforcée d'un système ne pouvant pas être patché (EOL), accès strictement supervisé

▸ Programme d'audit interne de sécurité — Cycle annuel

#	Phase	Actions et livrables
1	Planification annuelle	Définir le programme : périmètres à auditer, référentiels retenus (ISO 27001, PSSI, RGPD), ressources, calendrier, budget
2	Préparation de l'audit	Réunion d'ouverture, préparation du plan d'audit détaillé, envoi des demandes documentaires aux audités
3	Collecte des preuves	Entretiens avec les responsables, revue documentaire (procédures, logs, tickets), tests techniques, observations terrain
4	Analyse des écarts	Comparer la situation constatée au référentiel ; qualifier chaque écart (critique / majeur / mineur / observation)
5	Rédaction du rapport	Synthèse exécutive, constats détaillés, niveau de risque associé à chaque écart, recommandations priorisées
6	Réunion de clôture	Présentation des constats aux audités, recueil de leurs observations, validation de la liste des écarts

7	Plan d'action correctif (PAC)	Co-construire le PAC avec les responsables : action, responsable, délai, ressources, preuve de correction attendue
8	Suivi et vérification	Contrôler la mise en oeuvre aux jalons fixés ; clôturer les écarts ou escalader si délais non tenus

▸ Domaines et référentiels de contrôle interne

Domaine de contrôle	Référentiel de contrôle	Points clés à vérifier
Gestion des accès et des identités	ISO 27001 Annexe A — A.5.15 à A.5.18	MFA actif, revue trimestrielle des droits, comptes inactifs désactivés, journalisation des connexions privilégiées
Gestion des mises à jour	CIS Controls v8 — IG1 à IG3	Inventaire exhaustif, délais de patch respectés, systèmes EOL identifiés et migrés ou compensés
Sécurité réseau et périmétrique	ISO 27001 — A.8.20 à A.8.22	Règles firewall documentées et révisées, segmentation VLAN effective, flux non autorisés bloqués
Sauvegardes et restauration	ISO 27001 — A.8.13	Règle 3-2-1 appliquée, restaurations testées et documentées, RTO/RPO définis et testés
Gestion des incidents	ISO 27001 — A.5.24 à A.5.28	Procédure formalisée, délais de détection et traitement respectés, RETEX documentés
Sensibilisation et formation	ISO 27001 — A.6.3	Programme annuel en place, taux de complétion mesuré, campagnes de phishing documentées
Conformité RGPD	RGPD Art. 5, 24, 25, 32	Registre des traitements à jour, DPA signés, AIPD réalisées, notifications de violations conformes

▸ Qualification des écarts — Grille de criticité

Niveau	Définition	Délai de correction	Exemples
🔴 Critique	Non-conformité exposant à un risque élevé immédiat pour le SI ou les données	< 15 jours ou immédiat	Absence de MFA admin, données sensibles non chiffrées, CVE critique non patchée
🟠 Majeur	Non-conformité réduisant significativement l'efficacité des contrôles de sécurité	30 à 60 jours	Logs non conservés 12 mois, droits non revus depuis plus de 6 mois, PCA non testé
🟡 Mineur	Écart limité, contrôle partiellement en place ou documentation incomplète	90 à 180 jours	Charte non signée par certains prestataires, procédure obsolète, formation non tracée
🔵 Observation	Bonne pratique à améliorer, pas de risque identifiable à court terme	Prochaine revue annuelle	Indicateur non formalisé, modèle de rapport à standardiser

4. Suivi des Risques Résiduels et Amélioration Continue

Objectif : Maintenir le plan de sécurité et réévaluer les risques

Définition et gestion du risque résiduel

Le risque résiduel est le risque qui subsiste après la mise en oeuvre de l'ensemble des mesures de traitement. Il ne peut jamais être nul : toute organisation doit donc gérer formellement ses risques résiduels et décider, en connaissance de cause, de les accepter, surveiller ou traiter davantage.

Concept	Description et exigence
Risque résiduel accepté	Risque délibérément maintenu en l'état après arbitrage coût/bénéfice : décision formelle et signée par la direction (ISO 27001 exige une trace documentée)
Risque résiduel surveillé	Risque supérieur au seuil d'acceptation mais dont le traitement est en cours : fait l'objet d'indicateurs de surveillance rapprochée
Risque résiduel transféré	Risque couvert par un tiers (assurance cyber, clause contractuelle) : le risque financier est transféré mais pas le risque opérationnel
Appétit au risque résiduel	Seuil défini par la gouvernance en dessous duquel les risques sont automatiquement acceptés : doit être formalisé dans la politique de gestion des risques

Processus de réévaluation des risques — Déclencheurs et fréquences

Déclencheur de réévaluation	Fréquence	Impact sur la cartographie et le PTR
Revue périodique planifiée	Annuel (minimum)	Réévaluation complète : V, I et efficacité des mesures en place — nouvelle version de la cartographie
Incident de sécurité significatif	Ad hoc après incident	Réévaluation des scénarios liés, ajout de nouveaux risques, mise à jour immédiate du PTR
Résultats d'audit défavorables	Après chaque audit	Mise à jour des niveaux de risque pour les actifs et processus concernés par les écarts
Évolution de l'organisation	À chaque changement majeur	Fusion, acquisition, nouveau SI, nouveau prestataire : réévaluation du périmètre et des dépendances
Nouvelle réglementation	À chaque entrée en vigueur	Réévaluation des risques de non-conformité, mise à jour du PTR et des mesures compensatoires
CVE critique ou alerte CERT-FR	Dès publication	Réévaluation immédiate de la vraisemblance des scénarios concernés, remontée dans le PTR si nécessaire
Nouvelle menace ou attaque sectorielle	Dès information disponible	Ajout ou révision des scénarios EBIOS RM, mise à jour des sources de risques et des mesures associées

Le cycle d'amélioration continue — PDCA appliqué à la sécurité

Phase PDCA	Activité sécurité	Actions concrètes et livrables
🔵 PLAN	Analyser et planifier	Cartographie des risques, définition du PTR, budget sécurité, objectifs annuels SMSI — Livrable : PTR validé, roadmap
🟢 DO	Mettre en oeuvre	Déploiement des mesures techniques, formation des équipes, mise à jour des politiques et procédures — Livrable : preuves de mise en oeuvre
🟡 CHECK	Contrôler et mesurer	Audits internes, suivi des KPIs, tests de restauration, campagnes phishing — Livrable : rapport d'audit, tableau de bord KPIs
🔴 ACT	Améliorer et corriger	Traitement des non-conformités, mise à jour du PTR, réévaluation des risques, revue de direction — Livrable : PAC, nouvelle version cartographie

▸ La revue de direction — Exigence ISO 27001 (Chapitre 9.3)

La revue de direction est une réunion formelle et documentée au cours de laquelle la direction valide l'état du SMSI, arbitre les risques résiduels, valide les objectifs et alloue les ressources pour la période suivante.

Point à l'ordre du jour	Contenu et décisions attendues
État du plan de traitement (PTR)	Avancement des chantiers sécurité, actions en retard, demandes de ressources supplémentaires
Bilan des incidents de la période	Incidents significatifs, impacts constatés, efficacité des mesures de réponse, RETEX
Résultats des audits et contrôles	Synthèse des écarts, état du PAC, taux de conformité PSSI, résultats des campagnes phishing
Risques résiduels à valider	Liste des risques résiduels nécessitant une acceptation formelle ou une décision de traitement complémentaire
Évolutions réglementaires impactantes	Nouvelles obligations NIS2, DORA, RGPD : actions requises, délais, ressources nécessaires
Objectifs SMSI pour la période suivante	Validation des nouveaux objectifs, budget sécurité, projets prioritaires, indicateurs cibles

▸ Retour d'Expérience (RETEX) — Capitaliser après chaque incident ou audit

Étape du RETEX	Contenu et questions clés
1. Description factuelle	Que s'est-il passé ? Chronologie précise des événements depuis la détection jusqu'à la résolution
2. Analyse des causes racines	Pourquoi cela s'est-il produit ? Quelle vulnérabilité, quelle défaillance organisationnelle ou technique a permis l'incident ?
3. Évaluation de la réponse	Comment a-t-on réagi ? Les délais de détection et de traitement étaient-ils dans les objectifs ? Les procédures ont-elles été suivies ?
4. Mesures correctives	Quelles actions immédiates ont été prises ? Sont-elles suffisantes ou faut-il des mesures supplémentaires à long terme ?
5. Mise à jour du PTR et de la cartographie	Faut-il réviser des scénarios de risques ? Ajouter de nouvelles mesures au PTR ? Mettre à jour la PSSI ?

6. Communication et partage	Quelles leçons partager avec les équipes, les métiers, les prestataires ? Faut-il informer les autorités (ANSSI, CNIL) ?

▸ Indicateurs de maturité et de progression du SMSI

Indicateur de maturité	Mesure	Interprétation
Évolution du score de risque moyen	Score V×I moyen de la cartographie	Une baisse du score moyen traduit l'efficacité des mesures de traitement mises en oeuvre
Taux de risques critiques résolus	Nb risques critiques → zone orange/verte	Mesure directe de l'efficacité du PTR sur les risques les plus importants
Taux de conformité PSSI (évolution)	% contrôles conformes à l'audit N vs N-1	Progression de la conformité dans le temps — objectif : hausse régulière vers 100 %
Délai moyen de traitement des écarts	Jours entre détection et clôture d'un écart	Un délai qui diminue traduit l'amélioration de la réactivité et de l'organisation
Taux de respect des délais du PTR	% actions PTR réalisées dans les délais	Indicateur de pilotage et d'engagement des équipes — objectif > 85 %
Niveau de maturité SMSI (CMM)	Score CMM (1 à 5) mesuré annuellement	Permet de situer l'organisation sur l'échelle Initial → Reproductible → Défini → Géré → Optimisé

📌 Mémo Récapitulatif — À Retenir

🔲 Plan de Traitement (PTR)	📊 Pilotage & KPIs	🔍 Contrôles & Audits	🔄 Risques Résiduels & PDCA
• PTR = lien entre risque et action • 4 options : Réduire / Accepter / Transférer / Éviter • Prioriser : score V×I + réglementation + quick wins • Quick wins : MFA, patch, chiffrement, 3-2-1, SPF/DKIM • Gouvernance : COPIL mensuel, DG trimestriel • Statut RAG : 🔴 Non démarré → 🟢 Clôturé	• 3 types : KRI (risque) / KPI (perf.) / KCI (contrôle) • 3 niveaux de TDB : Stratégique / Tactique / Opérationnel • MTTD cible < 24h | MTTR critique < 4h • % PTR dans les délais > 85 % • TDB direction : 1 page RAG, 3-5 KPIs, décisions • Reporting → toujours déboucher sur des décisions	• 5 types de contrôles : préventif / détectif / correctif / dissuasif / compensatoire • Audit ≠ Contrôle : indépendance obligatoire pour l'audit • 8 phases du programme d'audit (plan → suivi PAC) • 4 niveaux d'écarts : 🔴🟠🟡🔵 • Critique → correction < 15 jours • PAC : action + responsable + délai + preuve	• Risque résiduel : accepté, surveillé ou transféré • Acceptation formelle signée par la DG (ISO 27001) • 7 déclencheurs de réévaluation des risques • PDCA : Plan→Do→Check→Act (cycle continu) • Revue de direction : exigence ISO 27001 ch. 9.3 • RETEX : 6 étapes après incident ou audit

Le cycle vertueux de la maîtrise des risques

Risques identifiés → PTR priorisé → KPIs & TDB → Contrôles & Audits → Risques résiduels réévalués → Amélioration continue (PDCA)