# FICHE DE RÉVISION

Module : Gouvernance et Stratégie de la Sécurité SI

Formation : Pilotage et Animation de la Cybersécurité

## 1. Introduction à la Gouvernance de la Sécurité

> **Objectif :** Comprendre le rôle du RSSI, les enjeux de gouvernance et de conformité

### Définition et enjeux de la gouvernance de la sécurité

La gouvernance de la sécurité des SI désigne l'ensemble des structures, processus et mécanismes permettant de diriger, contrôler et piloter la sécurité de l'information en cohérence avec la stratégie de l'organisation.

| Enjeu | Explication |
|---|---|
| Conformité réglementaire | Respecter le RGPD, NIS2, LPM, ISO 27001 pour éviter sanctions et responsabilités |
| Protection des actifs | Préserver la confidentialité, l'intégrité et la disponibilité des informations critiques |
| Continuité d'activité | Garantir la résilience opérationnelle face aux incidents et crises cyber |
| Confiance des parties prenantes | Clients, partenaires, régulateurs : la sécurité est un facteur de réputation et de compétitivité |
| Alignement stratégique | La sécurité n'est pas un frein : elle doit accompagner et sécuriser les projets métier |

### Le RSSI — Responsable de la Sécurité des Systèmes d'Information

| Dimension | Détail |
|---|---|
| Mission principale | Définir, piloter et animer la politique de sécurité de l'organisation |
| Positionnement | Rattachement idéal à la Direction Générale ou DSI — indépendance fonctionnelle essentielle |
| Compétences clés | Technique (réseaux, sécurité), juridique (RGPD, NIS2), management, communication, gestion des risques |
| Rôle vis-à-vis de la DG | Conseiller stratégique, reporter sur le niveau de risque, proposer des arbitrages |
| Rôle vis-à-vis des métiers | Partenaire de confiance, accompagnateur des projets (security by design) |
| Rôle vis-à-vis des équipes IT | Définir les exigences sécurité, auditer et contrôler leur application |

### Les acteurs de la gouvernance sécurité

| Acteur | Rôle | Interaction avec le RSSI |
|---|---|---|
| Direction Générale | Sponsor de la sécurité, arbitrage budgétaire, validation de la PSSI | Reporting mensuel/trimestriel, validation des risques résiduels |

| | | |
|---|---|---|
| DSI | Mise en oeuvre technique, gestion des infrastructures et projets SI | Coordination opérationnelle, exigences sécurité dans les projets |
| DPO | Conformité RGPD, gestion des droits des personnes, AIPD | Collaboration sur les traitements de données à risque |
| Direction Juridique | Conformité légale, gestion des contrats fournisseurs, incidents | Qualification juridique des incidents, clauses sécurité |
| Direction des Risques | Cartographie des risques globaux de l'entreprise (ERM) | Intégration du risque cyber dans la cartographie globale |
| Audit interne | Contrôle de l'application de la PSSI, conformité | Audits sécurité, recommandations, suivi du plan d'action |
| Métiers / Directions | Utilisateurs finaux, porteurs des processus critiques | Sensibilisation, remontée des besoins, validation des risques métier |

### ▸ Modèles de gouvernance de référence

| Modèle / Cadre | Domaine | Apport pour la gouvernance sécurité |
|---|---|---|
| COBIT 2019 | Gouvernance et management du SI | Alignement IT/business, objectifs de gouvernance, indicateurs de maturité |
| ISO/IEC 27014 | Gouvernance de la sécurité de l'information | Principes et processus dédiés à la gouvernance sécurité, rôle du CISO |
| NIST CSF 2.0 | Cadre de cybersécurité américain (international) | 5 fonctions : Govern, Identify, Protect, Detect, Respond, Recover |
| EBIOS Risk Manager | Gestion des risques (ANSSI) | Méthode française d'analyse de risques, compatible ISO 27005 et NIS2 |

## 🎯 2. Élaborer une Stratégie de Cybersécurité

> **Objectif :** Identifier les leviers organisationnels et stratégiques

### ▸ Les étapes d'élaboration d'une stratégie cyber

| # | Étape | Actions clés |
|---|---|---|
| 1 | Diagnostic de l'existant | Audit de l'existant (technique, organisationnel), cartographie des actifs, identification des vulnérabilités |
| 2 | Analyse des risques | Identification des menaces et scénarios d'attaque, évaluation de la criticité (EBIOS RM, ISO 27005) |
| 3 | Définition des objectifs | Niveau de sécurité cible, alignement avec la stratégie d'entreprise et les obligations réglementaires |
| 4 | Choix des leviers | Organisationnels, humains, techniques et juridiques (voir ci-dessous) |
| 5 | Feuille de route (roadmap) | Priorisation des actions, planification sur 3 ans, budgétisation, jalons mesurables |
| 6 | Pilotage et révision | KPIs, tableaux de bord, revues annuelles, adaptation aux nouvelles menaces |

## ▸ Les 4 leviers stratégiques

| Levier | Actions | Exemples concrets |
|---|---|---|
| 🏗️ Organisationnel | Structurer la gouvernance, définir des rôles et responsabilités clairs, créer des instances de pilotage | Comité de pilotage sécurité (COPIL), RSSI, référents sécurité par direction |
| 👥 Humain | Sensibiliser, former, responsabiliser l'ensemble des collaborateurs et de la direction | Campagnes de phishing simulé, e-learning, charte informatique, formations métiers |
| 🔧 Technique | Déployer et maintenir les équipements et solutions de sécurité adaptés aux risques | Firewalls NGFW, EDR, SIEM, MFA, chiffrement, segmentation réseau |
| ⚖️ Juridique & Contractuel | Intégrer la sécurité dans les contrats, les achats et les relations fournisseurs | Clauses de sécurité, audits fournisseurs, exigences SecNumCloud, assurance cyber |

## ▸ Modèle de maturité de la sécurité (Capability Maturity Model)

Évaluer le niveau de maturité actuel permet de fixer des objectifs réalistes et de prioriser les investissements.

| Niveau | Stade | Caractéristiques |
|---|---|---|
| 1 | Initial / Inexistant | Pas de processus formalisé, réaction ad hoc aux incidents, peu ou pas de sensibilisation |
| 2 | Reproductible | Processus basiques en place, documentation partielle, dépendant des individus clés |
| 3 | Défini | Processus documentés, PSSI formalisée, sensibilisation structurée, audits réguliers |
| 4 | Géré / Mesuré | KPIs définis et suivis, gestion des risques intégrée, reporting direction, plans d'action |
| 5 | Optimisé | Amélioration continue, anticipation proactive, veille active, benchmarking, culture cyber partagée |

## ▸ Construire la feuille de route cyber (roadmap)

| Critère | Court terme (0-6 mois) | Moyen terme (6-18 mois) | Long terme (18-36 mois) |
|---|---|---|---|
| Priorité | Mesures immédiates : parer aux risques critiques | Structuration et montée en compétences | Optimisation et certification |
| Actions types | MFA, patch management, sauvegarde, charte | SMSI, PSSI, SOC, sensibilisation, DPIA | ISO 27001, SIEM, gestion de crise, tests |
| Budget | Dépenses urgentes et rapides | Investissements structurants | Optimisation et recertification |
| Indicateur de succès | Réduction incidents critiques | Taux de conformité PSSI > 80 % | Certification ou label obtenu |

### Alignement stratégie cyber / stratégie d'entreprise

- Participer aux comités de direction et aux projets de transformation pour intégrer la sécurité dès la conception
- Traduire les risques cyber en impacts métier compréhensibles par la direction (perte financière, réputation, continuité)
- Défendre un budget sécurité argumenté : ROI de la sécurité, coût d'un incident vs. coût de la prévention
- Construire un argumentaire basé sur la réglementation, les benchmarks sectoriels et les incidents récents

## 3. Définir et Formaliser la PSSI

> **Objectif :** Construire la politique de sécurité adaptée à l'entreprise

### Qu'est-ce que la PSSI ?

La Politique de Sécurité des Systèmes d'Information (PSSI) est le document de référence qui formalise les orientations stratégiques, les règles et les responsabilités en matière de sécurité de l'information. Elle constitue le socle contractuel interne de la sécurité.

| Caractéristique | Détail |
|---|---|
| Approuvée par | La Direction Générale — engagement formel et visible |
| Destinée à | Tous les collaborateurs, prestataires et partenaires accédant au SI |
| Durée de validité | Généralement 2 à 3 ans, révisée en cas d'événement majeur (incident, réforme, acquisition) |
| Niveau d'abstraction | Stratégique et organisationnel — ne détaille pas les procédures techniques (celles-ci font l'objet de documents dédiés) |
| Opposabilité | Document opposable en cas d'incident : signature ou acceptation obligatoire |

### Structure type d'une PSSI

| § | Chapitre | Contenu attendu |
|---|---|---|
| 1 | Préambule et contexte | Présentation de l'organisation, enjeux, périmètre couvert par la PSSI |
| 2 | Cadre juridique et réglementaire | Textes applicables : RGPD, NIS2, LPM, RGS, normes ISO, sectorielles |
| 3 | Objectifs et principes de sécurité | CIA (Confidentialité, Intégrité, Disponibilité), non-répudiation, engagement de la direction |
| 4 | Organisation de la sécurité | Rôles et responsabilités : RSSI, DPO, référents, directions métier |
| 5 | Gestion des risques | Méthodologie retenue (EBIOS, ISO 27005), seuils d'acceptation, revue périodique |
| 6 | Règles de sécurité par domaine | Accès, mots de passe, télétravail, BYOD, messagerie, mobilité, cloud, tiers |
| 7 | Gestion des incidents | Procédure de signalement, classification, escalade, communication de crise |
| 8 | Sensibilisation et formation | Obligations de formation, charte informatique, sanctions en cas de manquement |
| 9 | Contrôle et audit | Audits internes et externes, indicateurs de suivi, processus d'amélioration |

| | | |
|---|---|---|
| 10 | Révision et mise à jour | Fréquence de révision, déclencheurs de mise à jour, processus de validation |

### ▸ Domaines couverts par la PSSI — Principales règles

| Domaine | Règles de sécurité associées |
|---|---|
| Gestion des accès | MFA obligatoire, principe de moindre privilège, revue trimestrielle des droits, comptes nominatifs |
| Mots de passe | 12 caractères min., complexité, renouvellement annuel, coffre-fort de mots de passe (ex. KeePass, Bitwarden) |
| Postes de travail | Chiffrement de disque, verrouillage automatique, politique de mises à jour, antivirus/EDR |
| Messagerie | SPF/DKIM/DMARC, interdiction de données sensibles en clair, vigilance phishing |
| Télétravail / BYOD | VPN obligatoire, séparation des usages pro/perso, interdiction des réseaux Wi-Fi publics non sécurisés |
| Données sensibles | Classification (public, interne, confidentiel, secret), chiffrement au repos et en transit, DLP |
| Fournisseurs et tiers | Clause de sécurité contractuelle, audit de conformité, restriction d'accès au strict nécessaire |
| Sauvegardes | Règle 3-2-1 (3 copies, 2 supports, 1 hors site), tests de restauration périodiques |

### ▸ Processus de validation et de déploiement de la PSSI

- Rédaction par le RSSI en concertation avec les métiers, la DSI, le DPO et la direction juridique
- Consultation et validation des directions impactées (DSI, RH, Achats, Finance)
- Approbation formelle par la Direction Générale — engagement visible et signé
- Communication institutionnelle : réunion de lancement, diffusion sur l'intranet, annexe au règlement intérieur
- Formation et sensibilisation : appropriation par les collaborateurs, signature de la charte
- Suivi : audit de conformité à 6 mois, revue annuelle, mise à jour en cas d'événement déclencheur

## 📣 4. Sensibilisation et Communication Interne

> **Objectif :** Concevoir des actions de sensibilisation et des supports adaptés

### ▸ Pourquoi sensibiliser ?

L'humain est impliqué dans plus de 80 % des incidents de sécurité (erreur, négligence, manipulation). La sensibilisation est le levier le plus rentable pour réduire la surface d'attaque.

| Objectif | Résultat attendu |
|---|---|
| Réduire les risques humains | Diminuer les clics sur liens malveillants, les fuites de données accidentelles, les mauvaises pratiques |
| Créer une culture sécurité | La sécurité devient un réflexe partagé, pas une contrainte imposée de l'extérieur |
| Responsabiliser les collaborateurs | Chaque individu se sent acteur de la sécurité de son organisation |

| | |
|---|---|
| Répondre aux obligations | RGPD (Art. 32), ISO 27001 (Annexe A - sensibilisation), NIS2 (formation des dirigeants) |

## Les cibles et messages adaptés

| Cible | Besoins spécifiques | Messages clés à adapter |
|---|---|---|
| Direction générale | Vision risque/ROI, enjeux de responsabilité légale | Cyber = risque stratégique, coût d'un incident, obligations NIS2/DORA |
| Managers / Encadrement | Exemplarité, relais de la culture sécurité, gestion d'équipes distantes | Bonne hygiène numérique, incidents de leur périmètre, comment réagir |
| Collaborateurs (tous) | Pratiques quotidiennes, phishing, mots de passe, télétravail | Bons réflexes, signalement incidents, charte informatique |
| Équipes IT / DSI | Sécurité by design, gestion des droits, incidents techniques | Procédures techniques, gestion des vulnérabilités, réponse incidents |
| Prestataires / Tiers | Exigences contractuelles, manipulation de données sensibles | Clauses PSSI, traçabilité des accès, obligations RGPD |

## Les formats de sensibilisation

| Format | Modalité | Avantages | Limites |
|---|---|---|---|
| E-learning / LMS | Formation en ligne asynchrone | Scalable, traçable, disponible 24/7 | Moins engageant, risque de zapping |
| Phishing simulé | Campagne de faux emails d'hameçonnage | Mesure réelle du comportement, pédagogie immédiate | À cadrer éthiquement, peut être vécu comme un piège |
| Ateliers / Wargames | Simulation d'incident, exercices de crise | Très engageant, ancrage durable | Coûteux en temps, nécessite une animation experte |
| Affichage / Intranet | Affiches, newsletters, vidéos courtes | Large diffusion, faible coût | Impact limité sans suivi, oublié rapidement |
| Réunions de sensibilisation | Présentations en équipe, quizz | Interactif, questions/réponses, contextualisé | Limité en taille de groupe, chronophage |
| Serious game / Escape game | Jeu pédagogique immersif | Très engageant, mémorisation élevée | Coût de conception élevé |

## Concevoir un plan de sensibilisation annuel

| Étape | Action | Responsable | Livrable |
|---|---|---|---|
| 1. Diagnostic | Identifier les comportements à risque, analyser les incidents passés | RSSI | Rapport diagnostic sensibilisation |

| | | | |
|---|---|---|---|
| 2. Ciblage | Définir les populations prioritaires et les messages associés | RSSI + RH | Matrice cibles / messages |
| 3. Planification | Choisir les formats, planifier les actions sur 12 mois, budgéter | RSSI + Com interne | Calendrier annuel de sensibilisation |
| 4. Déploiement | Lancer les actions : campagnes phishing, e-learnings, ateliers | RSSI + RH + IT | Indicateurs de participation |
| 5. Mesure | Évaluer l'impact : taux de clic phishing, résultats quiz, incidents | RSSI | Rapport de bilan et KPIs sensibilisation |

### ▸ Indicateurs d'efficacité de la sensibilisation

- Taux de clic sur campagnes de phishing simulé (objectif : < 5 % à 12 mois)
- Taux de signalement des emails suspects (objectif : > 30 % des cibles)
- Taux de complétion des formations e-learning (objectif : > 90 %)
- Score aux quiz de sensibilisation avant / après formation
- Nombre d'incidents liés à une erreur humaine (tendance sur 12 mois)
- Taux de signature de la charte informatique (objectif : 100 % des collaborateurs)

## 5. Indicateurs et Tableaux de Bord Sécurité

> **Objectif :** Concevoir des KPIs et des reportings pour la direction

### ▸ Pourquoi mesurer la sécurité ?

Ce qui ne se mesure pas ne se pilote pas. Les indicateurs de sécurité permettent de démontrer la valeur du programme sécurité, d'identifier les axes d'amélioration, de prioriser les ressources et de rendre des comptes à la direction.

### ▸ Taxonomie des indicateurs

| Type d'indicateur | Définition | Exemples |
|---|---|---|
| KRI — Key Risk Indicator | Mesure le niveau d'exposition au risque (en amont) | Nombre de vulnérabilités critiques non patchées, exposition périmétrique |
| KPI — Key Performance Indicator | Mesure la performance des processus de sécurité | Délai moyen de patch, taux de conformité PSSI, disponibilité des services |
| KCI — Key Control Indicator | Vérifie que les contrôles sont en place et efficaces | Taux de comptes avec MFA actif, couverture EDR sur les postes |
| Métriques opérationnelles | Données techniques et chiffrées en temps réel | Nombre d'alertes SIEM, temps de réponse incidents, logs analysés |

### ▸ Catalogue de KPIs par domaine

| Domaine | Indicateur (KPI) | Cible | Fréquence |
|---|---|---|---|
| Gestion des vulnérabilités | % de vulnérabilités critiques corrigées dans les délais | > 95 % | Mensuel |

| | | | |
|---|---|---|---|
| Gestion des vulnérabilités | Délai moyen de correction (MTTR) des CVE critiques | < 72 h | Mensuel |
| Gestion des accès | % de comptes avec MFA actif | > 99 % | Mensuel |
| Gestion des accès | Nombre de comptes inactifs non désactivés | = 0 | Trimestriel |
| Gestion des incidents | Nombre d'incidents critiques sur la période | Tendance ↓ | Mensuel |
| Gestion des incidents | Délai moyen de détection (MTTD) | < 24 h | Mensuel |
| Gestion des incidents | Délai moyen de résolution (MTTR incidents) | < 4 h (critiques) | Mensuel |
| Sensibilisation | Taux de clic phishing simulé | < 5 % | Trimestriel |
| Sensibilisation | Taux de complétion e-learning sécurité | > 90 % | Annuel |
| Conformité | % de conformité à la PSSI (audit interne) | > 80 % | Annuel |
| Conformité | Nombre d'écarts critiques ouverts sans plan d'action | = 0 | Trimestriel |
| Disponibilité | Taux de disponibilité des services critiques | > 99,9 % | Mensuel |
| Sauvegardes | % de restaurations testées avec succès | 100 % | Semestriel |

## ▸ Structure du tableau de bord sécurité pour la direction

| Rubrique du TDB | Contenu recommandé |
|---|---|
| 1. Synthèse exécutive | Niveau de risque global (vert/orange/rouge), faits marquants du mois, 2-3 messages clés |
| 2. Faits marquants | Incidents significatifs, vulnérabilités critiques détectées, alertes CERT-FR impactantes |
| 3. KPIs clés (3-5 max) | Évolution des indicateurs essentiels avec tendance et seuil cible (graphique simple) |
| 4. Avancement roadmap | Statut des chantiers sécurité (RAG : Red/Amber/Green), jalons atteints, risques projets |
| 5. Conformité réglementaire | Statut RGPD, NIS2, audits, actions correctives ouvertes |
| 6. Décisions à prendre | Arbitrages budgétaires, validations de risques résiduels, choix stratégiques |

## ▸ Principes pour un reporting efficace

- Adapter le niveau de détail à l'audience : 1 page pour la direction, 5-10 pages pour le COMEX, détail opérationnel pour le SOC
- Préférer les visuels (courbes de tendance, jauges RAG, histogrammes) aux tableaux de chiffres bruts
- Toujours contextualiser : comparer à N-1, au benchmark sectoriel et aux objectifs fixés
- Relier les indicateurs aux risques métier : un KPI sans enjeu business ne sera pas compris

- Fréquence adaptée : mensuel pour l'opérationnel, trimestriel pour la direction, annuel pour le COMEX
- Présenter les décisions à prendre : le reporting doit déboucher sur des arbitrages, pas juste de l'information

## 📌 Mémo Récapitulatif — À Retenir

| 🏛️ Gouvernance | 🎯 Stratégie | 📋 PSSI | 📣 Sensibilisation | 📊 KPIs & TDB |
|---|---|---|---|---|
| • RSSI : conseiller stratégique DG<br>• Alignement sécurité / métier<br>• COBIT / ISO 27014 / NIST CSF<br>• Parties prenantes : DG, DSI, DPO, Audit<br>• Gouvernance = structures + processus | • 6 étapes : diag → roadmap → pilotage<br>• 4 leviers : orga / humain / tech / juridique<br>• Maturité : 5 niveaux (Initial → Optimisé)<br>• Roadmap 3 ans : CT / MT / LT<br>• ROI sécurité = coût incident vs prévention | • Approuvée par la DG, opposable<br>• 10 chapitres types<br>• Révisée tous les 2-3 ans<br>• Règle 3-2-1 pour les sauvegardes<br>• Charte signée par tous | • 80 % des incidents = facteur humain<br>• Adapter le message à la cible<br>• Formats : e-learning, phishing, ateliers<br>• Clic phishing cible < 5 %<br>• Plan annuel : diag → mesure | • KRI / KPI / KCI = 3 types<br>• TDB direction : 1 page, RAG, 5 KPIs max<br>• MTTD < 24h / MTTR critique < 4h<br>• Contextualiser vs N-1 et benchmark<br>• Reporting → décisions à prendre |