ASIN
AGENCE DES SYSTÈMES D'INFORMATION ET DU NUMÉRIQUE
RÉPUBLIQUE DU BÉNIN



GUIDE DU **RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (RSSI)**

Gouvernance, responsabilités et pilotage de la cybersécurité dans les organisations

Guide du Responsable de la sécurité des systèmes d'information (RSSI)

Gouvernance, responsabilités et pilotage de la cybersécurité dans les organisations

Réalisé par Léandre **COSSI**
Expert cybersecurité
Security Compliance Officer de la PKI nationale

Sommaire

Avant-propos 10
Public cible du guide 13
Comment utiliser ce guide 13
Parcours de lecture par profil. 14
Une idée centrale 15

1. Comprendre la fonction RSSI 17
1.1 Transformation du paysage des cybermenaces 18
1.2 La cybersécurité comme enjeu business. 18
1.3 Pourquoi la cybersécurité ne peut plus être uniquement une responsabilité technique 19
1.4 Le RSSI comme acteur de la gouvernance 20
1.5 Le coût de l'absence ou de la mauvaise structuration de la fonction RSSI. 20
1.6 Trois scénarios béninois illustratifs. 21

2. Le RSSI : rôle, mandat et responsabilités. 24
2.1 Définition du RSSI. 25
2.2 Mission fondamentale du RSSI. 25
2.3 Les grandes responsabilités du RSSI 26
2.4 Ce que le RSSI doit faire 26
2.5 Ce que le RSSI ne doit pas faire 27
2.6 RSSI vs DSI. 28
2.7 RSSI vs SOC Manager 28
2.8 RSSI vs Risk Manager 29
2.9 RSSI vs DPO (Responsable de la protection des données) 29
2.10 RSSI vs Responsable de la continuité d'activité 30
2.11 RSSI vs Auditeur interne 30
2.12 Tableau comparatif synthétique des fonctions voisines. 31

3. Le positionnement du RSSI dans l'organisation 33
3.1 Pourquoi le positionnement du RSSI est stratégique 34
3.2 Les différents modèles organisationnels. 34
3.3 Avantages et limites de chaque modèle 34
3.4 Modèle recommandé selon la taille de l'organisation 35
3.5 Autorité et indépendance du RSSI. 36
3.6 Accès du RSSI à la Direction générale 36
3.7 Accès du RSSI au Conseil d'administration / Comité d'audit 37
3.8 Charte de la fonction RSSI 37

3.9 Lettre de mission du RSSI. 38
3.10 Délégation de pouvoirs et responsabilités. 38

4. Ce que le décideur doit attendre de son RSSI 40
4.1 Pourquoi nommer un RSSI ? 41
4.2 Quel problème le RSSI doit-il résoudre ? 41
4.3 Quelles ressources faut-il mettre à sa disposition ? 41
4.4 Quels objectifs assigner au RSSI ? 42
4.5 Quels indicateurs suivre ? 43
4.6 Comment évaluer la performance d'un RSSI ? 43
4.7 Pourquoi le RSSI ne doit pas être évalué uniquement sur le nombre d'incidents 44
4.8 Les erreurs fréquentes des dirigeants vis-à-vis du RSSI. 44
4.9 Les 10 questions que tout dirigeant devrait poser à son RSSI 45

Les 10 questions et leur évaluation. 46

5. Construire et piloter le dispositif de cybersécurité 49
5.1 Stratégie de cybersécurité 50
5.2 Politique de sécurité des systèmes d'information (PSSI) 50
5.3 Politiques et procédures de sécurité 50
5.4 Comité de sécurité 51
5.5 Comité de gestion des risques 52
5.6 Rôles et responsabilités 52
5.7 Modèle des trois lignes de défense 52
5.8 Gouvernance des exceptions de sécurité 53
5.9 Gestion des risques acceptés 53

6. Gestion des risques cyber 55
6.1 Pourquoi gérer les risques ? 56
6.2 Identification des actifs. 56
6.3 Identification des menaces 56
6.4 Identification des vulnérabilités 57
6.5 Évaluation des risques 57
6.6 Traitement des risques : réduction, évitement, transfert, acceptation. 58
6.7 Registre des risques 58
6.8 Cartographie des risques cyber 58
6.9 Appétence et tolérance au risque 59
6.10 Suivi des plans de traitement 59
6.11 Méthodes et référentiels : ISO 27005, EBIOS Risk Manager, NIST, OCTAVE 60

7. Construire le socle de sécurité 63
7.1 Gestion des identités et des accès (IAM) 64
7.2 Authentification forte et MFA 64
7.3 Gestion des comptes privilégiés (PAM) 64
7.4 Sécurité réseau. 65
7.5 Sécurité des postes de travail 65

7.6 Sécurité des serveurs . . . 65
7.7 Sécurité Cloud . . . 65
7.8 Sécurité des applications . . . 66
7.9 DevSecOps . . . 66
7.10 Sécurité des bases de données . . . 66
7.11 Chiffrement et gestion des clés . . . 66
7.12 PKI et services de confiance . . . 67
7.13 Sauvegarde et restauration . . . 67
7.14 Journalisation et SIEM . . . 67
7.15 Centre des opérations de sécurité (SOC) . . . 67
7.16 Gestion des vulnérabilités . . . 68
7.17 Sécurité physique et environnementale . . . 68
7.18 Sécurité des équipements mobiles . . . 68
7.19 Sécurité de l'Internet des objets (IoT) . . . 69
7.20 Sécurité des systèmes d'intelligence artificielle . . . 69

8. Gestion des incidents et crises cyber . . . 71
8.1 Définition d'un incident . . . 72
8.2 Préparation . . . 72
8.3 Détection . . . 72
8.4 Qualification . . . 73
8.5 Containment (endiguement) . . . 73
8.6 Éradication . . . 73
8.7 Restauration . . . 73
8.8 Retour d'expérience . . . 74
8.9 Communication de crise . . . 74
8.10 Gestion des relations avec les parties prenantes de l'incident . . . 74
8.11 Cellule de crise cyber . . . 75
8.12 Plan de Réponse aux Incidents de Cybersécurité (PRIC) . . . 75
8.13 Exercices de simulation . . . 76

9. Continuité d'activité et résilience . . . 77
9.1 Analyse d'impact sur l'activité (BIA) . . . 78
9.2 Plan de continuité d'activité (PCA) . . . 78
9.3 Plan de reprise d'activité (PRA) . . . 78
9.4 RTO et RPO . . . 79
9.5 Stratégie de sauvegarde . . . 79
9.6 Résilience des infrastructures . . . 79
9.7 Scénarios de crise cyber . . . 80
9.8 Tests de PRA . . . 80
9.9 Exercices de crise . . . 80

10. Conformité et réglementation . . . 82

10.1 Pourquoi la conformité fait partie des responsabilités du RSSI . . . 83
10.2 Réglementation nationale . . . 83
10.3 Protection des données personnelles . . . 83
10.4 Cybercriminalité . . . 84
10.5 Services numériques . . . 84
10.6 Exigences sectorielles . . . 84
10.7 Normes internationales : ISO 27001, ISO 27701, NIST CSF, CIS Controls, COBIT . . . 85
10.8 Audit et certification . . . 85
10.9 Gestion des écarts de conformité . . . 86

11. Le RSSI et les ressources humaines . . . 87
11.1 Sensibilisation . . . 88
11.2 Formation . . . 88
11.3 Culture de cybersécurité . . . 88
11.4 Gestion des habilitations . . . 88
11.5 Processus d'arrivée et de départ (Onboarding / Offboarding) . . . 89
11.6 Gestion des comptes des anciens collaborateurs . . . 89
11.7 Menaces internes . . . 89
11.8 Gestion des compétences cyber . . . 90
11.9 Plan de développement des compétences . . . 90
11.10 Construire une équipe cybersécurité . . . 90

12. Le RSSI et les fournisseurs . . . 91
12.1 Pourquoi les fournisseurs constituent un risque cyber . . . 92
12.2 Due diligence sécurité . . . 92
12.3 Exigences de sécurité dans les contrats . . . 92
12.4 SLA et exigences de cybersécurité . . . 92
12.5 Audit des prestataires . . . 93
12.6 Gestion des accès des prestataires . . . 93
12.7 Cloud et externalisation . . . 93
12.8 Fin de contrat et restitution des données . . . 94

13. Pilotage et reporting du RSSI . . . 95
13.1 Pourquoi le reporting est stratégique . . . 96
13.2 Tableau de bord du RSSI . . . 96
13.3 KPI et KRI . . . 96
13.4 Indicateurs techniques versus indicateurs décisionnels . . . 97
13.5 Reporting mensuel . . . 97
13.6 Reporting trimestriel à la Direction générale . . . 97
13.7 Reporting au Conseil d'administration . . . 98
13.8 Présenter un risque cyber à un dirigeant non technique . . . 98
13.9 Transformer une vulnérabilité technique en risque business . . . 98

14. Budget et investissements cybersécurité . . . 100
14.1 Construire un budget fondé sur les risques . . . 101

14.2 CAPEX et OPEX . . . 101
14.3 Priorisation des investissements . . . 101
14.4 Construire un business case cybersécurité . . . 102
14.5 Arbitrer entre outils, services et ressources humaines . . . 102
14.6 Mesurer le retour sur investissement . . . 102
14.7 Le coût de l'inaction . . . 103

15. Le RSSI dans les organisations africaines . . . 104
15.1 Maturité cyber des organisations . . . 105
15.2 Pénurie de compétences . . . 105
15.3 Contraintes budgétaires . . . 105
15.4 Dépendance aux prestataires et technologies étrangères . . . 106
15.5 Infrastructure et connectivité . . . 106
15.6 Gouvernance et culture organisationnelle . . . 106
15.7 Sensibilisation des utilisateurs . . . 106
15.8 Cadres réglementaires africains . . . 107
15.9 Coopération régionale . . . 107
15.10 Enjeux spécifiques aux administrations publiques . . . 107
15.11 Enjeux spécifiques aux banques et institutions financières . . . 108
15.12 Enjeux des opérateurs de télécommunications . . . 108
15.13 Enjeux des infrastructures critiques . . . 108
15.14 PME : comment avoir une fonction sécurité avec des moyens limités ? . . . 109

16. Le RSSI à l'ère de l'intelligence artificielle . . . 110
16.1 L'IA comme outil d'attaque . . . 111
16.2 L'IA comme outil de défense . . . 111
16.3 Shadow AI . . . 111
16.4 Sécurité des modèles d'IA . . . 112
16.5 Protection des données utilisées par l'IA . . . 112
16.6 Gouvernance de l'IA . . . 112
16.7 Risques liés à l'IA générative . . . 113
16.8 Deepfakes et fraude . . . 113
16.9 Automatisation de la cybersécurité . . . 113
16.10 Nouvelles compétences du RSSI . . . 113
16.11 Inventaire des usages de l'IA . . . 114
16.12 Procédure d'autorisation d'un usage de l'IA . . . 114
16.13 Classification des données utilisables avec l'IA . . . 115
16.14 Grille d'évaluation des fournisseurs d'IA . . . 115
16.15 Gestion du Shadow AI . . . 116

17. Profil, compétences et carrière du RSSI . . . 117
7.1 Compétences techniques . . . 118
17.2 Compétences en gouvernance . . . 118
17.3 Compétences en gestion des risques . . . 118
17.4 Compétences en gestion financière . . . 118

17.5 Compétences en management . . . 118
17.6 Compétences en communication . . . 119
17.7 Leadership . . . 119
17.8 Négociation . . . 119
17.9 Compréhension du business . . . 119
17.10 Éthique et déontologie . . . 120
17.11 Certifications pertinentes : CISSP, CISM, CRISC, ISO 27001, etc. . . . 120
17.12 Plan de carrière du RSSI . . . 121
18. Les 100 premiers jours du RSSI . . . 122
Jours 1 à 30 — Comprendre . . . 123
Jours 31 à 60 — Diagnostiquer . . . 123
Jours 61 à 100 — Transformer . . . 123
Livrables attendus au terme des cent jours . . . 124
19. Modèle de maturité de la fonction RSSI . . . 125
Niveau 1 — Initial / Réactif . . . 126
Niveau 2 — Sensibilisé . . . 126
Niveau 3 — Structuré . . . 126
Niveau 4 — Maîtrisé . . . 126
Niveau 5 — Optimisé . . . 127
Dimensions à évaluer . . . 127
Critères objectivables et preuves attendues . . . 127
20. Boîte à outils du RSSI . . . 130
Annexes . . . 134
Annexe 1 — Glossaire cybersécurité . . . 135
Annexe 2 — Référentiels et normes . . . 137
Annexe 3 — Principales réglementations africaines et cadre béninois . . . 138
Annexe 4 — Exemple d'organigramme cybersécurité . . . 140
Annexe 5 — Exemple de tableau de bord RSSI . . . 141
Annexe 6 — Auto-évaluation du RSSI . . . 141
Annexe 7 — Auto-évaluation de l'organisation . . . 142
Annexe 8 — Checklist « Mon organisation est-elle réellement sécurisée ? » . . . 142
Annexe 9 — Tableau de bord RSSI . . . 143
Gouvernance et pilotage . . . 144
Gestion des risques . . . 144
Protection et vulnérabilités . . . 145
Gestion des incidents . . . 145
Continuité d'activité . . . 146

Conformité réglementaire 146
Sensibilisation et culture sécurité. 146
Tiers et fournisseurs 147
Ressources et budget 147
Annexe 10 — Matrices RACI de la sécurité de l'information 148

Avant-propos

Pourquoi ce guide ?

Ce guide est né d'un constat simple, répété d'une organisation à l'autre, d'un secteur à l'autre, d'un pays à l'autre : la fonction de Responsable de la Sécurité des Systèmes d'Information (RSSI) est aujourd'hui indispensable, et pourtant elle reste, dans un grand nombre d'organisations, mal comprise, mal positionnée et mal outillée. Des dirigeants nomment un RSSI sans savoir précisément ce qu'ils attendent de lui. Des RSSI prennent leurs fonctions sans lettre de mission, sans budget, sans autorité réelle, et parfois sans même un rattachement hiérarchique cohérent avec leur mandat. Des collaborateurs qui portent le titre de RSSI passent le plus clair de leur temps à des tâches d'administration technique, faute d'avoir reçu une définition claire de leur rôle de pilotage du risque numérique.

Ce guide a donc une ambition double. La première est de donner aux dirigeants, aux administrateurs et aux décideurs les clés de compréhension nécessaires pour nommer, positionner, outiller et évaluer correctement leur RSSI. La seconde est de donner aux RSSI en poste, ainsi qu'à ceux qui aspirent à le devenir, un référentiel complet leur permettant de structurer leur action, de professionnaliser leur pratique et de faire reconnaître la valeur de leur fonction. Entre ces deux publics, ce guide cherche à construire un langage commun : celui de la gouvernance du risque numérique, plutôt que celui, trop souvent réducteur, de la seule technique informatique.

Évolution de la cybersécurité et transformation du rôle du RSSI

Pendant longtemps, la sécurité informatique a été perçue comme une simple extension de la fonction informatique : un ensemble de mesures techniques — pare-feu, antivirus, sauvegardes — destinées à protéger des équipements. Cette vision, qui pouvait suffire à une époque où les systèmes d'information étaient cloisonnés et peu exposés, ne correspond plus à la réalité des organisations d'aujourd'hui. La numérisation des processus métier, la généralisation du cloud, la mobilité des collaborateurs, l'interconnexion des chaînes d'approvisionnement et la place croissante des données dans la création de valeur ont transformé le risque cyber en un risque d'entreprise à part entière, au même titre que le risque financier, le risque juridique ou le risque de réputation.

Cette transformation du risque a entraîné une transformation symétrique de la fonction chargée de le maîtriser. Le RSSI n'est plus seulement celui qui configure des équipements de sécurité : il est celui qui identifie les risques numériques susceptibles d'affecter les objectifs de l'organisation, qui propose des arbitrages à la Direction, qui pilote un dispositif de protection cohérent avec la stratégie de l'entreprise, et qui rend compte de l'exposition au risque dans un langage compréhensible par des décideurs non techniques. Ce basculement, largement acté dans les grandes organisations occidentales depuis une quinzaine d'années, reste encore en construction dans de nombreuses organisations africaines — ce qui justifie précisément l'existence de ce guide.

Enjeux spécifiques des organisations africaines

Les organisations africaines évoluent dans un contexte à la fois porteur d'opportunités et traversé de contraintes particulières. La transformation numérique y est rapide : services financiers mobiles, administrations en ligne, plateformes de commerce électronique, dématérialisation des services publics, et s'accompagne d'une exposition croissante aux cybermenaces, sans que la maturité en matière de gouvernance de la sécurité ait toujours suivi le même rythme. Dans un nombre significatif d'organisations, la fonction RSSI n'existe pas formellement, ou bien elle est confondue avec la fonction informatique, ou encore elle est confiée à titre secondaire à un responsable déjà chargé d'autres missions.

À ces réalités organisationnelles s'ajoutent des contraintes structurelles : rareté des compétences spécialisées en cybersécurité, budgets contraints, dépendance forte à des prestataires et technologies étrangères, infrastructures parfois instables, cadres réglementaires en construction et culture managériale où la sécurité est encore perçue comme une dépense plutôt que comme un investissement. Ce guide ne prétend pas ignorer ces contraintes ; il les prend au contraire comme point de départ, en proposant des repères adaptés à des organisations qui doivent structurer une fonction de sécurité avec des moyens souvent limités, sans pour autant renoncer à la rigueur méthodologique qui fait la crédibilité de la fonction RSSI dans le reste du monde.

LE CONTEXTE BÉNINOIS

Le Bénin offre un cadre de référence utile pour illustrer les principes de ce guide : une administration fortement numérisée, un cadre juridique réuni dans un code du numérique et des institutions nationales dédiées à la sécurité numérique.

Transformation numérique

- Un portail national de services publics (service-public.bj) et une stratégie de numérisation de l'administration (projet « Smart Gouv » de la stratégie numérique 2016-2021, prolongé par les programmes de gouvernance suivants) placent le numérique au cœur de la relation avec les usagers.
- Une Stratégie nationale pour l'intelligence artificielle et les mégadonnées a été adoptée en 2023 (voir chapitre 16).

Cadre juridique et réglementaire

- Code du numérique : loi n° 2017-20 du 20 avril 2018, modifiée par la loi n° 2020-35 du 6 janvier 2021. Il couvre notamment les services de confiance, la protection des données à caractère personnel (Livre V), la sécurité des systèmes d'information et la cybercriminalité.
- Politique de sécurité des systèmes d'information de l'État (PSSIE), approuvée par le décret n° 2021-550 du 27 octobre 2021.
- Règles de protection des infrastructures d'information critiques, approuvées par le décret n° 2023-060 du 22 février 2023, qui visent les opérateurs d'infrastructures d'information critiques (OIIC).
- Stratégie nationale de sécurité numérique (SNSN) : première version élaborée en 2019, mise à jour pour la période 2023-2026.
- Engagements internationaux : Convention de Malabo (signée en 2015, ratifiée en novembre 2024) et adhésion à la Convention de Budapest sur la cybercriminalité (2024).

Écosystème cyber national

- ASIN, Agence des systèmes d'information et du numérique, créée en 2022 par la fusion de plusieurs agences, dont l'ANSSI qui exerçait les missions de sécurité des systèmes d'information prévues par le Code du numérique.
- bjCSIRT, équipe nationale de réponse aux incidents de sécurité informatique, opérationnelle depuis 2017, premier point de contact des institutions de l'État en cas d'incident.
- APDP, Autorité de protection des données à caractère personnel : formalités préalables, contrôle et sanctions.
- CNIN, Centre National d'Investigation Numérique : coordination des enquêtes judiciaires.
- Les secteurs régulés (banques et établissements financiers, télécommunications) relèvent en outre de leurs autorités sectorielles.

Voir l'Annexe 3 (cadre légal et réglementaire du Bénin) et la section 8.14 (circuit de déclaration et d'escalade).

Public cible du guide

Ce guide s'adresse à plusieurs publics, dont les besoins de lecture diffèrent mais se recoupent autour d'un objectif commun : mieux comprendre, mieux positionner et mieux piloter la fonction RSSI.

- RSSI en poste et futurs RSSI, qui y trouveront un référentiel complet de leurs responsabilités, des méthodes à mobiliser et des outils à déployer ;
- Directions générales, qui y trouveront les clés pour nommer, cadrer et évaluer un RSSI, et pour comprendre ce qui relève réellement de leurs propres décisions ;
- Administrateurs et membres de Conseils d'administration, qui exercent une responsabilité de supervision du risque cyber et doivent pouvoir en discuter avec le niveau d'exigence attendu d'un organe de gouvernance ;
- Directions des systèmes d'information (DSI), avec lesquelles le RSSI entretient une relation de proximité et de complémentarité qu'il est essentiel de clarifier ;
- Directions des risques et de la conformité, dont les référentiels et méthodes recoupent largement ceux de la cybersécurité ;
- Auditeurs et contrôleurs internes, appelés à évaluer la maîtrise du risque numérique au sein de l'organisation ;
- Directions des ressources humaines, parties prenantes essentielles de la sensibilisation, du recrutement et de la gestion des compétences cyber.

Comment utiliser ce guide

Ce guide n'est pas conçu pour être lu uniquement de manière linéaire, de la première à la dernière page. Il est structuré pour permettre plusieurs niveaux de lecture, adaptés à des besoins différents. Un dirigeant pressé pourra se concentrer sur les parties consacrées au positionnement du RSSI et à ce qu'un décideur doit attendre de sa fonction sécurité, ainsi que sur les encadrés de synthèse « Ce que la Direction doit savoir » qui ouvrent chaque chapitre. Un RSSI en prise de fonction pourra, quant à lui, suivre l'ensemble du guide comme un véritable manuel de référence, et revenir régulièrement sur les parties consacrées à la gouvernance, à la gestion des risques, au pilotage et au reporting.

Chaque chapitre s'efforce d'articuler trois niveaux de lecture complémentaires : ce que la Direction doit comprendre et décider, ce que le RSSI doit mettre en œuvre en tant que responsable de la fonction, et comment cette mise en œuvre se traduit concrètement sur le plan opérationnel. Cette architecture, expliquée plus en détail ci-après, vise à éviter deux écueils fréquents dans la littérature

existante sur le sujet : un contenu trop technique pour être utile aux dirigeants, ou au contraire trop théorique pour être directement exploitable par les praticiens.

Les vingt parties de ce guide sont regroupées en six blocs qui suivent la logique d'un cycle de maîtrise du risque : comprendre, gouverner, protéger, réagir et résister, piloter, se professionnaliser et s'adapter.

Bloc	Intitulé	Parties	Lecture prioritaire pour
Bloc 1	COMPRENDRE	Parties I à IV	Direction générale, administrateurs, DSI, futurs RSSI.
Bloc 2	GOUVERNER	Parties V à VI	RSSI, Direction générale, risk managers, comités de sécurité et d'audit.
Bloc 3	PROTÉGER	Partie VII	RSSI, DSI, équipes techniques et SOC.
Bloc 4	RÉAGIR ET RÉSISTER	Parties VIII à IX	Direction générale (rôle en cellule de crise), RSSI, DSI, responsable de la continuité, communication, juridique.
Bloc 5	PILOTER	Parties X à XIV	RSSI, DPO, juridique, DRH, achats, direction financière, Direction générale.
Bloc 6	SE PROFESSIONNALISER ET S'ADAPTER	Parties XV à XX	RSSI en poste ou futurs RSSI, Direction générale, organismes de formation.

Parcours de lecture par profil

Le tableau suivant permet à chaque lecteur d'aller directement à ce qui le concerne. Les parcours sont des suggestions : tout lecteur peut, bien entendu, élargir sa lecture.

Profil	À lire en priorité	Puis, selon les besoins
Dirigeant, Directeur général	Encadrés « Ce que la Direction doit savoir » ; Partie III ; Partie IV (dont 4.9) ; 8.11 ; Annexe 8	Chapitres 13 et 14 ; Partie X ; section 1.6
Administrateur, membre du comité d'audit	Chapitre 1 ; 3.7 ; 5.5 à 5.9 ; chapitre 13 ; Partie XIX	Chapitres 10 et 16 ; Annexe 9
DSI	2.6 ; 3.3 et 3.4 ; Partie VII ; chapitres 8 et 9	Chapitre 12 ; Annexe 10
RSSI en poste	L'ensemble du guide, en commençant par les Parties II, V, VI et VIII	Annexes 6, 9 et 10
RSSI en prise de fonction	Chapitre 18 ; Parties II et III ; chapitre 19	Chapitres 5, 6 et 13
DPO, juridique, conformité	2.9 ; Partie X ; 8.14 ; Annexe 3	Chapitre 12 ; chapitre 16
Risk manager, audit interne	2.8 et 2.11 ; Partie V ; Partie VI ; chapitre 19	Annexes 2 et 10
Direction des ressources humaines	Chapitre 11 ; 2.5 ; Annexe 10 (matrice RH)	Chapitre 17
PME ou petite structure	1.2 ; 3.4 ; section PME du chapitre 15 ; chapitre 18	Chapitres 6, 7 et 9

Une idée centrale

Au terme de ce parcours à travers l'ensemble des dimensions de la fonction, ce guide entend défendre une idée centrale, qui en constitue le fil conducteur : le RSSI n'est ni le « policier informatique » de l'organisation, chargé de sanctionner les manquements des utilisateurs, ni le technicien censé résoudre personnellement l'ensemble des problèmes de sécurité rencontrés. Il est le responsable de la maîtrise du risque numérique de l'organisation, et le conseiller de sa Direction en la matière, une fonction de gouvernance à part entière, dont la valeur se mesure à la qualité des décisions qu'elle éclaire, bien davantage qu'au nombre d'incidents qu'elle parvient, ou non, à empêcher.

Cette distinction entre responsabilité technique, responsabilité opérationnelle et responsabilité de gouvernance, développée tout au long de ce guide, constitue la clé de la professionnalisation et de la valorisation de la fonction RSSI. Elle s'adresse autant aux dirigeants, appelés à nommer, positionner et outiller correctement cette fonction, qu'aux RSSI eux-mêmes, invités à structurer leur action autour de cette vision élargie de leur rôle. C'est à cette double condition, une Direction qui comprend ce qu'elle doit attendre de son RSSI, et un RSSI qui exerce pleinement son rôle de gouvernance que la cybersécurité pourra occuper, dans les organisations africaines comme ailleurs, la place stratégique qui doit désormais être la sienne.



1

BLOC 1

Comprendre

Parties I à IV

Ce premier bloc répond à trois questions : pourquoi la fonction RSSI est devenue stratégique, qui est le RSSI (et qui il n'est pas), et comment le positionner dans l'organisation. Il se conclut par un guide à l'attention des dirigeants : ce qu'ils doivent attendre de leur RSSI et comment le lui demander.

Lecture prioritaire pour : Direction générale, administrateurs, DSI, futurs RSSI.

Partie	Contenu	Niveau principal
I	Comprendre la fonction RSSI (chapitre 1)	Décider
II	Le RSSI : rôle, mandat et responsabilités (chapitre 2)	Décider / Piloter
III	Le positionnement du RSSI dans l'organisation (chapitre 3)	Décider
IV	Ce que le décideur doit attendre de son RSSI (chapitre 4)	Décider

I

Comprendre la fonction RSSI

Pourquoi la fonction RSSI est devenue stratégique

CE QUE LA DIRECTION DOIT SAVOIR

1. La cybersécurité n'est plus un sujet technique : c'est un risque d'entreprise qui engage la continuité, la réputation et la responsabilité des dirigeants.
2. L'absence d'un pilotage structuré de ce risque expose l'organisation à des pertes financières, réglementaires et réputationnelles potentiellement majeures.
3. La Direction doit s'assurer qu'un responsable identifié, doté d'une autorité réelle, porte ce sujet au plus haut niveau de décision.

1.1 Transformation du paysage des cybermenaces

Le paysage des cybermenaces a connu, au cours de la dernière décennie, une transformation à la fois quantitative et qualitative. Sur le plan quantitatif, le nombre d'attaques recensées dans le monde ne cesse de croître, porté par la professionnalisation de la cybercriminalité, qui fonctionne désormais selon une logique d'écosystème économique structuré : développeurs de rançongiciels, courtiers en accès initiaux, plateformes de revente de données volées, et services de « ransomware-as-a-service » accessibles à des acteurs peu qualifiés techniquement. Cette industrialisation de la menace signifie qu'aucune organisation, quelle que soit sa taille ou son secteur, ne peut plus se considérer comme non exposée.

Sur le plan qualitatif, les modes opératoires se sont diversifiés et sophistiqués. Le rançongiciel (ransomware) demeure la menace la plus visible et la plus coûteuse : il combine désormais chiffrement des données et exfiltration préalable, dans une logique de double extorsion qui rend la simple restauration de sauvegardes insuffisante pour se prémunir des conséquences d'une attaque. La fraude et l'ingénierie sociale, hameçonnage, compromission de messagerie professionnelle, usurpation d'identité de dirigeants, exploitent la vulnérabilité humaine plutôt que la vulnérabilité technique, et représentent une part croissante des pertes financières directement imputables à des incidents cyber. La compromission des identités, facilitée par la réutilisation de mots de passe et l'absence d'authentification forte, constitue le point d'entrée privilégié d'un nombre croissant d'intrusions.

À ces menaces s'ajoutent les menaces internes, qu'elles soient malveillantes ou simplement négligentes, les attaques visant les infrastructures critiques (énergie, télécommunications, services financiers, administrations), particulièrement sensibles dans le contexte africain où ces secteurs connaissent une numérisation accélérée, ainsi que les attaques par la chaîne d'approvisionnement (supply chain attacks), qui consistent à compromettre un fournisseur ou un éditeur logiciel pour atteindre indirectement ses clients. Enfin, l'essor de l'intelligence artificielle générative introduit une nouvelle catégorie de menaces : automatisation des campagnes d'hameçonnage, génération de contenus frauduleux crédibles, et usage de deepfakes à des fins d'usurpation d'identité ou de fraude au dirigeant. Cette évolution rapide et continue du paysage des menaces impose une veille permanente, que seule une fonction dédiée et structurée peut assurer dans la durée.

1.2 La cybersécurité comme enjeu business

La cybersécurité ne peut plus être analysée comme une contrainte technique périphérique : elle conditionne directement la capacité de l'organisation à atteindre ses objectifs stratégiques. La continuité d'activité en est l'illustration la plus immédiate : une attaque par rançongiciel qui paralyse les systèmes d'information peut interrompre la production, la facturation, les paiements ou la délivrance de services publics pendant des jours, voire des semaines, avec des conséquences économiques directement proportionnelles à la durée de l'interruption. La protection des données : données clients, données financières, secrets industriels, données personnelles des employés, constitue un second

enjeu majeur, tant la valeur économique et la sensibilité de ces informations ne cessent de croître.

La réputation et la confiance des clients représentent un troisième enjeu, souvent sous-estimé dans son ampleur réelle : une fuite de données ou un incident rendu public peut durablement affecter la confiance des clients, des partenaires et des investisseurs, avec des conséquences commerciales qui excèdent largement le coût technique de l'incident lui-même. La conformité réglementaire constitue un enjeu croissant, à mesure que les cadres légaux relatifs à la protection des données personnelles et à la cybersécurité se développent sur le continent africain, exposant les organisations non conformes à des sanctions financières et administratives.

Enfin, le risque financier, le risque juridique et le risque stratégique se trouvent directement engagés par une mauvaise maîtrise du risque cyber : coûts de remédiation, rançons éventuellement versées, pertes d'exploitation, actions en responsabilité de la part de clients ou de partenaires lésés, et, dans les cas les plus graves, remise en cause de la viabilité même du modèle économique de l'organisation. C'est cette convergence entre risque numérique et risque d'entreprise qui justifie que la cybersécurité soit désormais traitée comme un sujet de gouvernance, et non comme une simple ligne budgétaire de la direction informatique.

1.3 Pourquoi la cybersécurité ne peut plus être uniquement une responsabilité technique

Confier la cybersécurité à la seule responsabilité technique de la direction informatique revient à confondre la mise en œuvre d'un dispositif avec le pilotage du risque qu'il est censé maîtriser. Une direction informatique a naturellement vocation à privilégier la disponibilité et la performance des systèmes, ainsi que la rapidité de mise en œuvre des projets numériques — des objectifs qui peuvent, dans certaines circonstances, entrer en tension avec des exigences de sécurité perçues comme un frein. Cette tension structurelle explique pourquoi les référentiels de gouvernance recommandent, dès que la taille, la criticité ou la maturité de l'organisation le justifient, une séparation claire entre la fonction qui construit et exploite les systèmes d'information (la DSI) et la fonction qui définit les exigences de sécurité et en contrôle le respect (le RSSI).

Cette séparation ne traduit pas une défiance envers la DSI, mais répond à un principe de gouvernance élémentaire : celui qui est responsable de la performance opérationnelle d'un système ne peut être simultanément seul juge de son niveau de sécurité, sans risquer un conflit d'intérêts, même involontaire. Le RSSI apporte un regard indépendant, centré sur la maîtrise du risque, et une capacité à faire remonter à la Direction des arbitrages qui dépassent le seul périmètre technique — par exemple lorsqu'un investissement de sécurité doit être priorisé au détriment d'un projet métier, ou lorsqu'un risque doit être formellement accepté au plus haut niveau de l'organisation.

1.4 Le RSSI comme acteur de la gouvernance

Placer le RSSI au rang d'acteur de la gouvernance signifie reconnaître que sa mission dépasse la mise en œuvre de mesures techniques pour englober la structuration même de la manière dont l'organisation décide, arbitre et rend compte en matière de risque numérique. À ce titre, le RSSI contribue à la définition de la stratégie de cybersécurité, propose les politiques et procédures qui l'encadrent, anime les instances de gouvernance dédiées (comité de sécurité, comité des risques), et alimente les organes de direction et de supervision — comité de direction, comité d'audit, conseil d'administration — en informations leur permettant d'exercer une décision éclairée.

Cette dimension de gouvernance suppose que le RSSI dispose d'une autorité et d'une indépendance suffisantes pour exercer un contrôle crédible, y compris, le cas échéant, vis-à-vis de la direction informatique elle-même. Elle suppose également que la Direction générale et le Conseil d'administration reconnaissent explicitement le RSSI comme un interlocuteur de gouvernance à part entière, et non comme un simple prestataire technique interne. Ces questions de positionnement organisationnel, essentielles à l'efficacité réelle de la fonction, sont développées en détail dans la Partie III de ce guide.

Cette exigence d'indépendance doit toutefois être comprise de manière proportionnée. Elle ne se réduit pas à un organigramme : elle repose sur trois garanties que toute organisation, quelle que soit sa taille, peut assurer, l'indépendance de jugement du RSSI dans son appréciation du risque, un droit d'alerte formalisé à l'égard de la Direction générale, et un accès direct au niveau décisionnel approprié à la gravité du sujet. La forme que prend la séparation entre DSI et RSSI (rattachement distinct, modèle matriciel ou, dans les petites structures, fonction partagée assortie de garde-fous) dépend de la criticité des activités, de la taille et de la maturité de l'organisation, comme le détaille la section 3.4.

1.5 Le coût de l'absence ou de la mauvaise structuration de la fonction RSSI

L'absence d'une fonction RSSI clairement définie, ou sa mauvaise structuration, a un coût qui, bien que souvent invisible tant qu'aucun incident majeur ne survient, se révèle considérable lorsque le risque se matérialise. Ce coût se manifeste d'abord par une absence de vision globale du risque numérique : sans responsable identifié et mandaté, les décisions de sécurité sont prises de manière fragmentée, projet par projet, sans cohérence d'ensemble ni priorisation fondée sur une analyse de risque structurée. Il en résulte typiquement une allocation de ressources déséquilibrée, avec des investissements importants sur certains sujets visibles et une exposition non maîtrisée sur d'autres, souvent plus critiques mais moins apparents.

Ce coût se manifeste également par une moindre capacité de détection et de réponse aux incidents : en l'absence d'un dispositif de pilotage structuré, les incidents sont détectés plus tardivement, traités de manière improvisée, et donnent lieu à une communication de crise défaillante, aggravant les conséquences réputationnelles et réglementaires. Il se traduit enfin par une vulnérabilité accrue

face aux exigences de conformité, aux exigences contractuelles des partenaires et clients internationaux, et aux attentes croissantes des régulateurs — autant de facteurs qui peuvent, dans certains secteurs, conditionner l'accès à des marchés ou à des financements. Structurer correctement la fonction RSSI n'est donc pas une dépense discrétionnaire : c'est un investissement dont le coût de renoncement, bien que difficile à chiffrer a priori, se révèle systématiquement supérieur au coût de sa mise en place.

1.6 Trois scénarios béninois illustratifs

Pour rendre concrets les enjeux de gouvernance décrits dans ce chapitre, trois scénarios types sont proposés, situés dans des secteurs structurants de l'économie béninoise : l'administration publique, les services financiers et de paiement, et la santé. Chacun met en évidence les décisions que la Direction aurait à prendre et renvoie aux sections du guide qui y répondent.



SCÉNARIO A — UNE ADMINISTRATION PUBLIQUE

Contexte. Un ministère propose des démarches en ligne aux usagers et gère un fichier d'agents et d'usagers. L'équipe informatique est réduite et l'hébergement est confié à un prestataire.

Scénario. Des agents reçoivent un courriel d'hameçonnage imitant une communication institutionnelle. Plusieurs comptes sont compromis, dont un compte aux droits étendus sur la plateforme. L'attaquant consulte et exporte des dossiers d'usagers pendant plusieurs jours sans être détecté, faute de journalisation centralisée.

Décisions de gouvernance. Qui décide de suspendre le service ? Qui informe la hiérarchie, le bjCSIRT et, s'agissant de données personnelles, l'APDP ? Qui s'adresse aux usagers ?

Ce que le guide apporte. Authentification forte et comptes à privilèges (7.2, 7.3) ; journalisation et détection (7.14) ; circuit de déclaration (8.14) ; coordination RSSI–DPO (2.9) ; pouvoirs d'urgence délégués (3.10).



SCÉNARIO B — UNE BANQUE ET UN SERVICE DE PAIEMENT MOBILE

Contexte. Un établissement financier et un opérateur de paiement mobile partagent une interface d'échange. Les services sont ouverts 24 h sur 24.

Scénario. Une campagne de fraude combine hameçonnage ciblé d'agents de distribution, usurpation d'identité et exploitation d'un accès de prestataire insuffisamment contrôlé. Des opérations frauduleuses sont initiées pendant un week-end ; le SOC externalisé escalade tardivement.

Décisions de gouvernance. Faut-il couper un service critique au prix d'un impact sur les clients ? Qui déclare à l'autorité sectorielle ? Que prévoit le contrat avec le prestataire et le SOC ? Comment informer les clients ?

Ce que le guide apporte. Matrice des pouvoirs d'urgence (3.10) ; gouvernance des tiers (12.2 à 12.6) ; astreinte et escalade (8.3, 8.4) ; indicateurs de détection et de réponse (Annexe 9).



SCÉNARIO C — UN CENTRE HOSPITALIER

Contexte. Un hôpital a numérisé les dossiers patients, l'imagerie et la facturation. Les sauvegardes sont stockées sur le même réseau que la production.

Scénario. Un rançongiciel chiffre le serveur de dossiers et une partie des sauvegardes ; les soins se poursuivent en mode papier. Des données de santé, catégorie sensible de données personnelles, ont pu être exfiltrées.

Décisions de gouvernance. Quand et comment remettre les systèmes en service ? Quelles notifications (APDP, personnes concernées) ? Faut-il déposer plainte ? Que dire aux patients et au personnel ?

Ce que le guide apporte. Sauvegardes isolées et testées (7.13, 9.5) ; PCA, PRA et mode dégradé (9.2, 9.3) ; notification des violations de données (2.9, 8.14) ; exercices de crise (8.13).

II

PARTIE II · CHAPITRE 2

Le RSSI : rôle, mandat et responsabilités

Qui est le RSSI ?

CE QUE LA DIRECTION DOIT SAVOIR

1. Le RSSI est le responsable de la maîtrise du risque numérique de l'organisation, et le conseiller de la Direction en la matière — pas l'exécutant technique de la sécurité.

2. Sa mission se distingue clairement de celle de la DSI, du SOC Manager, du Risk Manager, du DPO, du responsable de continuité d'activité et de l'auditeur interne.

3. Confondre ces fonctions est l'une des erreurs de gouvernance les plus fréquentes et les plus coûteuses observées dans les organisations.

2.1 Définition du RSSI

Le Responsable de la Sécurité des Systèmes d'Information, communément désigné par l'acronyme RSSI (en anglais Chief Information Security Officer, CISO), est le responsable désigné de la définition, du pilotage de la mise en œuvre, du contrôle et de l'amélioration continue de la politique de sécurité de l'information au sein d'une organisation. Il n'est ni un administrateur système, ni un ingénieur réseau, ni un simple expert technique : il est le point focal de la gouvernance du risque numérique, chargé d'assurer que l'ensemble des risques liés à l'information et aux systèmes qui la traitent sont identifiés, évalués, traités et communiqués de manière cohérente à l'échelle de l'organisation.

Cette définition, en apparence simple, porte en elle une distinction essentielle que ce guide s'attache à développer tout au long de ses pages : le RSSI n'est pas celui qui « fait » la sécurité au sens de sa mise en œuvre technique quotidienne, cette responsabilité incombe le plus souvent à la DSI et aux équipes opérationnelles de sécurité (SOC, administrateurs, ingénieurs), mais celui qui définit ce qui doit être fait, pourquoi, avec quelles priorités, et qui vérifie que cela est effectivement réalisé. Cette distinction entre le « quoi » et le « comment », entre la gouvernance et l'exécution, est au cœur de la professionnalisation de la fonction RSSI.

2.2 Mission fondamentale du RSSI

La mission fondamentale du RSSI peut se résumer en une phrase : garantir que l'organisation maîtrise, à un niveau acceptable pour sa Direction, les risques liés à la sécurité de son information et de ses systèmes. Cette mission se décline en plusieurs objectifs permanents :

- protéger la disponibilité, l'intégrité et la confidentialité de l'information, en y ajoutant explicitement l'authenticité et la traçabilité lorsque le contexte réglementaire ou métier l'exige (preuve électronique, signature, journalisation, transactions financières, services publics en ligne) ;
- assurer la résilience de l'organisation face aux incidents et aux crises cyber ;
- garantir la conformité aux obligations légales, réglementaires et contractuelles applicables ;
- contribuer à instaurer une culture de la sécurité partagée par l'ensemble des collaborateurs.

Au-delà de ces objectifs opérationnels, la mission du RSSI comporte une dimension de conseil et d'éclairage de la décision : il doit être en mesure de traduire des risques techniques en enjeux compréhensibles par des décideurs non spécialistes, de proposer des arbitrages fondés sur une analyse de risque rigoureuse, et d'accompagner l'organisation dans ses choix stratégiques — transformation numérique, migration vers le cloud, ouverture de nouveaux services digitaux — en intégrant la dimension sécurité dès la conception, plutôt qu'en la traitant comme une contrainte a posteriori.

2.3 Les grandes responsabilités du RSSI

Les responsabilités du RSSI s'organisent autour de dix grands domaines, développés en détail dans les parties suivantes de ce guide, mais qu'il convient d'introduire ici comme cartographie d'ensemble de la fonction. Le tableau suivant constitue le référentiel de responsabilités du RSSI : pour chaque domaine, il précise la responsabilité attendue et les livrables que la Direction est en droit d'exiger.

Domaine	Responsabilité du RSSI	Livrables attendus	Voir
Gouvernance	Définir la stratégie de sécurité, animer les instances dédiées, rendre compte à la Direction et au Conseil	Stratégie cyber pluriannuelle ; calendrier et comptes rendus du comité de sécurité ; reporting trimestriel à la Direction	Parties V, XIII
Gestion des risques	Identifier, évaluer, traiter et suivre les risques liés à l'information et aux systèmes	Registre et cartographie des risques ; plans de traitement ; registre des risques acceptés	Partie VI
Politique de sécurité	Élaborer et faire approuver le corpus documentaire encadrant la sécurité de l'information	PSSI approuvée ; politiques thématiques et procédures ; registre des dérogations	5.2, 5.3, 5.8
Protection des actifs	Définir les exigences de protection des données, applications, infrastructures et équipements	Exigences de sécurité par domaine ; revues de sécurité des projets ; tableau de couverture des mesures	Partie VII
Gestion des incidents	Préparer, détecter, qualifier et piloter la réponse aux incidents de sécurité	Plan de réponse aux incidents de cybersécurité testé ; grille de criticité ; registre des incidents ; retours d'expérience ; circuit de déclaration	Partie VIII
Continuité d'activité	Contribuer à la résilience de l'organisation face aux scénarios de crise cyber	Scénarios cyber intégrés au BIA, au PCA et au PRA ; comptes rendus de tests de restauration et d'exercices	Partie IX
Conformité	S'assurer du respect des obligations légales, réglementaires, sectorielles et contractuelles	Registre des oblig ; suivi des écarts	Partie X
Sensibilisation	Développer la culture de sécurité et les compétences des collaborateurs	Plan annuel de sensibilisation ; campagnes et indicateurs ; parcours de formation	Partie XI
Pilotage des fournisseurs	Maîtriser le risque cyber lié aux tiers et prestataires	Grille d'évaluation ; clauses de sécurité types ; revue annuelle des fournisseurs critiques	Partie XII
Veille et anticipation	Suivre l'évolution des menaces, des technologies et des référentiels	Note de veille périodique ; alertes traitées (dont bulletins du bjCSIRT) ; mise à jour des référentiels	15.9, chap. 16

2.4 Ce que le RSSI doit faire

Le RSSI doit, en premier lieu, construire et faire vivre une vision claire et documentée des risques numériques de l'organisation, actualisée régulièrement et partagée avec la Direction. Il doit définir un corpus de politiques et de règles de sécurité proportionné aux enjeux réels de l'organisation, ni excessivement contraignant au point d'entraver l'activité, ni insuffisant au point de laisser des risques majeurs sans traitement. Il doit piloter, sans nécessairement exécuter lui-même, la mise en œuvre des mesures de sécurité, en s'assurant que les équipes techniques disposent des moyens et des priorités nécessaires pour les déployer.

Il doit également organiser la capacité de détection et de réponse aux incidents, entretenir des relations de qualité avec l'ensemble des parties prenantes internes et externes concernées par la sécurité, rendre compte régulièrement à la Direction générale et, le cas échéant, au Conseil d'administration, et enfin exercer une veille active sur l'évolution des menaces et des exigences réglementaires. Dans l'ensemble de ces missions, le RSSI agit comme un chef d'orchestre du risque numérique, davantage que comme un exécutant technique isolé.

2.5 Ce que le RSSI ne doit pas faire

À l'inverse, plusieurs pratiques, bien que fréquemment observées, s'écartent du mandat propre du RSSI et fragilisent à terme la crédibilité et l'efficacité de la fonction. Le RSSI ne doit pas être le seul responsable opérationnel de l'administration quotidienne des équipements de sécurité : pare-feu, antivirus, systèmes de détection ; cette responsabilité relevant normalement des équipes techniques de la DSI ou du SOC, sous le contrôle du RSSI. Il ne doit pas non plus être positionné comme le « policier » chargé de sanctionner les utilisateurs, une posture qui nuit à l'adhésion des collaborateurs et détourne la fonction de son rôle véritable de conseiller et de facilitateur de la maîtrise du risque.

POINT IMPORTANT

Le RSSI ne doit pas être confondu avec l'administrateur systèmes, le responsable réseau ou le responsable IT. Ces fonctions relèvent de la mise en œuvre technique ; le RSSI relève de la définition des exigences et du contrôle de leur application.

Le RSSI ne doit pas davantage être seul décisionnaire sur l'acceptation d'un risque majeur : cette décision relève de la Direction générale, éventuellement du Conseil d'administration, le RSSI ayant pour rôle d'éclairer cette décision et d'en assurer la traçabilité. Enfin, le RSSI ne doit pas porter seul la responsabilité de la sécurité de l'organisation : la sécurité de l'information est une responsabilité partagée par l'ensemble des directions et des collaborateurs, le RSSI en étant l'animateur et le garant méthodologique, non l'unique responsable en cas de défaillance.

Au-delà de l'acceptation des risques majeurs, plusieurs sujets ne devraient jamais reposer sur le seul RSSI. Le tableau suivant précise, pour chacun, qui décide ou assume, et quel est le rôle du RSSI. Cette clarification protège autant l'organisation que le RSSI lui-même.

Sujet	Qui décide ou assume	Rôle du RSSI
Acceptation d'un risque	Direction générale pour les risques majeurs ; directeur de l'entité pour les risques modérés ; Conseil au-delà des seuils fixés	Éclairer la décision, la documenter et tenir le registre des risques acceptés
Sanctions disciplinaires	Direction des ressources humaines et Direction générale, selon le règlement intérieur et le droit du travail	Fournir les faits techniques et la qualification de l'incident, sans instruire ni prononcer de sanction
Conformité juridique globale	Direction juridique, fonction conformité et DPO (données personnelles)	Traduire les obligations en exigences de sécurité et contrôler leur mise en œuvre

Sujet	Qui décide ou assume	Rôle du RSSI
Continuité d'activité métier	Directions métier et responsable de la continuité	Contribuer aux scénarios cyber et à la reprise des systèmes ; ne pas porter la continuité des processus métier
Sécurité au quotidien	Chaque direction et chaque collaborateur	Animer, outiller et contrôler

2.6 RSSI vs DSI

La relation entre le RSSI et la Direction des systèmes d'information (DSI) est probablement la plus structurante, et la plus souvent source de confusion, de l'ensemble des relations fonctionnelles du RSSI. La DSI a pour mission de construire, exploiter et faire évoluer les systèmes d'information au service des besoins métier de l'organisation, avec des impératifs de performance, de disponibilité et de délais. Le RSSI, quant à lui, a pour mission de définir les exigences de sécurité que ces systèmes doivent respecter, et de contrôler que ces exigences sont effectivement appliquées.

Cette distinction fonctionnelle conduit les référentiels de gouvernance à insister sur l'indépendance du RSSI vis-à-vis de la fonction qu'il est chargé de contrôler. Ce qui importe, plus que le schéma hiérarchique lui-même, c'est que trois garanties soient effectivement réunies : l'indépendance de jugement, le droit d'alerte et l'accès direct au niveau décisionnel approprié. Lorsque ces garanties sont assurées, plusieurs schémas peuvent être admissibles selon la criticité des activités, la taille et la maturité de l'organisation ; lorsqu'elles ne le sont pas, un rattachement à la DSI crée un risque de conflit d'intérêts, la DSI pouvant être tentée d'arbitrer en faveur de la performance ou des délais au détriment d'exigences de sécurité qu'elle serait simultanément chargée de contrôler elle-même. Cette question de rattachement organisationnel est développée dans la Partie III de ce guide (voir notamment la section 3.4). En pratique, RSSI et DSI doivent entretenir une relation de collaboration étroite et quotidienne, fondée sur la clarté des rôles : le RSSI définit et contrôle, la DSI met en œuvre et exploite.

2.7 RSSI vs SOC Manager

Le SOC Manager (Security Operations Center Manager) est responsable du pilotage opérationnel du centre des opérations de sécurité, chargé de la surveillance continue des systèmes, de la détection des incidents et de la réponse de premier niveau. Il s'agit d'une fonction opérationnelle et technique, centrée sur l'exécution du dispositif de détection et de réponse défini par le RSSI. Le RSSI, en revanche, définit la stratégie de détection et de réponse aux incidents, fixe les priorités et les niveaux de service attendus du SOC, et porte la responsabilité de rendre compte à la Direction de l'efficacité globale du dispositif.

Dans les organisations de taille suffisante pour disposer d'un SOC dédié — interne ou externalisé — le SOC Manager rapporte fonctionnellement au RSSI, qui reste responsable in fine de la performance du dispositif de détection et de réponse, même lorsque son exécution quotidienne est déléguée. Dans les organisations de taille plus modeste, ces deux fonctions peuvent être exercées par une même

personne, à condition que cette double casquette n'occulte pas la nécessité, pour le RSSI, de conserver une vision de gouvernance au-delà du seul pilotage opérationnel.

2.8 RSSI vs Risk Manager

Le Risk Manager (responsable de la gestion des risques) a pour mission de piloter l'ensemble des risques de l'organisation — financiers, opérationnels, juridiques, réputationnels — dans une approche intégrée de gestion des risques d'entreprise (Enterprise Risk Management). Le RSSI, quant à lui, se concentre spécifiquement sur les risques liés à l'information et aux systèmes qui la traitent. Ces deux fonctions doivent collaborer étroitement, le risque cyber constituant l'une des composantes majeures du profil de risque global de l'organisation, et devant à ce titre être intégré dans les registres et les instances de gouvernance des risques de l'entreprise.

Dans les organisations dotées d'une fonction de gestion des risques structurée, le RSSI alimente le dispositif global de gestion des risques avec son expertise spécifique au domaine cyber, tout en conservant la responsabilité opérationnelle du traitement de ces risques. Cette articulation, développée plus en détail dans la Partie VI de ce guide consacrée à la gestion des risques cyber, évite tant la duplication des dispositifs que l'isolement du risque cyber par rapport à la cartographie globale des risques de l'organisation.

2.9 RSSI vs DPO (Responsable de la protection des données)

Le Délégué à la Protection des Données (DPO), fonction dont la reconnaissance se développe progressivement dans les cadres réglementaires africains à mesure que se multiplient les lois de protection des données à caractère personnel, a pour mission de veiller à la conformité du traitement des données personnelles par l'organisation, et de constituer le point de contact avec les autorités de protection des données et les personnes concernées. Cette mission, de nature principalement juridique et de conformité, se distingue de celle du RSSI, dont le périmètre couvre l'ensemble de l'information de l'organisation — pas seulement les données à caractère personnel — sous l'angle de la sécurité technique et organisationnelle.

Ces deux fonctions sont néanmoins fortement complémentaires : la protection des données personnelles repose largement sur des mesures de sécurité — chiffrement, contrôle d'accès, journalisation — dont la définition et le contrôle relèvent du RSSI, tandis que la qualification juridique des traitements, la gestion des consentements et des droits des personnes, et les relations avec les autorités de contrôle relèvent du DPO. Une collaboration étroite entre RSSI et DPO, formalisée par des points de coordination réguliers, est indispensable pour éviter tout angle mort dans la protection des données personnelles de l'organisation.

CONTEXTE BÉNINOIS — PROTECTION DES DONNÉES, APDP ET COORDINATION

La protection des données à caractère personnel relève du Livre V du Code du numérique (loi n° 2017-20 du 20 avril 2018, modifiée en 2021) et est supervisée par l'APDP, Autorité de protection des données à caractère personnel. Les traitements sont soumis à des formalités préalables auprès de l'APDP, qui dispose de pouvoirs de contrôle, d'injonction et de sanction.

L'article 427 prévoit que le responsable du traitement notifie sans délai, à l'APDP et à la personne concernée, toute rupture de la sécurité ayant affecté ses données personnelles, et que le sous-traitant avertit sans délai le responsable du traitement. Le texte retient la formule « sans délai » ; l'organisation a intérêt à fixer en interne un délai cible court et documenté.

La désignation et le rôle d'un délégué ou correspondant à la protection des données doivent être vérifiés au regard des dispositions applicables et des orientations publiées par l'APDP.

Qui fait quoi en cas de violation de données personnelles

- RSSI : détecte, qualifie techniquement l'incident, évalue les données touchées, préserve la preuve.
- DPO : qualifie la violation au regard de la réglementation, évalue le risque pour les personnes, prépare les notifications.
- Juridique : valide les termes des notifications et la stratégie vis-à-vis des autorités.
- Direction générale : décide de la notification et de la communication externe, sur proposition du RSSI et du DPO.

Cette coordination gagne à être formalisée par des points réguliers et par la matrice RACI « protection des données » de l'Annexe 10.

2.10 RSSI vs Responsable de la continuité d'activité

Le Responsable de la continuité d'activité (Business Continuity Manager) a pour mission d'assurer que l'organisation dispose des dispositifs nécessaires pour maintenir ou reprendre rapidement ses activités critiques en cas de sinistre majeur, qu'il soit d'origine cyber, naturelle, sanitaire ou autre. Le RSSI se concentre spécifiquement sur les scénarios de sinistre d'origine cyber et sur la dimension technique de la reprise des systèmes d'information, tandis que le responsable de la continuité d'activité porte une vision plus large, englobant l'ensemble des processus métier, des ressources humaines, des locaux et des chaînes d'approvisionnement.

La coordination entre ces deux fonctions est particulièrement critique lors de l'élaboration du Plan de Continuité d'Activité (PCA) et du Plan de Reprise d'Activité (PRA), documents qui doivent intégrer les scénarios de crise cyber aux côtés des autres scénarios de sinistre, ainsi que lors de la conduite d'exercices de simulation de crise. Cette articulation est développée en détail dans la Partie IX de ce guide.

2.11 RSSI vs Auditeur interne

L'auditeur interne a pour mission d'évaluer, de manière indépendante et objective, l'efficacité des dispositifs de contrôle interne et de gestion des risques de

l'organisation, y compris en matière de sécurité de l'information. Cette fonction relève de la troisième ligne de défense, selon le modèle des trois lignes de défense développé dans la Partie V de ce guide, et se distingue fondamentalement du RSSI, qui relève de la deuxième ligne de défense en tant que fonction de définition et de contrôle des politiques de sécurité.

Cette distinction est essentielle sur le plan de la gouvernance : l'auditeur interne évalue, de manière indépendante, la qualité du dispositif que le RSSI a mis en place et pilote. Un RSSI ne saurait être son propre auditeur, sous peine de compromettre l'objectivité de l'évaluation. La relation entre RSSI et audit interne doit néanmoins être constructive : les recommandations d'audit constituent pour le RSSI une source précieuse d'amélioration continue de son dispositif, et une légitimité supplémentaire pour obtenir les ressources nécessaires à la remédiation des faiblesses identifiées.

2.12 Tableau comparatif synthétique des fonctions voisines

Les sections 2.6 à 2.11 ont distingué le RSSI de six fonctions voisines. Le tableau ci-dessous en propose une synthèse comparative, à utiliser comme grille de lecture lors de la rédaction de la charte, de la lettre de mission et des matrices RACI (Annexe 10). Les rattachements indiqués sont des possibilités, à arbitrer selon la taille, la criticité et la maturité de l'organisation.

Fonction	Mission	Responsabilité	Décision	Exécution	Contrôle	Rattachement possible
RSSI	Définir, piloter la mise en œuvre, contrôler et améliorer la sécurité de l'information	Maîtrise du risque numérique : cadre, exigences, reporting	Exigences de sécurité ; exceptions mineures ; mesures d'urgence déléguées	Animation du dispositif et pilotage des plans d'action (mise en œuvre confiée à la DSI et aux métiers)	Contrôle de deuxième ligne	Direction générale (recommandé), Direction des risques ou modèle matriciel ; DSI sous garanties d'indépendance (3.4)
DSI	Construire, exploiter et faire évoluer les systèmes d'information	Disponibilité, performance, délais, mise en œuvre technique	Choix d'architecture et d'exploitation, dans le respect des exigences de sécurité	Exécution principale des mesures techniques	Contrôle de première ligne sur ses opérations	Direction générale ou direction générale adjointe
SOC Manager	Surveiller, détecter, répondre au premier niveau	Efficacité opérationnelle de la détection	Qualification et traitement des alertes selon les procédures	Exécution de la détection et de la réponse	Contrôle opérationnel des alertes	RSSI (fonctionnel) ; DSI ou prestataire selon le modèle
Risk Manager	Piloter l'ensemble des risques de l'entreprise	Cohérence et agrégation des risques, appétence	Méthodologie ; arbitrages avec la Direction	Animation des revues de risques	Contrôle de deuxième ligne (risques)	Direction générale ou direction financière
DPO	Veiller à la conformité du traitement des données personnelles	Conformité aux règles de protection des données ; point de contact des autorités et des personnes	Avis et recommandations ; la décision relève du responsable du traitement	Registre des traitements, analyses d'impact, droits des personnes	Contrôle de conformité (deuxième ligne)	Direction générale ou juridique, avec indépendance (statut à vérifier selon le droit applicable)

Fonction	Mission	Responsabilité	Décision	Exécution	Contrôle	Rattachement possible
Responsable continuité	Maintenir ou reprendre les activités critiques	Résilience métier globale (BIA, PCA)	Stratégies de continuité avec les métiers	Exercices de continuité	Suivi des tests	Direction des risques, DG ou opérations
Audit interne	Évaluer de manière indépendante le dispositif de maîtrise	Assurance indépendante (troisième ligne)	Plan d'audit validé par le comité d'audit	Missions d'audit	Contrôle indépendant de troisième ligne	Comité d'audit ou Direction générale, indépendant des audités

III

PARTIE III · CHAPITRE 3

Le positionnement du RSSI dans l'organisation

Positionnement organisationnel et indépendance

CE QUE LA DIRECTION DOIT SAVOIR

1. Le rattachement hiérarchique du RSSI détermine directement son indépendance et sa capacité à exercer un contrôle crédible sur le risque numérique.

2. Un RSSI rattaché à la DSI qu'il est censé contrôler se trouve en situation de conflit d'intérêts potentiel, qui doit être compensé par des garanties d'indépendance explicites.

3. Le RSSI doit disposer d'un droit d'alerte et d'un accès direct à la Direction générale, ainsi que, périodiquement, au Conseil d'administration ou au Comité d'audit.

3.1 Pourquoi le positionnement du RSSI est stratégique

Le positionnement organisationnel du RSSI — c'est-à-dire la question de savoir à qui il est rattaché hiérarchiquement, avec quel niveau d'accès à la Direction et quelle autonomie budgétaire — conditionne très largement l'efficacité réelle de la fonction, indépendamment même des compétences individuelles de la personne qui l'occupe. Un RSSI compétent mais mal positionné, dépourvu d'autorité et de visibilité auprès de la Direction, ne pourra pas exercer pleinement sa mission, quelle que soit son expertise technique. À l'inverse, un positionnement adapté crée les conditions d'une fonction efficace, capable d'alerter, d'arbitrer et d'obtenir les ressources nécessaires à la maîtrise du risque numérique.

Ce constat, largement documenté dans les référentiels internationaux de gouvernance de la sécurité, revêt une importance particulière dans les organisations africaines où la fonction RSSI est souvent récente et où les schémas organisationnels ne se sont pas encore stabilisés. Les décideurs qui structurent aujourd'hui cette fonction disposent d'une opportunité réelle de l'ancrer, dès l'origine, sur des bases organisationnelles saines, plutôt que de devoir corriger ultérieurement un positionnement défaillant, souvent au prix d'une crise de confiance.

3.2 Les différents modèles organisationnels

Plusieurs modèles de rattachement du RSSI coexistent dans les organisations, chacun présentant des caractéristiques propres.

- RSSI rattaché à la DSI : modèle historique, encore répandu, dans lequel le RSSI dépend hiérarchiquement du Directeur des systèmes d'information ;
- RSSI rattaché à la Direction générale : le RSSI rapporte directement au Directeur général ou à un membre du Comité de direction, hors de la ligne hiérarchique de la DSI ;
- RSSI rattaché à la Direction des risques : le RSSI est intégré à la fonction de gestion des risques de l'entreprise, aux côtés du Risk Manager ;
- RSSI rattaché à l'audit ou au contrôle interne : modèle plus rare, qui pose des questions spécifiques d'indépendance vis-à-vis de la fonction d'audit elle-même ;
- Modèle matriciel : le RSSI dispose d'un rattachement hiérarchique (par exemple à la Direction générale ou aux risques) et d'un rattachement fonctionnel à la DSI pour les aspects opérationnels, combinant indépendance de gouvernance et proximité opérationnelle.

3.3 Avantages et limites de chaque modèle

Le rattachement à la DSI présente l'avantage de la proximité opérationnelle et d'une bonne compréhension des enjeux techniques, mais souffre d'une limite structurelle majeure : il place le RSSI en situation de devoir contrôler la structure dont il dépend hiérarchiquement, ce qui affaiblit son indépendance et sa capacité

à faire remonter des arbitrages défavorables à la DSI. Ce modèle, bien qu'encore majoritaire dans certaines organisations, est de moins en moins recommandé par les référentiels de gouvernance internationaux, précisément pour cette raison, sauf lorsque des garanties d'indépendance compensatoires (droit d'alerte, accès direct à la Direction générale) sont formalisées.

Le rattachement à la Direction générale offre le niveau d'indépendance et de visibilité le plus élevé, garantissant au RSSI un accès direct aux décideurs et une légitimité renforcée pour porter des arbitrages sensibles. Sa limite réside dans le risque d'un éloignement excessif des réalités opérationnelles si ce rattachement n'est pas accompagné de mécanismes de coordination étroite avec la DSI. Le rattachement à la Direction des risques présente l'avantage d'une intégration naturelle du risque cyber dans la cartographie globale des risques de l'entreprise, mais suppose une fonction de gestion des risques suffisamment mature pour porter cette intégration. Le modèle matriciel, enfin, cherche à combiner les avantages des modèles précédents, au prix d'une complexité de gouvernance qui nécessite une définition très précise des rôles et des lignes de reporting.

3.4 Modèle recommandé selon la taille de l'organisation

Il n'existe pas de modèle organisationnel universellement optimal : le choix dépend de la taille de l'organisation, de sa maturité en matière de gouvernance des risques, et du secteur dans lequel elle opère. Dans les grandes organisations — grands groupes, banques, opérateurs de télécommunications, administrations publiques d'envergure — un rattachement direct à la Direction générale ou à la Direction des risques est fortement recommandé, avec un accès périodique formalisé au Conseil d'administration ou au Comité d'audit, conformément aux meilleures pratiques de gouvernance internationale.

Dans les organisations de taille intermédiaire, où les ressources dédiées à la sécurité restent limitées, un rattachement à la Direction générale reste préférable chaque fois que possible ; à défaut, un modèle matriciel avec rattachement fonctionnel à la DSI mais accès direct et documenté à la Direction générale pour les sujets stratégiques peut constituer un compromis acceptable. Dans les petites organisations et les PME, où un RSSI à temps plein n'est pas toujours envisageable, la question du positionnement se pose différemment et est traitée spécifiquement dans la Partie XV de ce guide, consacrée aux enjeux propres au contexte africain, notamment à la section relative aux PME.

Le tableau ci-dessous propose une approche graduée fondée sur trois critères : la criticité des activités, la taille et la maturité. Il s'agit d'un repère indicatif destiné à nourrir l'arbitrage de la Direction, et non d'une règle universelle.

Profil de l'organisation	Rattachement recommandé	Garanties minimales d'indépendance	Points de vigilance
Forte criticité ou grande taille (banque, opérateur de télécommunications, OIIC, administration centrale, santé)	Direction générale ou Direction des risques ; accès périodique au Conseil ou au comité d'audit	Mandat écrit ; droit d'alerte ; accès direct à la DG et au comité d'audit ; budget propre	Éviter l'éloignement des opérations : coordination formalisée avec la DSI

Profil de l'organisation	Rattachement recommandé	Garanties minimales d'indépendance	Points de vigilance
Taille intermédiaire, criticité modérée, maturité en construction	Direction générale ou modèle matriciel (hiérarchique DG, fonctionnel DSI)	Droit d'alerte écrit ; accès direct à la DG sur les sujets stratégiques ; revue annuelle du mandat	Clarifier les arbitrages ; éviter la double casquette DSI et RSSI
PME, petite structure, criticité faible à modérée	RSSI à temps partiel, fonction partagée ou RSSI externalisé à temps partagé, rattaché à la DG	Lettre de mission ; point de contact DG ; séparation des tâches de contrôle autant que possible	Compenser par des audits externes périodiques ; ne pas confier le rôle au seul administrateur système
Maturité initiale (niveaux 1 et 2)	Direction générale dès que possible ; rattachement transitoire à la DSI admissible	Plan daté de sortie du rattachement transitoire ; droit d'alerte ; reporting à la DG	Le rattachement transitoire ne doit pas devenir définitif par inertie

3.5 Autorité et indépendance du RSSI

L'autorité du RSSI ne se décrète pas : elle se construit à travers plusieurs leviers organisationnels que la Direction doit activer explicitement. Le premier levier est le rattachement hiérarchique, déjà évoqué, qui conditionne l'indépendance de jugement du RSSI. Le second levier est la reconnaissance formelle de son mandat, à travers une lettre de mission et une charte de fonction clairement approuvées par la Direction générale, qui légitiment son droit d'alerte, d'accès à l'information et d'interpellation des autres directions.

Le troisième levier est l'accès effectif à la Direction générale et, périodiquement, aux organes de gouvernance de l'organisation, qui garantit que les alertes et recommandations du RSSI ne restent pas bloquées à un niveau hiérarchique intermédiaire. Le quatrième levier, enfin, est la disponibilité de ressources — budget, effectifs, outils — proportionnées aux missions confiées, sans lesquelles l'autorité formelle du RSSI resterait purement théorique. L'indépendance du RSSI ne signifie pas son isolement : elle signifie sa capacité à porter, sans filtre ni pression hiérarchique excessive, une appréciation objective du risque numérique jusqu'aux plus hauts niveaux de décision de l'organisation.

En synthèse, trois exigences fondamentales structurent l'autorité du RSSI : l'indépendance de jugement, le droit d'alerte et l'accès direct au niveau décisionnel approprié. Elles constituent le socle minimal à garantir quels que soient le modèle de rattachement et la taille de l'organisation.

3.6 Accès du RSSI à la Direction générale

Un accès régulier et direct à la Direction générale constitue l'un des marqueurs les plus fiables de la maturité de gouvernance d'une organisation en matière de cybersécurité. Cet accès doit se traduire concrètement par une participation périodique du RSSI aux réunions du Comité de direction, à titre de bonne pratique indicative, lors de la présentation du reporting trimestriel de sécurité, ainsi que par la possibilité, pour le RSSI, de solliciter une audience de la Direction générale en dehors de ce rythme périodique en cas d'incident majeur ou de risque nécessitant un arbitrage urgent.

Les fréquences mentionnées dans cette section et dans la suivante constituent des repères indicatifs de bonne pratique, à moduler selon la taille, le secteur, le niveau de risque et les obligations réglementaires de l'organisation. Elles ne constituent pas une règle universelle.

À l'inverse, l'absence d'un tel accès — lorsque le RSSI ne communique avec la Direction générale que par l'intermédiaire de la DSI, ou uniquement de manière informelle et non systématique — constitue un signal d'alerte sur la maturité de gouvernance de l'organisation, quels que soient par ailleurs la qualité technique du dispositif de sécurité en place et les compétences individuelles du RSSI.

3.7 Accès du RSSI au Conseil d'administration / Comité d'audit

Au-delà de la Direction générale, les meilleures pratiques de gouvernance recommandent que le RSSI dispose d'un accès périodique — généralement annuel ou semestriel, à titre indicatif — au Conseil d'administration ou au Comité d'audit, afin de présenter une synthèse de l'exposition au risque cyber de l'organisation, l'état d'avancement du plan de traitement des risques et, le cas échéant, un retour sur les incidents significatifs survenus. Cette pratique, encore peu répandue dans de nombreuses organisations africaines, tend cependant à se généraliser, portée par la responsabilisation croissante des administrateurs sur les questions de risque numérique, y compris sur le plan juridique.

Cet accès ne doit pas être perçu comme une marque de défiance envers la Direction générale, mais comme l'expression d'un principe de gouvernance largement admis : le Conseil d'administration, responsable in fine de la supervision des risques majeurs de l'organisation, doit pouvoir accéder à une information de première main sur l'un des risques les plus significatifs auxquels les organisations contemporaines sont exposées. Les modalités pratiques de ce reporting au Conseil sont détaillées dans la Partie XIII de ce guide.

3.8 Charte de la fonction RSSI

La charte de la fonction RSSI est le document de gouvernance qui formalise le mandat, les responsabilités, l'autorité et les prérogatives du RSSI au sein de l'organisation. Approuvée par la Direction générale, et idéalement portée à la connaissance du Conseil d'administration, cette charte constitue le socle juridique et organisationnel sur lequel repose la légitimité de l'ensemble de l'action du RSSI. Elle précise notamment le rattachement hiérarchique du RSSI, son périmètre d'intervention, son droit d'accès à l'information et aux systèmes, son droit d'alerte auprès de la Direction générale, ainsi que les modalités de collaboration attendues avec les autres directions de l'organisation.

L'absence d'une telle charte, fréquente dans les organisations où la fonction RSSI a été créée de manière informelle, constitue une fragilité majeure : elle laisse le RSSI dépourvu de base formelle pour faire valoir son autorité en cas de résistance d'une autre direction, et prive l'organisation d'un cadre de référence stable, indépendant des personnes qui occupent successivement la fonction.

3.9 Lettre de mission du RSSI

Distincte de la charte de fonction, qui a une portée générale et pérenne, la lettre de mission est un document individuel, adressé au titulaire du poste de RSSI lors de sa prise de fonction, qui précise les objectifs spécifiques qui lui sont assignés pour une période donnée, les moyens mis à sa disposition, et les modalités selon lesquelles sa performance sera évaluée. Cette lettre de mission constitue un outil de clarification réciproque essentiel : elle permet à la Direction générale de formaliser ses attentes, et au RSSI de disposer d'un mandat écrit sur lequel s'appuyer pour prioriser son action et solliciter les ressources nécessaires.

L'absence de lettre de mission, très fréquente dans la pratique observée dans de nombreuses organisations, est l'une des causes principales du décalage constaté entre les attentes implicites de la Direction et l'action effective du RSSI — décalage qui nourrit, à terme, une insatisfaction réciproque difficile à corriger faute d'un référentiel commun explicite.

3.10 Délégation de pouvoirs et responsabilités

La question de la délégation de pouvoirs se pose avec une acuité particulière pour la fonction RSSI, dans la mesure où certaines de ses décisions : blocage d'un accès, isolement d'un système compromis, arrêt d'un service en cas d'incident majeur, peuvent avoir des conséquences opérationnelles immédiates et significatives pour l'organisation. Il est essentiel que l'étendue exacte des pouvoirs délégués au RSSI soit clairement définie, notamment sur trois plans : le pouvoir de décision technique en situation d'urgence (par exemple, la capacité à isoler un système sans validation préalable en cas de suspicion d'incident actif), le pouvoir d'arbitrage sur les exceptions aux politiques de sécurité, et le pouvoir d'engagement budgétaire dans le cadre de son périmètre.

Cette délégation doit être formalisée par écrit — le plus souvent dans la charte de fonction ou dans un document de délégation spécifique — et doit prévoir explicitement les seuils au-delà desquels une validation de la Direction générale demeure requise. Une délégation insuffisante expose l'organisation à des délais de réaction inacceptables face à un incident actif ; une délégation excessive ou mal encadrée expose au contraire l'organisation à des décisions disproportionnées prises sans validation appropriée. L'équilibre entre ces deux écueils doit être trouvé au cas par cas, en fonction de la maturité de l'organisation et du niveau de confiance établi avec le titulaire de la fonction.

Pour que la délégation soit opérationnelle, elle gagne à être traduite en une matrice des pouvoirs d'urgence précisant, pour chaque mesure, qui peut décider, avec quelle validation préalable, à qui rendre compte et dans quel délai la décision doit être validée a posteriori. La matrice ci-dessous est un modèle indicatif : les délais sont des repères à adapter.

Mesure d'urgence	Qui décide	Validation préalable	Escalade / information	Validation a posteriori (délai indicatif)
Isolement d'un poste ou d'un compte utilisateur compromis	RSSI ou SOC	Non	Responsable hiérarchique et DSI	RSSI : compte rendu sous 24 h

Mesure d'urgence	Qui décide	Validation préalable	Escalade / information	Validation a posteriori (délai indicatif)
Blocage de flux, d'adresses, de domaines ou de comptes de service	RSSI ou SOC (sur délégation)	Non, sauf impact connu sur un service critique	DSI immédiatement ; direction métier concernée	RSSI, sous 24 h
Isolement d'un serveur ou d'un segment réseau non critique	RSSI, en lien avec la DSI	Non (information préalable de la DSI si possible)	DSI ; direction métier propriétaire	Responsable de la cellule de crise, sous 24 h
Coupure ou dégradation volontaire d'un service applicatif critique	Direction générale (ou responsable de la cellule de crise) sur proposition du RSSI	Oui ; à défaut, RSSI en cas de risque immédiat et de Direction injoignable	DG, direction métier, DSI, communication	DG, sous 24 h
Coupure des connexions Internet ou des liaisons avec des partenaires	Direction générale sur proposition RSSI et DSI	Oui	DG, partenaires concernés, juridique	DG, sous 24 h
Désactivation massive de comptes ou réinitialisation générale des mots de passe	RSSI et DSI	Oui (DG si impact sur l'ensemble des collaborateurs)	DRH, directions métier	Cellule de crise, sous 24 h
Activation de la cellule de crise cyber	RSSI ou DSI selon la grille de criticité	Non	DG informée immédiatement	DG, sous 24 h
Déclaration à l'autorité de référence (bjCSIRT, APDP, régulateur sectoriel)	Direction générale ou responsable désigné, sur proposition du RSSI et du DPO ou du juridique	Oui	Juridique, DPO, communication	Selon les obligations (voir 8.14)
Communication externe (clients, médias)	Direction générale et communication	Oui	RSSI, juridique	Selon le plan de communication
Paiement d'une rançon ou contact avec les attaquants	Direction générale, voire Conseil ; jamais le RSSI seul	Oui	Juridique, assureur, autorités	Conseil si requis

IV

PARTIE IV · CHAPITRE 4

Ce que le décideur doit attendre de son RSSI

Guide à l'attention des dirigeants

CE QUE LA DIRECTION DOIT SAVOIR

1. Nommer un RSSI ne suffit pas : il faut lui assigner des objectifs clairs, lui fournir des ressources proportionnées et définir des indicateurs de performance pertinents.

2. Un RSSI ne doit jamais être évalué au seul nombre d'incidents constatés, sous peine d'encourager la dissimulation plutôt que la transparence.

3. Dix questions simples permettent à tout dirigeant de tester, en quelques minutes, la maturité réelle du dispositif de sécurité de son organisation.

4.1 Pourquoi nommer un RSSI ?

La nomination d'un RSSI répond à un besoin de gouvernance précis : disposer d'un point de responsabilité unique, identifié et mandaté, pour la maîtrise du risque numérique de l'organisation. Sans ce point de responsabilité unique, la sécurité de l'information devient l'affaire de tous et, en pratique, de personne : chaque direction gère les aspects de sécurité qui la concernent directement, sans vision d'ensemble, sans priorisation cohérente et sans capacité à arbitrer entre des intérêts contradictoires. Nommer un RSSI, c'est donc avant tout créer une fonction de synthèse et d'arbitrage, indispensable dès lors que l'organisation dépasse une taille critique ou que son exposition au risque numérique devient significative.

Au-delà de cette logique de gouvernance interne, la nomination d'un RSSI répond également à des attentes croissantes des parties prenantes externes : clients et partenaires exigeant des garanties de sécurité dans le cadre de leurs relations contractuelles, régulateurs imposant la désignation d'un responsable identifié pour certains secteurs sensibles, et investisseurs ou bailleurs de fonds intégrant de plus en plus la maturité cyber dans leurs critères d'évaluation. Dans ce contexte, l'absence d'un RSSI clairement identifié peut devenir, en elle-même, un facteur de risque commercial et réputationnel.

4.2 Quel problème le RSSI doit-il résoudre ?

Avant de nommer un RSSI, il est utile pour un dirigeant de clarifier le problème précis que cette nomination doit résoudre, car cette clarification conditionne directement le profil recherché, le positionnement organisationnel retenu et les objectifs assignés. Dans certaines organisations, le problème central est l'absence totale de dispositif de sécurité structuré, et la priorité du RSSI sera alors de construire les fondations — politique de sécurité, cartographie des risques, mesures de protection élémentaires. Dans d'autres organisations, disposant déjà d'un socle technique mais dépourvues de gouvernance, le problème central sera de structurer le pilotage, le reporting et la conformité, plus que de renforcer la technique elle-même.

Dans d'autres cas encore, le problème principal est réglementaire : l'organisation doit se conformer à une exigence légale ou sectorielle imposant la désignation d'un responsable sécurité, et la priorité du RSSI sera alors orientée vers la mise en conformité et la certification. Cette clarification préalable, souvent négligée, évite l'écueil fréquent consistant à nommer un RSSI sans lui donner de mandat précis, puis à s'étonner que son action ne réponde pas à des attentes qui n'ont jamais été explicitées.

4.3 Quelles ressources faut-il mettre à sa disposition ?

Un mandat sans ressources proportionnées reste un mandat théorique. La Direction doit mettre à la disposition du RSSI un budget dédié, dont le niveau doit être calibré en fonction du profil de risque de l'organisation plutôt que fixé de manière arbitraire ou résiduelle ; des ressources humaines suffisantes, qu'il s'agisse d'une équipe interne ou d'un recours structuré à des prestataires externes ; des

outils adaptés à la taille et à la complexité du système d'information ; et, le cas échéant, des prestataires spécialisés pour les compétences que l'organisation ne peut ou ne souhaite pas internaliser.

- Budget : dédié, arbitré au regard du niveau de risque plutôt que fixé en pourcentage résiduel du budget informatique ;
- Ressources humaines : équipe interne proportionnée, ou recours structuré et contractualisé à des prestataires externes ;
- Outils : solutions techniques adaptées à la taille et à la maturité de l'organisation, sans surinvestissement technologique déconnecté des besoins réels ;
- Prestataires : partenaires spécialisés pour les compétences rares (tests d'intrusion, forensic, réponse à incident) ;
- Formation : budget et temps dédiés au maintien à jour des compétences du RSSI et de son équipe ;
- Accès : accès aux informations, aux rapports d'audit, aux journaux (logs), aux actifs et à leurs responsables métiers, selon les habilitations requises et dans le respect des règles de confidentialité ;
- Autorité : mandat formel, reconnu et communiqué à l'ensemble de l'organisation, sans lequel les ressources matérielles resteront sous-exploitées.

Ce dernier point — l'autorité — est souvent le plus négligé alors qu'il conditionne l'efficacité de tous les autres : un RSSI doté d'un budget confortable mais dépourvu de reconnaissance formelle de son autorité peinera à faire appliquer ses décisions par des directions métier peu enclines à intégrer des contraintes perçues comme externes à leur activité.

4.4 Quels objectifs assigner au RSSI ?

Les objectifs assignés au RSSI doivent être formulés en termes de maîtrise du risque et de maturité du dispositif, plutôt qu'en termes de résultats binaires du type « zéro incident », un objectif à la fois irréaliste et contre-productif, comme développé à la section 4.7. Des objectifs pertinents peuvent porter sur la réduction du niveau de risque résiduel sur les actifs les plus critiques, l'atteinte d'un niveau de maturité cible sur les référentiels utilisés par l'organisation, la mise en conformité avec des obligations réglementaires identifiées, la réduction des délais de détection et de réponse aux incidents, ou encore l'amélioration mesurable du niveau de sensibilisation des collaborateurs.

Ces objectifs doivent être fixés conjointement entre la Direction générale et le RSSI, formalisés dans la lettre de mission évoquée à la section 3.9, et révisés périodiquement en fonction de l'évolution du contexte de risque et de la maturité déjà atteinte par l'organisation. Des objectifs trop ambitieux au regard des ressources allouées exposent le RSSI à un échec programmé ; des objectifs trop modestes privent l'organisation du bénéfice d'une véritable dynamique d'amélioration continue.

4.5 Quels indicateurs suivre ?

Le suivi de la performance du RSSI et de la maturité du dispositif de sécurité repose sur un ensemble d'indicateurs qui doivent combiner mesures techniques et mesures de pilotage. Parmi les indicateurs les plus pertinents figurent : le taux de couverture des actifs critiques par une évaluation de risque à jour, le délai moyen de détection et de traitement des incidents, le taux de correction des vulnérabilités critiques dans les délais cibles, le taux de complétion des campagnes de sensibilisation, le niveau de conformité aux obligations réglementaires applicables, et l'évolution du niveau de maturité globale mesuré selon un référentiel reconnu.

Ces indicateurs n'ont toutefois ni la même nature ni les mêmes destinataires. Il convient de distinguer quatre familles, présentées ci-dessous et développées en 13.3 et en Annexe 9. Les fréquences sont indicatives.

Famille	Ce qu'elle mesure	Exemples	Destinataires	Fréquence indicative
KPI opérationnels	Efficacité des processus de sécurité	Délai de correction des vulnérabilités par priorité ; MTTD et MTTR ; taux de couverture EDR et sauvegarde	RSSI, DSI, SOC	Hebdomadaire à mensuelle
KRI (indicateurs de risque)	Niveau d'exposition au risque	Vulnérabilités critiques exposées ; comptes privilégiés sans MFA ; fournisseurs critiques non évalués	RSSI, risk manager, comité de sécurité	Mensuelle à trimestrielle
Indicateurs de conformité	Niveau de respect des obligations	Obligations applicables couvertes ; écarts majeurs ouverts ; recommandations d'audit clôturées	RSSI, DPO, juridique, audit interne, comité d'audit	Trimestrielle à semestrielle
Indicateurs destinés au CODIR et au Conseil	Exposition globale et décisions à prendre	Cinq à dix indicateurs de synthèse avec tendance, cibles et arbitrages attendus	Direction générale, Comité de direction, Conseil ou comité d'audit	Trimestrielle (CODIR) ; annuelle ou semestrielle (Conseil)

Ces indicateurs, développés en détail dans la Partie XIII de ce guide consacrée au pilotage et au reporting du RSSI, doivent être présentés à la Direction sous une forme synthétique et orientée décision, évitant l'écueil fréquent d'un reporting exclusivement technique, incompréhensible pour des décideurs non spécialistes et, de ce fait, rarement exploité dans la prise de décision effective.

4.6 Comment évaluer la performance d'un RSSI ?

Évaluer la performance d'un RSSI suppose de dépasser la seule appréciation intuitive pour s'appuyer sur des critères objectivés, alignés sur les objectifs fixés dans sa lettre de mission. Ces critères peuvent porter sur la progression effective de la maturité du dispositif de sécurité, la qualité et la régularité du reporting fourni à la Direction, la capacité démontrée à gérer efficacement les incidents survenus, la qualité de la relation établie avec les autres directions de l'organisation, et la capacité à faire progresser la culture de sécurité au sein de l'organisation.

Cette évaluation gagne à être conduite de manière structurée, au moins annuellement, associant la Direction générale et, pour les organisations disposant d'un tel niveau de gouvernance, le Comité d'audit ou le Conseil d'administration.

Elle doit s'appuyer sur des éléments factuels et documentés — tableaux de bord, rapports d'incident, retours d'audit — plutôt que sur la seule perception, nécessairement partielle, qu'en a la Direction générale au fil de l'année.

4.7 Pourquoi le RSSI ne doit pas être évalué uniquement sur le nombre d'incidents

L'une des erreurs les plus fréquentes, et les plus dommageables, consiste à évaluer implicitement ou explicitement la performance du RSSI au seul nombre d'incidents constatés au cours de la période. Ce critère, en apparence intuitif, est en réalité trompeur et contre-productif à plusieurs égards. D'une part, le nombre d'incidents détectés dépend directement de la qualité du dispositif de détection : un dispositif de détection efficace révélera davantage d'incidents — y compris mineurs — qu'un dispositif défaillant qui laisserait ces mêmes incidents passer inaperçus. Pénaliser le RSSI pour un nombre élevé d'incidents détectés revient ainsi, paradoxalement, à décourager l'investissement dans la détection.

D'autre part, ce critère crée une incitation perverse à la dissimulation : un RSSI évalué sur le nombre d'incidents pourrait être tenté de minimiser ou de ne pas remonter certains événements à la Direction, ce qui prive précisément l'organisation de la transparence nécessaire à une gestion saine du risque. Enfin, un grand nombre d'incidents mineurs correctement détectés et traités rapidement témoigne souvent d'une meilleure maîtrise du risque qu'une organisation qui ne détecte quasiment aucun incident, faute de dispositif de surveillance adéquat. L'évaluation du RSSI doit donc privilégier des critères de maturité, de délai de détection et de réponse, et de qualité du traitement des incidents, plutôt que leur seul nombre brut.

4.8 Les erreurs fréquentes des dirigeants vis-à-vis du RSSI

Plusieurs postures, régulièrement observées chez des dirigeants pourtant bien intentionnés, fragilisent durablement l'efficacité de la fonction RSSI. La première consiste à assimiler l'absence d'incident constaté à une preuve de sécurité effective, alors qu'elle peut tout aussi bien traduire une absence de capacité de détection. La deuxième consiste à considérer que la sécurité relève exclusivement de la DSI, ce qui prive l'organisation d'une gouvernance indépendante du risque et reproduit le conflit d'intérêts structurel évoqué à la section 2.6.

EXEMPLES DE POSTURES À ÉVITER

- *« Nous n'avons jamais eu d'incident, donc nous sommes sécurisés. »*
- *« La sécurité relève de la DSI. »*
- *« Nous n'avons pas besoin d'un RSSI, nous avons déjà un administrateur réseau. »*
- *« Le RSSI doit tout sécuriser avec le budget informatique existant. »*

La troisième erreur, fréquente dans les organisations de taille modeste, consiste à considérer qu'un administrateur réseau ou système peut assumer de facto le rôle de RSSI, en confondant compétence technique et mandat de gouvernance. La quatrième erreur consiste à ne pas allouer de budget spécifique à la sécurité, en

considérant qu'elle doit être financée par prélèvement sur le budget informatique existant, ce qui institutionnalise une compétition permanente entre projets métier et exigences de sécurité, généralement défavorable à ces dernières. Ces postures, bien que compréhensibles dans des contextes de ressources contraintes, doivent être identifiées et corrigées consciemment par la Direction pour permettre à la fonction RSSI de produire ses effets attendus.

4.9 Les 10 questions que tout dirigeant devrait poser à son RSSI

Pour permettre à un dirigeant, même non spécialiste des questions techniques, d'évaluer rapidement la maturité réelle du dispositif de sécurité de son organisation, dix questions simples, à poser directement au RSSI ou à formuler à son intention, constituent un point de départ éprouvé.

Pour chaque question, attribuez un score de 0 à 4 selon le barème ci-dessous, en fonction de la qualité et de la précision de la réponse obtenue. Notez la réponse ou le constat dans la colonne prévue à cet effet, ainsi qu'un commentaire ou une action à envisager si nécessaire.

Barème de notation

0	**Aucune réponse / Non maîtrisé**	Le RSSI ne peut pas répondre, ou la réponse révèle une absence totale de dispositif sur ce point.
1	**Réponse vague / Débutant**	Une intention ou une démarche informelle existe, mais rien n'est documenté ni suivi dans la durée.
2	**Partiellement maîtrisé**	Un dispositif existe et est partiellement appliqué, mais présente des lacunes significatives ou n'est pas régulièrement actualisé.
3	**Globalement maîtrisé**	Le dispositif est documenté, appliqué et suivi, avec des axes d'amélioration mineurs identifiés.
4	**Pleinement maîtrisé**	Réponse précise, documentée, régulièrement testée ou actualisée, et alignée sur les bonnes pratiques du secteur.

Les 10 questions et leur évaluation

N°	Question à poser au RSSI	Réponse / Constat	Score (0 à 4)	Commentaire / Action à envisager
1	Disposons-nous d'une cartographie à jour de nos risques numériques les plus critiques ?			
2	Quels sont nos trois principaux risques cyber actuellement non traités, et pourquoi ?			
3	Combien de temps nous faudrait-il pour détecter une intrusion active sur nos systèmes ?			
4	Disposons-nous d'un plan de réponse aux incidents de cybersécurité testé au cours des douze derniers mois ?			
5	Nos sauvegardes critiques sont-elles isolées et testées régulièrement en restauration ?			
6	Quel est notre niveau de conformité aux obligations réglementaires qui nous sont applicables ?			
7	Nos prestataires critiques ont-ils été évalués sur le plan de la sécurité ?			
8	Quel pourcentage de nos collaborateurs a suivi une sensibilisation à la sécurité au cours de l'année écoulée ?			
9	Quel est notre budget de sécurité rapporté à notre budget informatique global, et comment se compare-t-il aux pratiques de notre secteur ?			
10	Si un incident majeur survenait demain, qui ferait quoi, dans quel ordre, et avec quelle autorité de décision ?			
SCORE TOTAL (somme des 10 scores, sur 40 points)			_____ / 40	

Grille de lecture du score

Score	Niveau	Interprétation
0 – 10	Dispositif non maîtrisé	L'organisation ne dispose pas d'un pilotage structuré du risque numérique. Une action urgente de structuration de la fonction sécurité est nécessaire (voir Partie I à III du Guide du RSSI).
11 – 20	Dispositif émergent	Des premières bases existent mais restent fragiles et peu formalisées. Les fondations de gouvernance (politique de sécurité, registre des risques, comité de sécurité) doivent être consolidées en priorité.
21 – 30	Dispositif en structuration	L'organisation a engagé une démarche structurée, avec des marges de progression identifiables. Un plan de traitement des risques et un tableau de bord régulier permettront d'accélérer la progression.
31 – 36	Dispositif globalement maîtrisé	La majorité des dimensions essentielles sont couvertes et documentées. L'enjeu principal devient le maintien dans la durée et l'amélioration continue.
37 – 40	Dispositif maîtrisé	Le dispositif de sécurité de l'organisation est solide sur l'ensemble des dimensions testées. Il convient de maintenir ce niveau et de rester vigilant face à l'évolution des menaces.

L'incapacité du RSSI, ou de l'organisation dans son ensemble, à répondre avec précision à plusieurs de ces questions constitue en elle-même un indicateur fiable de l'existence de lacunes significatives dans la gouvernance du risque numérique, indépendamment de toute évaluation technique approfondie. Ces dix questions, volontairement simples dans leur formulation, ouvrent en réalité sur l'ensemble des thématiques développées dans les parties suivantes de ce guide.



2

BLOC 2

Gouverner

Parties V à VI

Ce bloc décrit comment la sécurité est gouvernée : instances, politiques, exceptions et risques acceptés, puis gestion des risques cyber, cœur méthodologique du métier de RSSI.

Lecture prioritaire pour : RSSI, Direction générale, risk managers, comités de sécurité et d'audit.

Partie	Contenu	Niveau principal
V	Construire et piloter le dispositif de cybersécurité (chapitre 5)	Piloter
VI	Gestion des risques cyber (chapitre 6)	Piloter

V

PARTIE V · CHAPITRE 5

Construire et piloter le dispositif de cybersécurité

Gouvernance de la sécurité

CE QUE LA DIRECTION DOIT SAVOIR

1

La gouvernance de la sécurité est le système de règles, d'instances et de responsabilités qui permet à l'organisation de décider, d'arbitrer et de rendre compte de manière cohérente en matière de risque numérique.

2

Sans instances de gouvernance formalisées (comités, politiques, rôles), le RSSI agit seul, sans légitimité collective ni capacité d'arbitrage.

3

Le modèle des trois lignes de défense clarifie qui fait, qui contrôle, et qui audite — une distinction essentielle pour éviter que le RSSI ne devienne juge et partie.

5.1 Stratégie de cybersécurité

La stratégie de cybersécurité est le document de cadrage pluriannuel qui fixe les orientations, les priorités et la trajectoire de transformation du dispositif de sécurité de l'organisation, en cohérence avec sa stratégie globale et son appétence au risque. Elle répond à des questions structurantes : quels sont les risques numériques les plus critiques pour l'atteinte des objectifs de l'organisation ? Quel niveau de maturité vise-t-on, et à quel horizon ? Quels investissements, humains et budgétaires, cette trajectoire suppose-t-elle ?

Élaborée par le RSSI, cette stratégie doit être validée par la Direction générale, car elle engage des arbitrages qui dépassent le seul périmètre technique — priorisation des investissements, niveau de risque accepté, calendrier de mise en conformité. Une stratégie de cybersécurité efficace n'est ni un catalogue exhaustif de mesures techniques, ni un document théorique déconnecté des réalités opérationnelles : elle doit rester lisible par un comité de direction, s'appuyer sur une analyse de risque documentée, et être révisée à intervalle régulier — généralement tous les deux à trois ans, ou lors d'un changement significatif du contexte de risque de l'organisation.

5.2 Politique de sécurité des systèmes d'information (PSSI)

La Politique de Sécurité des Systèmes d'Information (PSSI) est le document de référence qui énonce les principes directeurs, les règles générales et les responsabilités en matière de sécurité de l'information, applicables à l'ensemble de l'organisation. Elle constitue le socle normatif à partir duquel se déclinent l'ensemble des politiques thématiques, procédures et standards techniques plus détaillés. Une PSSI type couvre notamment la classification de l'information, les règles d'accès, les responsabilités des utilisateurs, les exigences applicables aux systèmes et aux prestataires, ainsi que les sanctions applicables en cas de non-respect.

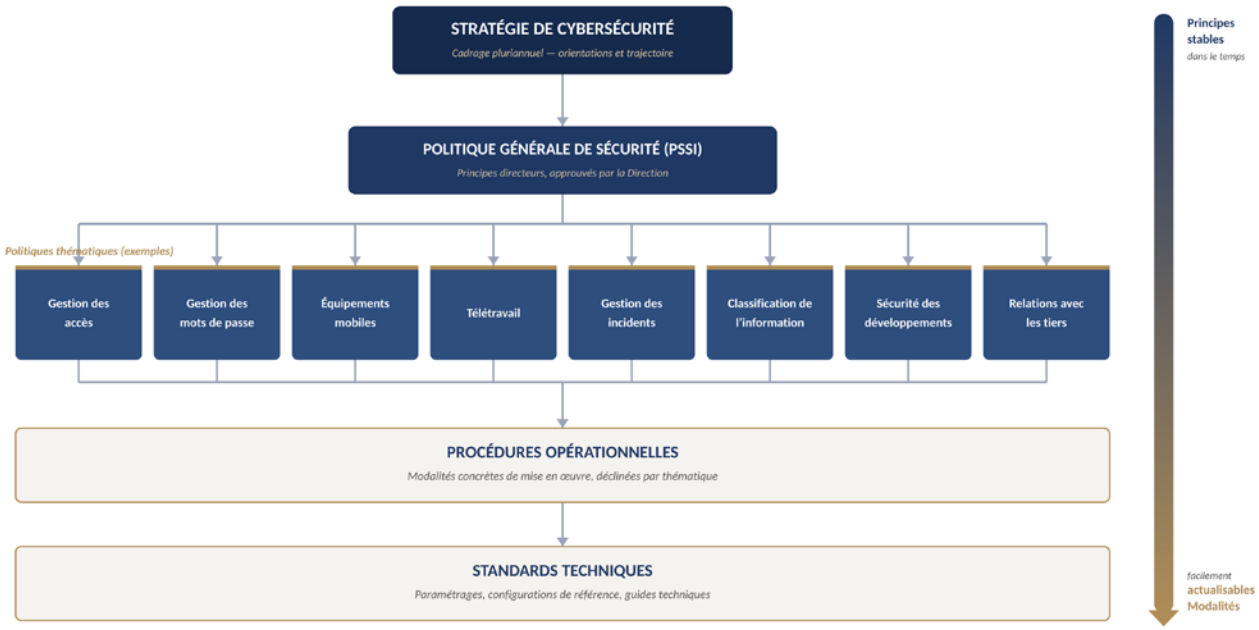
Pour être réellement opérante, la PSSI doit être approuvée formellement par la Direction générale — ce qui lui confère une autorité qu'un simple document technique rédigé par le RSSI seul ne saurait avoir — diffusée à l'ensemble des collaborateurs, et déclinée en documents opérationnels compréhensibles par leurs destinataires. Une PSSI trop générale reste lettre morte ; une PSSI trop détaillée devient rapidement obsolète et illisible. L'enjeu pour le RSSI est de trouver le niveau de granularité adapté à la maturité et à la taille de son organisation.

5.3 Politiques et procédures de sécurité

Sous la PSSI se déploie un corpus de politiques thématiques (gestion des accès, gestion des mots de passe, utilisation des équipements mobiles, télétravail, gestion des incidents, classification de l'information, sécurité des développements, relations avec les tiers, etc.) et de procédures opérationnelles qui précisent les modalités concrètes de mise en œuvre de ces politiques. Cette hiérarchie documentaire — stratégie, politique générale, politiques thématiques, procédures, standards techniques — permet d'articuler des principes stables dans le temps avec des modalités d'application plus facilement actualisables.

La gestion de ce corpus documentaire constitue une responsabilité à part entière du RSSI : chaque document doit être daté, versionné, doté d'un propriétaire identifié et revu périodiquement. Un corpus documentaire à jour, cohérent et accessible aux collaborateurs concernés est l'un des premiers éléments examinés lors d'un audit de sécurité ou d'une démarche de certification, et constitue souvent un indicateur fiable, quoique partiel, de la maturité globale de l'organisation en matière de gouvernance de la sécurité.

Hiérarchie documentaire de la sécurité de l'information



POURQUOI CETTE HIÉRARCHIE

- *Elle sépare ce qui doit rester stable (les principes, validés au plus haut niveau) de ce qui doit pouvoir évoluer rapidement (les modalités techniques), sans que la révision d'un paramétrage n'impose de revoir la stratégie ou la PSSI.*
- *Elle facilite la gouvernance documentaire : chaque niveau a un propriétaire, une instance de validation et un rythme de révision qui lui sont propres.*
- *Elle permet d'auditer la cohérence verticale du dispositif : toute procédure ou standard technique doit pouvoir se rattacher explicitement à une politique thématique, elle-même rattachée à la PSSI et à la stratégie.*

5.4 Comité de sécurité

Le Comité de sécurité est l'instance de gouvernance opérationnelle animée par le RSSI, réunissant généralement les représentants de la DSI, des principales directions métier et, selon les sujets, de la conformité, des risques et des ressources humaines. Ce comité a vocation à suivre l'avancement du plan de sécurité, à examiner les incidents significatifs et les enseignements qui en découlent, à arbitrer les priorités entre projets de sécurité concurrents, et à préparer les décisions qui devront être portées, le cas échéant, au niveau de la Direction générale.

La régularité de ce comité — généralement mensuelle ou trimestrielle selon la taille de l'organisation — et la qualité de sa préparation conditionnent largement

son utilité réelle : un comité mal préparé, réduit à une présentation descendante d'indicateurs sans échange ni arbitrage, perd rapidement sa valeur ajoutée et voit sa fréquentation décliner. Le RSSI a tout intérêt à structurer ce comité autour de décisions concrètes à prendre, plutôt que d'un simple reporting d'activité.

5.5 Comité de gestion des risques

Distinct du comité de sécurité, dont le périmètre est propre au risque numérique, le Comité de gestion des risques est une instance transversale, réunissant les responsables des différentes catégories de risque de l'organisation (financier, juridique, opérationnel, cyber, réputationnel), sous l'égide de la Direction générale ou de la fonction « Risques » lorsqu'elle existe. Le RSSI y intervient comme contributeur, apportant l'éclairage spécifique au risque numérique dans une vision consolidée des risques de l'organisation.

Cette articulation permet d'éviter un écueil fréquent : celui d'un risque cyber traité en silo, sans mise en perspective avec les autres risques de l'organisation, alors même que ses conséquences — financières, réputationnelles, juridiques — sont directement comparables à celles des autres catégories de risque. Dans les organisations qui ne disposent pas encore d'un tel comité transversal, le RSSI a intérêt à en promouvoir la création, ou à défaut à s'assurer que le risque cyber est explicitement intégré à la cartographie globale des risques examinée par la Direction générale.

5.6 Rôles et responsabilités

La clarification des rôles et responsabilités en matière de sécurité de l'information est une condition de l'efficacité de tout dispositif de gouvernance. Au-delà du RSSI lui-même, cette clarification doit couvrir la Direction générale (responsable ultime de l'acceptation des risques majeurs), les directions métier (responsables de la sécurité de leurs processus et de leurs équipes), la DSI (responsable de la mise en œuvre technique des exigences de sécurité), les collaborateurs (responsables du respect des règles applicables à leur usage quotidien des systèmes), et les prestataires (responsables contractuellement du respect des exigences de sécurité applicables à leurs prestations).

Cette répartition, souvent formalisée dans une matrice de type RACI (voir annexe 10) pour les processus critiques, doit être documentée et communiquée, faute de quoi elle reste implicite et sujette à interprétation divergente selon les acteurs — situation qui se révèle particulièrement problématique lors de la gestion d'un incident, lorsque chacun découvre, dans l'urgence, ce qu'il était censé faire.

5.7 Modèle des trois lignes de défense

Le modèle des trois lignes de défense, largement reconnu dans les référentiels de gouvernance et de contrôle interne, structure la répartition des responsabilités en matière de maîtrise des risques au sein d'une organisation.

La première ligne de défense est constituée des opérationnels — DSI, équipes métier — qui mettent en œuvre les mesures de sécurité au quotidien et sont responsables de la gestion directe du risque dans leur périmètre.

La deuxième ligne de défense est constituée des fonctions de définition des politiques et de contrôle, au premier rang desquelles le RSSI, ainsi que les fonctions risques et conformité, qui définissent le cadre et vérifient son application sans en assurer eux-mêmes la mise en œuvre opérationnelle.

La troisième ligne de défense est constituée de l'audit interne, qui évalue de manière indépendante l'efficacité de l'ensemble du dispositif — y compris celui piloté par le RSSI en deuxième ligne. Ce modèle, déjà évoqué à la section 2.11 de ce guide, offre un cadre de référence précieux pour situer précisément la fonction RSSI dans l'architecture de contrôle de l'organisation, et pour éviter la confusion, fréquente dans les organisations moins matures, entre les rôles d'exécutant, de contrôleur et d'auditeur.

5.8 Gouvernance des exceptions de sécurité

Aucune politique de sécurité ne peut anticiper l'ensemble des situations opérationnelles auxquelles une organisation est confrontée ; des demandes de dérogation à une règle de sécurité — pour des raisons techniques, commerciales ou de calendrier — sont donc inévitables et légitimes dans certaines circonstances. Il est essentiel que ces exceptions soient gérées par un processus formalisé, plutôt que par des arrangements informels qui échappent à toute traçabilité et finissent, par accumulation, par vider la politique de sécurité de sa substance.

Un processus de gestion des exceptions efficace prévoit une demande documentée, précisant la règle concernée, la justification de la dérogation, les mesures compensatoires envisagées et la durée de validité de l'exception, ainsi qu'une validation par une autorité clairement identifiée — le RSSI pour les exceptions mineures, la Direction générale pour les exceptions touchant des risques significatifs. Un registre des exceptions accordées, revu périodiquement, permet de s'assurer qu'aucune dérogation n'est reconduite indéfiniment sans réexamen, et offre une vision consolidée précieuse lors des exercices d'audit.

Toute dérogation devrait avoir une échéance, un responsable nommé et une mesure compensatoire documentée ; à l'échéance, elle est soit clôturée, soit soumise à une nouvelle décision.

5.9 Gestion des risques acceptés

L'acceptation du risque est l'une des quatre options de traitement du risque, développée en détail à la section 6.6 de ce guide, mais elle mérite une attention particulière sur le plan de la gouvernance : accepter un risque est une décision qui engage l'organisation, et qui ne peut relever de la seule appréciation du RSSI, sous peine de le placer en situation de porter seul la responsabilité d'une décision qui n'est pas, par nature, la sienne.

Un dispositif de gouvernance mature prévoit que toute acceptation de risque significatif fasse l'objet d'une formalisation écrite, mentionnant le risque concerné,

son niveau d'exposition, les raisons de l'acceptation, la durée de validité de cette acceptation, et la signature de l'autorité compétente — généralement le directeur de l'entité concernée pour les risques modérés, la Direction générale pour les risques majeurs. Le RSSI a la responsabilité de maintenir un registre de ces risques acceptés, de le présenter périodiquement en comité de sécurité, et de s'assurer qu'aucun risque n'est accepté par défaut, faute d'une décision explicite.

VI

PARTIE VI · CHAPITRE 6

Gestion des risques cyber

Le RSSI et le management des risques

CE QUE LA DIRECTION DOIT SAVOIR

1. La gestion des risques est le cœur méthodologique du métier de RSSI : c'est elle qui permet de prioriser objectivement les investissements de sécurité plutôt que de réagir aux menaces les plus médiatisées.

2. Un registre des risques à jour, avec des risques évalués, traités et suivis, est l'outil de pilotage fondamental que toute Direction devrait pouvoir consulter.

3. L'appétence au risque de l'organisation doit être définie par la Direction, et non déduite implicitement des seules pratiques du RSSI.

6.1 Pourquoi gérer les risques ?

La gestion des risques constitue le fondement méthodologique de l'ensemble de l'action du RSSI, pour une raison simple : aucune organisation ne dispose de ressources illimitées pour se protéger contre l'ensemble des menaces possibles. La gestion des risques permet de sortir d'une logique réactive, où les investissements de sécurité seraient dictés par l'actualité des menaces ou par la dernière recommandation d'audit, pour adopter une logique proactive et priorisée, fondée sur une évaluation objective de ce qui expose le plus l'organisation à des conséquences significatives.

Cette démarche répond également à une exigence de gouvernance : elle permet au RSSI de justifier ses arbitrages auprès de la Direction sur la base d'une méthode reconnue et reproductible, plutôt que sur la seule base de son jugement individuel, et elle permet à la Direction de comprendre et, le cas échéant, de contester ces arbitrages en connaissance de cause. La gestion des risques cyber n'est donc pas un exercice académique périphérique : elle est l'outil de dialogue central entre le RSSI et sa Direction.

6.2 Identification des actifs

La première étape de toute démarche de gestion des risques consiste à identifier les actifs informationnels de l'organisation dont la compromission, en disponibilité, intégrité ou confidentialité, aurait un impact significatif. Ces actifs comprennent les données elles-mêmes (données clients, données financières, secrets d'affaires, données personnelles), les applications et systèmes qui les traitent, les infrastructures qui les hébergent, ainsi que les processus métier qui en dépendent.

Cette identification doit s'accompagner d'une classification, permettant de distinguer les actifs critiques, dont l'indisponibilité ou la compromission menacerait directement la continuité ou la réputation de l'organisation, des actifs secondaires, dont l'impact serait plus limité. Cette hiérarchisation, souvent négligée au profit d'une approche uniforme appliquant les mêmes exigences à l'ensemble du système d'information, est pourtant ce qui permet ensuite de concentrer les efforts de protection là où ils sont le plus nécessaires, en particulier dans des contextes de ressources contraintes.

6.3 Identification des menaces

L'identification des menaces consiste à recenser les sources potentielles de risque susceptibles d'affecter les actifs identifiés : acteurs malveillants externes (cybercriminels, groupes étatiques, hacktivistes), menaces internes (erreur humaine, malveillance, négligence), défaillances techniques (panne, obsolescence, erreur de configuration), et événements externes (catastrophe naturelle, défaillance d'un prestataire critique, instabilité des infrastructures). Cette identification s'appuie utilement sur une veille active des menaces sectorielles et régionales, ainsi que sur le retour d'expérience des incidents déjà survenus au sein de l'organisation ou de son secteur d'activité.

Il est important que cette identification ne se limite pas aux seules menaces techniques les plus médiatisées, mais couvre également des scénarios moins spectaculaires mais statistiquement plus fréquents — erreur de configuration, perte d'un équipement mobile non chiffré, envoi d'information sensible au mauvais destinataire — dont l'accumulation représente souvent une part significative des incidents réels constatés dans les organisations.

6.4 Identification des vulnérabilités

Une vulnérabilité est une faiblesse, technique ou organisationnelle, susceptible d'être exploitée par une menace pour porter atteinte à un actif. L'identification des vulnérabilités techniques s'appuie sur des outils spécialisés — scanners de vulnérabilités, tests d'intrusion, revues de configuration — développés à la section 7.16 de ce guide, tandis que l'identification des vulnérabilités organisationnelles repose davantage sur des audits de processus, des entretiens et l'observation des pratiques réelles, souvent éloignées des procédures formellement documentées.

Le croisement entre une menace identifiée et une vulnérabilité exploitable constitue le scénario de risque, unité de base de l'analyse de risque : un acteur malveillant externe (menace) exploitant une absence d'authentification forte sur un compte à privilèges (vulnérabilité) pour accéder à des données sensibles (actif) illustre ce raisonnement. C'est la combinaison systématique de ces trois dimensions — actifs, menaces, vulnérabilités — qui permet de construire une cartographie des risques réellement opérationnelle plutôt qu'une simple liste de bonnes pratiques génériques.

6.5 Évaluation des risques

L'évaluation des risques consiste à estimer, pour chaque scénario identifié, une probabilité d'occurrence et un impact potentiel, généralement exprimés selon une échelle qualitative (faible, modéré, élevé, critique) ou semi-quantitative, permettant de hiérarchiser les risques entre eux et de les positionner sur une matrice de criticité. Cette évaluation, par nature partiellement subjective, gagne en robustesse lorsqu'elle mobilise plusieurs sources : retour d'expérience interne, statistiques sectorielles, avis d'experts métier et techniques, et référentiels de menaces reconnus.

L'impact doit être évalué selon plusieurs dimensions — financière, opérationnelle, réputationnelle, réglementaire, juridique — plutôt que sous le seul angle technique, afin de permettre une comparaison pertinente avec les autres catégories de risque de l'organisation. Cette évaluation multidimensionnelle est ce qui permet ensuite au RSSI de dialoguer avec la Direction générale dans un langage de risque d'entreprise, plutôt que dans un langage exclusivement technique peu mobilisateur pour des décideurs non spécialistes.

6.6 Traitement des risques : réduction, évitement, transfert, acceptation

Une fois évalué, chaque risque doit faire l'objet d'une décision de traitement, parmi quatre options classiquement retenues.

La réduction consiste à mettre en œuvre des mesures — techniques, organisationnelles ou humaines — visant à diminuer la probabilité d'occurrence ou l'impact du risque, sans l'éliminer totalement ; c'est l'option la plus fréquemment retenue en pratique.

L'évitement consiste à renoncer à l'activité ou au processus générateur du risque, une option radicale, rarement praticable pour des risques liés à des systèmes essentiels à l'activité, mais parfois pertinente lors de la conception d'un nouveau projet.

Le transfert consiste à faire porter tout ou partie des conséquences financières du risque par un tiers, typiquement via une police d'assurance cyber, sans pour autant réduire la probabilité d'occurrence de l'incident lui-même — un point souvent mal compris, l'assurance cyber ne dispensant en rien de la mise en œuvre de mesures de sécurité adéquates, et étant d'ailleurs de plus en plus conditionnée par les assureurs à un niveau de maturité minimal. **L'acceptation**, enfin, consiste à assumer consciemment le risque en l'état, sans mesure de traitement supplémentaire, une décision qui, comme évoqué à la section 5.9, doit être formalisée et validée au niveau de gouvernance approprié.

6.7 Registre des risques

Le registre des risques est l'outil central de pilotage de la fonction de gestion des risques cyber : il recense l'ensemble des scénarios de risque identifiés, leur évaluation, la décision de traitement retenue, le plan d'action associé, son état d'avancement et son propriétaire désigné. Ce registre doit être vivant — actualisé au fil de l'identification de nouveaux risques, de la réalisation d'incidents ou de l'évolution du contexte — et non un document figé produit une fois par an à l'occasion d'un exercice formel déconnecté du pilotage courant.

Un registre des risques bien tenu constitue également un outil de preuve précieux pour démontrer, lors d'un audit ou d'un contrôle réglementaire, que l'organisation dispose d'une démarche structurée de maîtrise du risque numérique, indépendamment même du niveau de risque résiduel constaté. La qualité de la tenue de ce registre — exhaustivité, actualisation, traçabilité des décisions — est d'ailleurs l'un des tout premiers éléments examinés par un auditeur externe évaluant la maturité de gouvernance du risque cyber d'une organisation.

6.8 Cartographie des risques cyber

La cartographie des risques cyber est la représentation synthétique, le plus souvent visuelle, de l'ensemble des risques identifiés, positionnés selon leur probabilité et leur impact sur une matrice de criticité. Cet outil de communication, complémentaire du registre des risques qui en constitue la source détaillée, est particulièrement adapté à une présentation en comité de direction ou en conseil

d'administration, où il permet en un coup d'œil d'identifier les risques prioritaires nécessitant une attention ou un arbitrage de la Direction.

Pour conserver sa valeur de pilotage, cette cartographie doit être actualisée à un rythme régulier — généralement semestriel ou annuel — et doit faire apparaître explicitement l'évolution des risques d'une période à l'autre, permettant ainsi de visualiser les progrès réalisés grâce aux plans de traitement mis en œuvre, ou au contraire l'émergence de nouveaux risques nécessitant une action renforcée.

6.9 Appétence et tolérance au risque

L'appétence au risque désigne le niveau de risque global qu'une organisation est prête à accepter dans la poursuite de ses objectifs stratégiques, tandis que la tolérance au risque en précise les limites acceptables pour chaque catégorie de risque. Ces notions, bien établies en matière de risque financier, restent encore peu formalisées dans de nombreuses organisations en matière de risque cyber, alors qu'elles constituent le référentiel indispensable permettant au RSSI de déterminer si un niveau de risque résiduel est acceptable ou non, sans avoir à solliciter systématiquement un arbitrage individuel de la Direction Générale pour chaque décision.

La définition de l'appétence au risque cyber relève de la responsabilité de la Direction Générale et, pour les organisations les plus matures, du Conseil d'administration — non du RSSI seul, qui n'a pas vocation à définir seul le niveau de risque que l'organisation est disposée à assumer. En pratique, cette appétence peut être formulée de manière qualitative (par exemple : « l'organisation ne tolère aucun risque susceptible de compromettre la continuité des services aux clients au-delà de 24 heures ») ou quantitative, et doit être révisée périodiquement à mesure que le contexte de risque et la maturité de l'organisation évoluent.

6.10 Suivi des plans de traitement

L'identification et l'évaluation des risques ne produisent de valeur que si elles débouchent sur des plans de traitement effectivement mis en œuvre et suivis dans la durée. Le suivi de ces plans doit préciser, pour chaque action, un propriétaire responsable de sa mise en œuvre, une échéance, et des jalons intermédiaires permettant de détecter précocement tout retard ou blocage. Ce suivi doit faire l'objet d'un reporting régulier au comité de sécurité, avec une attention particulière portée aux actions en retard sur les risques les plus critiques.

Une pratique fréquemment observée, et qu'il convient d'éviter, consiste à considérer l'identification et l'évaluation d'un risque comme suffisantes en elles-mêmes, sans assurer un suivi rigoureux de sa remédiation effective : un registre de risques exhaustif mais dont les plans d'action ne progressent pas ne constitue, en définitive, qu'un exercice documentaire sans impact réel sur le niveau de sécurité de l'organisation.

6.11 Méthodes et référentiels : ISO 27005, EBIOS Risk Manager, NIST, OCTAVE

Plusieurs méthodologies reconnues encadrent la démarche de gestion des risques cyber, et le choix de l'une d'entre elles dépend largement du contexte réglementaire, sectoriel et de la maturité de l'organisation. La norme ISO/CEI 27005 fournit un cadre méthodologique général, complémentaire de la norme ISO/CEI 27001 relative aux systèmes de management de la sécurité de l'information, et constitue une référence largement reconnue à l'échelle internationale, y compris par des organismes de certification actifs sur le continent africain.

La méthode EBIOS Risk Manager, développée par l'agence nationale française de sécurité des systèmes d'information, propose une approche structurée en ateliers, centrée sur les scénarios stratégiques et opérationnels de risque, de plus en plus utilisée dans les organisations francophones. Le cadre de gestion des risques du NIST (National Institute of Standards and Technology), notamment au travers du NIST Cybersecurity Framework et du Risk Management Framework, constitue une référence particulièrement répandue dans les organisations en lien avec des partenaires ou clients nord-américains. La méthode OCTAVE, plus ancienne, reste également utilisée, en particulier dans une logique d'auto-évaluation portée par les équipes internes plutôt que par des consultants externes. Le choix d'une méthode importe moins que la constance de son application dans la durée : une méthode simple, appliquée avec rigueur et régularité, produit davantage de valeur qu'une méthode sophistiquée appliquée de manière ponctuelle et superficielle.

Pour éviter qu'un choix de méthode ne devienne un obstacle, la grille suivante rapproche les quatre approches selon des critères pratiques.

Critère	ISO/CEI 27005:2022	EBIOS Risk Manager (v1.5)	NIST (CSF 2.0 / RMF)	OCTAVE (Allegro)
Nature	Cadre de processus de gestion des risques liés à l'information, sans méthode imposée	Méthode d'appréciation et de traitement du risque numérique en cinq ateliers, avec livrables et vocabulaire définis	Cadre de gestion (fonctions et catégories) et processus d'autorisation des systèmes (RMF)	Méthode d'auto-évaluation centrée sur les actifs informationnels
Origine	ISO/CEI (international)	ANSSI (France), avec le Club EBIOS	NIST (États-Unis)	SEI, Carnegie Mellon (États-Unis)
À choisir quand	Un SMSI ISO 27001 existe ou est visé ; besoin d'un cadre reconnu des certificateurs	Systèmes ou services critiques, projets numériques à enjeux, administrations et opérateurs francophones ; besoin de scénarios concrets	Partenaires ou clients nord-américains ; pilotage par fonctions et niveaux de mise en œuvre	Équipes internes souhaitant s'auto-évaluer sans appui extérieur lourd
Ressources nécessaires	Modérées	Élevées (ateliers, animateur formé)	Modérées à élevées	Modérées
Points d'attention	Ne dit pas « comment » : à compléter par une méthode ou des outils internes	Lourdeur sur de petits périmètres : adapter la granularité	Peu prescriptif sur l'analyse de scénarios	Méthode ancienne ; moins de supports actualisés
Articulation	Base de l'appréciation des risques d'un SMSI	Version 1.5 conforme à ISO/CEI 27005:2022 selon l'ANSSI ; peut alimenter un SMSI	Mise en correspondance possible avec ISO 27001	Alimente un registre des risques

Repère pratique. Une organisation visant la certification ISO 27001 s'appuiera sur ISO/CEI 27005 pour le cadre et pourra mobiliser EBIOS RM pour les analyses détaillées de ses systèmes les plus critiques. Une PME privilégiera une démarche simplifiée (registre de quinze à vingt-cinq risques, mesures de base de type CIS Controls) plutôt que de lancer une méthode lourde qu'elle ne pourra pas entretenir.

Le guide recommande aux organisations béninoises, en particulier aux administrations publiques, aux opérateurs de services essentiels et aux opérateurs d'infrastructures d'information critiques (OIIC), de retenir EBIOS Risk Manager comme méthode d'analyse de risque, selon la logique suivante :

1. Une méthode, pas une norme nationale. EBIOS RM est publiée par l'ANSSI française et n'a pas de valeur normative au Bénin. Son adoption relève d'un choix de l'organisation, pas d'une obligation légale.

2. Des arguments pratiques en sa faveur.
   - Elle est rédigée en français, ce qui facilite son appropriation par les équipes et les décideurs.
   - Son découpage (socle de sécurité, scénarios stratégiques, scénarios opérationnels, traitement du risque) convient à l'analyse des systèmes d'information publics et des services essentiels.
   - Sa version 1.5 est alignée sur ISO/CEI 27005:2022, ce qui permet de l'articuler avec un SMSI ISO 27001 et de présenter une analyse lisible par des partenaires internationaux.

3. Conduite à tenir.
   - Si l'ASIN impose ou recommande une autre méthode, appliquer celle-ci.
   - En l'absence d'exigence spécifique, privilégier EBIOS RM pour les systèmes les plus critiques.
   - Pour les périmètres modestes, une démarche simplifiée fondée sur ISO/CEI 27005 reste préférable à une méthode lourde qui ne pourrait pas être entretenue.
   - Dans tous les cas, appliquer la méthode retenue de manière constante, documentée et traçable.



3

BLOC 3

Protéger

Partie VII

Ce bloc présente le socle technique que le RSSI doit comprendre, exiger et contrôler : identités, réseaux, postes, données, sauvegardes, détection, vulnérabilités, cloud et intelligence artificielle (aspects techniques).

Lecture prioritaire pour : RSSI, DSI, équipes techniques et SOC.

Partie	Contenu	Niveau principal
VII	Construire le socle de sécurité (chapitre 7)	Opérer

VII

PARTIE VII · CHAPITRE 7

Construire le socle de sécurité

Les domaines techniques que le RSSI doit maîtriser

CE QUE LA DIRECTION DOIT SAVOIR

1. Le RSSI n'a pas vocation à être l'expert technique de chacun des domaines suivants : il doit en comprendre les enjeux, définir les exigences attendues, et contrôler leur mise en œuvre par la DSI et les équipes techniques.

2. Un socle de sécurité incomplet sur un seul de ces domaines — par exemple l'authentification ou les sauvegardes — peut suffire à rendre inopérantes des mesures par ailleurs solides sur les autres domaines.

3. La Direction n'a pas à maîtriser ces sujets techniquement, mais doit s'assurer que le RSSI dispose d'une vue d'ensemble documentée de la couverture de chacun de ces domaines.

Le RSSI n'a pas vocation à être l'expert technique de chaque domaine listé ci-dessous — cette expertise relève des équipes spécialisées de la DSI, du SOC ou de prestataires externes. Il doit néanmoins en comprendre suffisamment les enjeux pour définir les exigences de sécurité applicables, challenger les choix techniques proposés, et contrôler que la mise en œuvre effective correspond bien à ces exigences. C'est cette capacité à parler le langage de chaque domaine technique, sans nécessairement en maîtriser tous les détails d'implémentation, qui distingue un RSSI efficace d'un RSSI cantonné à un rôle purement administratif.

7.1 Gestion des identités et des accès (IAM)

La gestion des identités et des accès (Identity and Access Management) régit l'ensemble du cycle de vie des identités numériques — création, modification, suspension, suppression — et des droits d'accès associés aux systèmes et applications de l'organisation. Le RSSI doit s'assurer de l'application rigoureuse du principe du moindre privilège, selon lequel chaque utilisateur ne dispose que des droits strictement nécessaires à l'exercice de ses fonctions, et de la mise en place de revues périodiques des habilitations, particulièrement critiques lors des mouvements de personnel (départs, changements de poste), source fréquente de droits d'accès obsolètes et non révoqués.

7.2 Authentification forte et MFA

L'authentification multifacteurs (MFA), qui combine au moins deux éléments de preuve d'identité parmi un mot de passe, un dispositif physique et une caractéristique biométrique, constitue aujourd'hui l'une des mesures de sécurité au meilleur rapport coût-efficacité pour réduire drastiquement le risque de compromission de comptes, principal vecteur d'intrusion observé dans la majorité des incidents recensés. Le RSSI doit prioriser son déploiement, a minima sur l'ensemble des comptes à privilèges et des accès exposés sur internet, avant d'envisager sa généralisation à l'ensemble des utilisateurs.

7.3 Gestion des comptes privilégiés (PAM)

Les comptes privilégiés — administrateurs systèmes, comptes de service, comptes techniques — constituent une cible prioritaire pour tout attaquant, dans la mesure où leur compromission offre un accès étendu aux systèmes de l'organisation. La gestion des accès privilégiés (Privileged Access Management) repose sur des principes spécifiques : inventaire exhaustif de ces comptes, coffre-fort sécurisé pour le stockage des identifiants, traçabilité renforcée des actions réalisées, et limitation stricte du nombre de comptes disposant de privilèges permanents au profit d'un octroi temporaire et justifié des droits élevés.

7.4 Sécurité réseau

La sécurité réseau vise à protéger les infrastructures de communication de l'organisation par une architecture de segmentation limitant la propagation d'une éventuelle intrusion, des équipements de filtrage (pare-feu) contrôlant les flux autorisés, et des dispositifs de détection des intrusions surveillant les comportements anormaux. Le RSSI doit s'assurer que cette architecture est documentée, régulièrement revue, et que les réseaux les plus sensibles (systèmes industriels, données critiques) sont isolés des réseaux plus exposés, en particulier de ceux offrant un accès à Internet.

7.5 Sécurité des postes de travail

Les postes de travail — ordinateurs fixes et portables des collaborateurs — constituent un point d'entrée fréquent pour les attaques, en particulier via l'hameçonnage. Leur sécurisation repose sur un socle de mesures désormais standard : solution de protection contre les logiciels malveillants (antivirus ou EDR), gestion centralisée des mises à jour et correctifs de sécurité, chiffrement du disque en cas de perte ou de vol, et restriction des droits d'administration locale des utilisateurs, mesure simple mais déterminante pour limiter l'impact d'une compromission.

7.6 Sécurité des serveurs

Les serveurs, qu'ils soient hébergés sur site ou dans le cloud, hébergent généralement les données et applications les plus critiques de l'organisation, et requièrent à ce titre un niveau de protection renforcé : durcissement de la configuration selon des standards reconnus, application rigoureuse et rapide des correctifs de sécurité, segmentation vis-à-vis des autres environnements, et surveillance renforcée des accès et des comportements anormaux, en particulier pour les serveurs hébergeant les actifs identifiés comme critiques dans l'analyse de risque de l'organisation.

7.7 Sécurité Cloud

La migration croissante des systèmes d'information vers des environnements cloud (infrastructure, plateforme ou logiciel en tant que service) transforme profondément le périmètre de responsabilité du RSSI, sans pour autant l'alléger : le modèle de responsabilité partagée qui caractérise le cloud impose de clarifier précisément ce qui relève de la sécurité assurée par le fournisseur cloud et ce qui reste de la responsabilité de l'organisation cliente — configuration des accès, chiffrement des données, gestion des identités notamment. Une mauvaise compréhension de cette répartition est une source fréquente d'incidents, la mauvaise configuration des services cloud figurant parmi les causes les plus courantes de fuites de données constatées ces dernières années.

7.8 Sécurité des applications

La sécurité des applications vise à s'assurer que les logiciels développés ou acquis par l'organisation ne présentent pas de vulnérabilités exploitables par un attaquant. Elle repose sur des pratiques telles que les revues de code sécurisé, les tests de sécurité applicative (statiques et dynamiques), la gestion rigoureuse des dépendances logicielles tierces, souvent source de vulnérabilités importées, et l'intégration systématique d'exigences de sécurité dès les phases de conception des projets applicatifs, plutôt qu'un contrôle tardif juste avant mise en production.

7.9 DevSecOps

L'approche DevSecOps consiste à intégrer les exigences et contrôles de sécurité directement dans les chaînes de développement et de déploiement continu (CI/CD) des équipes de développement, plutôt que de les traiter comme une étape de validation séparée et tardive. Cette intégration, qui suppose une collaboration étroite entre le RSSI et les équipes de développement, permet de détecter et corriger les vulnérabilités bien plus tôt dans le cycle de vie des applications, à un coût significativement inférieur à celui d'une correction post-production, tout en préservant la rapidité de mise sur le marché recherchée par les équipes produit.

7.10 Sécurité des bases de données

Les bases de données, qui concentrent souvent les informations les plus sensibles de l'organisation, requièrent des mesures de protection spécifiques : chiffrement des données au repos, contrôle d'accès granulaire limitant les droits aux seuls besoins fonctionnels réels, journalisation des accès aux données sensibles, et masquage ou anonymisation des données dans les environnements de test et de développement, une pratique encore trop rarement appliquée alors qu'elle constitue une source fréquente d'exposition de données réelles hors du périmètre de production sécurisé.

7.11 Chiffrement et gestion des clés

Le chiffrement des données, au repos comme en transit, constitue une mesure de protection fondamentale contre l'accès non autorisé à l'information, y compris en cas de compromission d'un support ou d'interception d'une communication. L'efficacité de cette protection dépend toutefois entièrement de la robustesse de la gestion des clés cryptographiques associées : une clé mal protégée ou mal gérée réduit à néant la protection apportée par le chiffrement lui-même. Le RSSI doit s'assurer de l'existence d'une politique de gestion des clés couvrant leur génération, leur stockage sécurisé, leur rotation périodique et leur révocation en cas de compromission suspectée.

7.12 PKI et services de confiance

L'infrastructure à clés publiques (Public Key Infrastructure, PKI) fournit les mécanismes de certificats numériques permettant d'authentifier des identités, de sécuriser des communications et de garantir l'intégrité de documents électroniques. Ces services de confiance prennent une importance croissante dans les organisations engagées dans des démarches de dématérialisation — signature électronique, certification de documents, authentification de services en ligne — un enjeu particulièrement pertinent dans le contexte de développement des services numériques publics et privés sur le continent africain.

7.13 Sauvegarde et restauration

La sauvegarde des données constitue l'ultime ligne de défense face à un incident majeur, en particulier face à un rançongiciel qui viserait à chiffrer ou détruire les données de production. Une politique de sauvegarde robuste repose sur la règle communément admise dite « 3-2-1 » : conserver au moins trois copies des données, sur deux supports différents, dont une copie isolée hors ligne ou immuable, protégée d'une éventuelle propagation de l'attaque aux sauvegardes elles-mêmes. Le RSSI doit surtout s'assurer que ces sauvegardes font l'objet de tests de restauration réguliers : une sauvegarde jamais testée en restauration ne garantit en réalité rien, un constat malheureusement fréquent lors de la survenue d'incidents réels.

7.14 Journalisation et SIEM

La journalisation consiste à enregistrer de manière systématique les événements significatifs survenant sur les systèmes, applications et équipements de sécurité de l'organisation, constituant une source d'information indispensable tant pour la détection d'activités suspectes que pour l'investigation a posteriori d'un incident. Un système de gestion des informations et des événements de sécurité (SIEM) centralise, corrèle et analyse ces journaux, permettant de détecter des scénarios d'attaque qui resteraient invisibles si chaque source de journal était examinée isolément. Le RSSI doit s'assurer de la couverture suffisante des systèmes critiques par cette journalisation, ainsi que de sa durée de conservation, souvent encadrée par des obligations réglementaires spécifiques.

7.15 Centre des opérations de sécurité (SOC)

Le Centre des Opérations de Sécurité (Security Operations Center, SOC) assure la surveillance continue des systèmes d'information, la détection des incidents de sécurité et la réponse de premier niveau, sur la base des informations remontées notamment par le SIEM. Un SOC peut être interne, externalisé auprès d'un prestataire spécialisé, ou hybride, ce dernier modèle étant fréquemment retenu par des organisations de taille intermédiaire souhaitant bénéficier d'une couverture 24/7 sans supporter le coût d'une équipe interne dédiée à temps

plein. Le RSSI définit les cas d'usage à détecter, les niveaux de service attendus et les procédures d'escalade, quel que soit le modèle organisationnel retenu.

7.16 Gestion des vulnérabilités

La gestion des vulnérabilités consiste à identifier de manière systématique et régulière les failles de sécurité présentes sur les systèmes de l'organisation, au moyen d'outils de scan automatisés et de tests d'intrusion plus approfondis, puis à prioriser et suivre leur correction selon leur niveau de criticité. Un processus de gestion des vulnérabilités mature repose sur un cycle continu — scan, analyse, priorisation, remédiation, vérification — plutôt que sur des campagnes ponctuelles isolées, et s'appuie sur des délais cibles de correction différenciés selon la criticité de la vulnérabilité et l'exposition du système concerné.

Les délais de correction ne devraient pas être déterminés par la seule note de sévérité CVSS, qui mesure la gravité technique théorique d'une faille et non le risque qu'elle fait réellement courir. Une priorisation robuste combine la sévérité (CVSS), l'exploitabilité (existence d'un code d'exploitation public, exploitation active signalée, par exemple dans le catalogue des vulnérabilités exploitées de la CISA ou dans les bulletins d'alerte du bjCSIRT, ou score EPSS), l'exposition (accessible depuis Internet ou seulement en interne) et la criticité de l'actif concerné. Une grille indicative est proposée en Annexe 9, section 3.

7.17 Sécurité physique et environnementale

La sécurité de l'information ne se limite pas à sa dimension numérique : la protection physique des locaux hébergeant les équipements informatiques (contrôle d'accès, vidéosurveillance, protection contre l'incendie et les dégâts des eaux) et la protection environnementale (alimentation électrique de secours, climatisation des salles serveurs) constituent des prérequis souvent négligés mais essentiels à la disponibilité des systèmes. Ces enjeux revêtent une importance particulière dans des contextes où la fiabilité des infrastructures électriques n'est pas toujours garantie, justifiant des dispositifs de continuité électrique robustes pour les équipements critiques.

7.18 Sécurité des équipements mobiles

La généralisation des smartphones, tablettes et ordinateurs portables professionnels, ainsi que le développement de pratiques telles que le BYOD (Bring Your Own Device, utilisation d'équipements personnels à des fins professionnelles), élargit considérablement la surface d'exposition de l'organisation. La sécurisation de ces équipements repose sur des solutions de gestion des terminaux mobiles (Mobile Device Management), permettant d'imposer des règles de sécurité minimales (chiffrement, verrouillage, effacement à distance en cas de perte), et sur des politiques claires encadrant les usages autorisés, en particulier pour les équipements personnels accédant à des ressources professionnelles.

7.19 Sécurité de l'Internet des objets (IoT)

Le déploiement croissant d'objets connectés — capteurs industriels, équipements de vidéosurveillance, dispositifs médicaux connectés, compteurs intelligents — introduit une catégorie de risques spécifique, ces équipements présentant souvent des capacités de sécurisation limitées (mots de passe par défaut non modifiés, absence de mécanisme de mise à jour, protocoles de communication peu sécurisés) tout en étant connectés au système d'information de l'organisation. Le RSSI doit veiller à l'inventaire de ces équipements, à leur isolement sur des segments réseau dédiés, et à l'intégration d'exigences de sécurité minimales dans les processus d'acquisition de ce type de matériel.

7.20 Sécurité des systèmes d'intelligence artificielle

L'adoption croissante de systèmes d'intelligence artificielle, notamment générative, au sein des organisations introduit des risques émergents que le RSSI doit désormais intégrer à son périmètre de vigilance : fuite de données sensibles via des outils d'IA grand public utilisés sans cadre par les collaborateurs, manipulation de modèles par injection de contenus malveillants, biais ou erreurs dans les décisions automatisées, et usage de l'IA générative par des attaquants pour industrialiser des campagnes d'hameçonnage ou générer des contenus frauduleux crédibles. Ce domaine, encore en construction sur le plan des référentiels et des pratiques, nécessite du RSSI une veille active et l'établissement, même provisoire, d'un cadre d'usage encadrant le recours de l'organisation à ces technologies.



4

BLOC 4

Réagir et résister

Parties VIII à IX

Ce bloc prépare l'organisation à l'incident et à l'indisponibilité : détection, réponse, crise, circuit béninois de déclaration, continuité et reprise d'activité.

Lecture prioritaire pour : Direction générale (rôle en cellule de crise), RSSI, DSI, responsable de la continuité, communication, juridique.

Partie	Contenu	Niveau principal
VIII	Gestion des incidents et crises cyber (chapitre 8)	Piloter / Opérer
IX	Continuité d'activité et résilience (chapitre 9)	Piloter / Opérer

VIII

PARTIE VIII · CHAPITRE 8

Gestion des incidents et crises cyber

Le RSSI face à l'incident de cybersécurité

CE QUE LA DIRECTION DOIT SAVOIR

1. Aucun dispositif de sécurité, aussi robuste soit-il, n'élimine totalement le risque d'incident : la préparation à la réponse est donc aussi importante que la prévention elle-même.

2. La qualité de la réponse à un incident — rapidité, coordination, communication — a souvent plus d'impact sur les conséquences finales pour l'organisation que la gravité initiale de l'incident lui-même.

3. La Direction générale doit connaître, avant qu'une crise ne survienne, son rôle précis au sein de la cellule de crise cyber.

8.1 Définition d'un incident

Un incident de sécurité de l'information peut être défini comme tout événement, avéré ou suspecté, portant atteinte ou susceptible de porter atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information ou des systèmes qui la traitent. Cette définition volontairement large couvre un spectre très étendu de situations, depuis un incident mineur sans conséquence opérationnelle (tentative d'hameçonnage bloquée, alerte de sécurité sans exploitation avérée) jusqu'à la crise majeure menaçant la continuité de l'organisation (rançongiciel paralysant l'ensemble des systèmes, fuite massive de données sensibles).

Il est essentiel que l'organisation dispose d'une définition claire et partagée de ce qui constitue un incident devant être formellement déclaré et traité selon le processus établi, faute de quoi des événements significatifs risquent de ne jamais être signalés, par méconnaissance du seuil de déclaration ou par crainte, mal fondée, de conséquences négatives pour celui qui les rapporte.

8.2 Préparation

La préparation à la gestion des incidents constitue l'étape la plus déterminante, bien qu'elle se déroule en amont de toute crise réelle : elle conditionne directement la rapidité et l'efficacité de la réponse le jour où un incident survient effectivement. Cette préparation comprend l'élaboration d'un plan de réponse aux incidents de cybersécurité documenté (voir section 8.12), la constitution et la formation d'une équipe de réponse, la mise en place d'outils de détection et d'investigation, et la conduite régulière d'exercices de simulation (voir section 8.13) permettant de tester et d'améliorer continuellement ce dispositif.

Une préparation insuffisante se traduit systématiquement, lors d'un incident réel, par une perte de temps précieuse consacrée à improviser une organisation de crise plutôt qu'à traiter l'incident lui-même, par des décisions prises dans la précipitation faute de procédures préétablies, et par une communication de crise défaillante qui aggrave souvent les conséquences réputationnelles bien au-delà de l'impact technique initial de l'incident.

8.3 Détection

La phase de détection consiste à identifier qu'un incident est en cours ou a eu lieu, à travers des mécanismes automatisés (alertes du SIEM, du SOC, des solutions de protection des postes) ou des signalements humains (collaborateur constatant un comportement anormal, alerte d'un client ou d'un partenaire, notification d'un tiers tel qu'un chercheur en sécurité). La capacité de détection d'une organisation, mesurée notamment par le délai moyen de détection (Mean Time To Detect), constitue l'un des indicateurs les plus révélateurs de la maturité réelle de son dispositif de sécurité, comme évoqué à la section 4.7 de ce guide.

8.4 Qualification

Une fois un événement détecté, la phase de qualification consiste à déterminer s'il s'agit effectivement d'un incident de sécurité avéré, à en évaluer la nature, l'ampleur et la criticité, et à déclencher le niveau de réponse approprié — traitement courant par les équipes opérationnelles pour un incident mineur, activation de la cellule de crise pour un incident majeur. Cette qualification, qui doit intervenir le plus rapidement possible après la détection, s'appuie sur une grille de criticité préétablie, permettant d'objectiver la décision plutôt que de la laisser à la seule appréciation, potentiellement variable, de la personne en charge de l'analyse initiale.

8.5 Containment (endiguement)

L'endiguement (containment) vise à limiter la propagation et l'aggravation de l'incident, par des mesures telles que l'isolement des systèmes compromis, la désactivation de comptes utilisés par l'attaquant, ou la coupure temporaire de certains accès réseau. Ces mesures, souvent radicales et pouvant avoir un impact opérationnel significatif (interruption d'un service, indisponibilité d'une application), doivent pouvoir être décidées rapidement, ce qui suppose une délégation de pouvoir clairement établie au bénéfice du RSSI ou du responsable de la cellule de crise, comme évoqué à la section 3.10 de ce guide relative à la délégation de pouvoirs.

8.6 Éradication

L'éradication consiste à éliminer la cause profonde de l'incident — suppression du logiciel malveillant, fermeture de la vulnérabilité exploitée, révocation des accès compromis — de manière à s'assurer que l'attaquant ne dispose plus d'aucun point d'accès résiduel au système d'information. Cette phase, techniquement exigeante, nécessite souvent le recours à une expertise spécialisée en investigation numérique (forensic), en particulier pour les incidents les plus sophistiqués, afin de s'assurer qu'aucun mécanisme de persistance n'a été laissé en place par l'attaquant avant la phase de restauration.

8.7 Restauration

La restauration consiste à remettre en fonctionnement normal les systèmes affectés par l'incident, à partir de sauvegardes saines lorsque cela est nécessaire, en s'assurant que l'éradication a été complète avant toute remise en production, sous peine de restaurer un système encore compromis. Cette phase doit être conduite de manière méthodique et progressive, avec une surveillance renforcée des systèmes restaurés durant la période suivant immédiatement l'incident, afin de détecter rapidement tout signe de compromission résiduelle ou de récidive.

8.8 Retour d'expérience

Chaque incident significatif doit donner lieu à un retour d'expérience formalisé (post-mortem), conduit dans un esprit constructif d'amélioration continue plutôt que de recherche de responsabilité individuelle, qui analyse le déroulement de l'incident, l'efficacité de la réponse apportée, et les enseignements à tirer pour améliorer la prévention, la détection ou la réponse future. Ce retour d'expérience doit déboucher sur des actions concrètes, intégrées au plan de traitement des risques, et non rester un exercice purement documentaire sans suite opérationnelle. C'est cette capacité d'apprentissage continu qui distingue une organisation dont la maturité en matière de sécurité progresse réellement dans le temps.

8.9 Communication de crise

La communication, interne et externe, constitue une dimension à part entière de la gestion d'un incident majeur, dont la qualité influence directement les conséquences réputationnelles de l'événement. Une communication transparente, factuelle et maîtrisée dans son calendrier limite les rumeurs et la perte de confiance ; une communication tardive, contradictoire ou perçue comme dissimulatrice aggrave systématiquement les conséquences de l'incident, indépendamment même de sa gravité technique réelle. Le RSSI doit contribuer à la préparation d'éléments de langage factuels, mais la décision et la responsabilité de la communication externe relèvent de la Direction générale et de la fonction communication de l'organisation.

8.10 Gestion des relations avec les parties prenantes de l'incident

La gestion d'un incident majeur mobilise un ensemble de parties prenantes dont les attentes et les besoins d'information diffèrent :

- la Direction générale, qui doit être informée sans délai et associée aux décisions structurantes ;
- la DSI, partenaire opérationnel indispensable de la réponse technique ;
- les autorités compétentes, notamment lorsque l'incident implique des données personnelles ou relève d'obligations sectorielles de notification ;
- les forces de sécurité, en cas d'infraction pénale avérée ;
- les prestataires, en particulier ceux impliqués dans les systèmes affectés ou mobilisés en renfort ;
- les clients, lorsque l'incident affecte des services ou des données les concernant ;
- les médias, dans les situations où l'incident acquiert une dimension publique.

La coordination de ces relations, qui ne peut reposer sur la seule improvisation le jour de l'incident, doit être anticipée dans le plan de réponse aux incidents de cybersécurité, avec une identification préalable des interlocuteurs, des canaux de communication et des responsabilités de chacun, afin d'éviter la confusion et les messages contradictoires qui caractérisent trop souvent la gestion des crises non préparées.

8.11 Cellule de crise cyber

La cellule de crise cyber est l'instance exceptionnelle activée en cas d'incident majeur, réunissant les décideurs et experts nécessaires à la gestion coordonnée de la crise : Direction générale, RSSI, DSI, direction juridique, direction de la communication, et selon les cas direction des ressources humaines ou direction métier concernée. Cette cellule a vocation à centraliser la prise de décision durant la crise, à assurer la coordination entre les équipes techniques et les décideurs, et à cadencer la communication interne et externe.

La composition précise de cette cellule, les rôles de chacun de ses membres et les modalités de son activation doivent être définis en amont, dans le cadre du plan de réponse aux incidents de cybersécurité, et non improvisés au moment où survient la crise. Il est notamment essentiel que la Direction générale connaisse précisément, avant qu'une crise ne survienne, son rôle au sein de cette cellule — rôle qui n'est généralement pas celui d'un pilotage technique, mais celui de la prise de décisions stratégiques (arbitrage sur le paiement éventuel d'une rançon, décision de communication publique, mobilisation de ressources exceptionnelles) sur la base des éléments présentés par le RSSI et la cellule opérationnelle.

8.12 Plan de Réponse aux Incidents de Cybersécurité (PRIC)

Le Plan de Réponse aux Incidents de Cybersécurité (PRIC) est le document de référence qui formalise l'ensemble du dispositif décrit dans les sections précédentes : définition des niveaux de criticité, procédures de qualification et d'escalade, composition et modalités d'activation de la cellule de crise, contacts des parties prenantes internes et externes, modèles de communication préétablis, et procédures techniques de containment, d'éradication et de restauration pour les scénarios les plus probables. Ce document doit être accessible même en cas d'indisponibilité des systèmes d'information habituels — un incident majeur pouvant précisément rendre inaccessible l'intranet ou la messagerie sur lesquels ce plan serait exclusivement stocké.

Un plan de réponse aux incidents de cybersécurité qui n'a jamais été testé reste, comme une sauvegarde jamais restaurée, une garantie largement théorique : c'est l'objet des exercices de simulation, développés à la section suivante, que de transformer ce document en une capacité opérationnelle réellement mobilisable le jour où elle devient nécessaire.

8.13 Exercices de simulation

Les exercices de simulation de crise cyber consistent à mettre en situation, de manière contrôlée, les équipes et décideurs concernés face à un scénario d'incident réaliste, afin de tester le plan de réponse, d'identifier ses lacunes, et de familiariser l'ensemble des parties prenantes avec leur rôle avant qu'une crise réelle ne survienne. Ces exercices peuvent prendre plusieurs formes, du simple exercice sur table (tabletop exercise), consistant en une discussion structurée autour d'un scénario sans mobilisation technique réelle, jusqu'à la simulation technique complète impliquant l'activation effective des procédures de containment et de restauration sur des environnements de test.

La conduite régulière de ces exercices — au moins annuellement pour les organisations les plus exposées — présente un double bénéfice : elle améliore concrètement la préparation opérationnelle de l'organisation, et elle constitue, pour la Direction générale et les administrateurs, l'occasion la plus tangible de mesurer, en dehors de toute crise réelle, la maturité effective du dispositif de réponse aux incidents de leur organisation, souvent plus révélatrice qu'un rapport d'audit purement documentaire.

IX

PARTIE IX · CHAPITRE 9

Continuité d'activité et résilience

Préparer l'organisation à l'indisponibilité

CE QUE LA DIRECTION DOIT SAVOIR

1. La continuité d'activité ne se limite pas à la sauvegarde des données : elle consiste à garantir que les processus essentiels de l'organisation peuvent se poursuivre, ou reprendre rapidement, en cas de sinistre cyber majeur.

2. Les délais de reprise (RTO) et de perte de données maximale tolérée (RPO) sont des décisions de gestion, pas des paramètres techniques : c'est à la Direction de les fixer, sur proposition du RSSI.

3. Un plan de continuité jamais testé offre une garantie largement illusoire — seul un test réel révèle s'il fonctionnera le jour venu.

9.1 Analyse d'impact sur l'activité (BIA)

L'analyse d'impact sur l'activité (Business Impact Analysis, BIA) est l'exercice fondateur de toute démarche de continuité d'activité : elle consiste à évaluer, pour chaque processus métier de l'organisation, les conséquences d'une interruption prolongée — pertes financières, impact réglementaire, atteinte à la réputation, conséquences pour les clients ou les usagers — et à en déduire le degré de criticité et les délais de reprise tolérables. Cette analyse permet de hiérarchiser les processus, tous ne justifiant pas le même niveau d'investissement en matière de résilience.

La BIA doit être conduite en étroite collaboration avec les directions métier, qui sont seules en mesure d'apprécier avec précision les conséquences réelles d'une interruption de leurs activités — le RSSI apportant la méthodologie et la vision transverse, sans se substituer à l'expertise métier. Cet exercice, souvent perçu comme fastidieux, constitue pourtant le socle sans lequel l'ensemble du dispositif de continuité repose sur des hypothèses non vérifiées quant à ce qui est réellement critique pour l'organisation.

9.2 Plan de continuité d'activité (PCA)

Le Plan de Continuité d'Activité (PCA) définit l'ensemble des dispositions organisationnelles, humaines et techniques permettant à l'organisation de maintenir ou de reprendre rapidement ses activités essentielles en cas de sinistre majeur, quelle qu'en soit l'origine — cyber, naturelle, sanitaire, ou autre. Ce document couvre notamment les modes de fonctionnement dégradés envisageables, les ressources de secours mobilisables (sites de repli, équipements alternatifs), et l'organisation de crise permettant de piloter la reprise d'activité.

Le PCA ne se substitue pas au Plan de Reprise d'Activité (PRA), développé à la section suivante, qui en constitue le volet spécifiquement technique et informatique : le PCA porte une vision englobante de la continuité des processus métier, tandis que le PRA se concentre sur la reprise des systèmes d'information qui les soutiennent. Le RSSI contribue activement à l'élaboration du PCA pour la dimension liée aux scénarios de sinistre cyber, mais la responsabilité globale du PCA relève généralement d'une fonction dédiée ou de la Direction générale elle-même.

9.3 Plan de reprise d'activité (PRA)

Le Plan de Reprise d'Activité (PRA) formalise les procédures techniques permettant de restaurer les systèmes d'information après un sinistre, dans les délais fixés par la BIA. Il précise, pour chaque système critique, les modalités de reprise — basculement vers un site de secours, restauration à partir de sauvegardes, activation d'une infrastructure de repli hébergée dans le cloud — ainsi que l'ordre de priorité de reprise des différents systèmes, une organisation ne pouvant généralement pas restaurer l'ensemble de son système d'information simultanément.

L'élaboration du PRA relève d'une responsabilité partagée entre le RSSI, qui apporte l'expertise sur les scénarios de sinistre cyber et les exigences de sécurité

applicables à la reprise, et la DSI, responsable de la mise en œuvre technique effective des mécanismes de reprise. Un PRA insuffisamment documenté ou reposant sur des compétences individuelles non formalisées constitue une fragilité majeure, particulièrement si les personnes détentrices de ce savoir venaient à quitter l'organisation.

9.4 RTO et RPO

Le délai de reprise cible (Recovery Time Objective, RTO) désigne le temps maximal tolérable d'indisponibilité d'un système avant que les conséquences ne deviennent inacceptables pour l'organisation, tandis que la perte de données maximale tolérée (Recovery Point Objective, RPO) désigne la quantité maximale de données que l'organisation accepte de perdre, exprimée en durée depuis la dernière sauvegarde valide. Ces deux paramètres, définis pour chaque système critique à partir des conclusions de la BIA, structurent l'ensemble des choix techniques de la stratégie de sauvegarde et de reprise.

Un point essentiel, souvent mal compris, mérite d'être souligné : le RTO et le RPO ne sont pas des paramètres techniques que le RSSI ou la DSI peuvent fixer seuls, mais des décisions de gestion qui engagent des arbitrages coûteux — un RTO très court impose généralement des investissements en infrastructures de secours nettement plus onéreux qu'un RTO plus tolérant. Il revient à la Direction générale, éclairée par le RSSI, de valider ces objectifs pour chaque système critique, en connaissance de leurs implications budgétaires.

9.5 Stratégie de sauvegarde

La stratégie de sauvegarde, déjà évoquée sous son angle technique à la section 7.13, doit être directement articulée avec les objectifs de RPO fixés pour chaque système : un RPO de quatre heures suppose une fréquence de sauvegarde au moins équivalente, tandis qu'un RPO de vingt-quatre heures peut se satisfaire d'une sauvegarde quotidienne. Cette articulation entre exigence métier (le RPO) et mise en œuvre technique (la fréquence et la méthode de sauvegarde) illustre la manière dont le RSSI doit traduire des exigences de gouvernance en spécifications techniques concrètes pour la DSI.

9.6 Résilience des infrastructures

La résilience des infrastructures désigne la capacité du système d'information à absorber une défaillance partielle sans interruption de service, grâce à des mécanismes de redondance — duplication des serveurs critiques, redondance des liens réseau et des sources d'alimentation électrique, réplication des données entre plusieurs sites géographiquement distincts. Cet enjeu revêt une importance particulière dans des contextes où la fiabilité des infrastructures énergétiques et de connectivité n'est pas toujours garantie, justifiant des investissements en résilience proportionnés à ces contraintes spécifiques plutôt qu'un simple copier-coller de standards conçus pour des environnements plus stables.

9.7 Scénarios de crise cyber

Au-delà des scénarios de sinistre classiques (incendie, panne matérielle, catastrophe naturelle), le PCA et le PRA doivent intégrer explicitement des scénarios propres à la crise cyber, dont les caractéristiques diffèrent sensiblement : un rançongiciel peut affecter simultanément les systèmes de production et leurs sauvegardes si celles-ci ne sont pas correctement isolées ; une fuite de données massive peut ne nécessiter aucune interruption technique mais exiger une gestion de crise réputationnelle et réglementaire intense ; une compromission prolongée et non détectée peut nécessiter une reconstruction complète de l'infrastructure plutôt qu'une simple restauration.

Cette spécificité des scénarios cyber, encore insuffisamment prise en compte dans de nombreux plans de continuité hérités d'une approche centrée sur les sinistres physiques traditionnels, justifie une revue régulière, pilotée par le RSSI, de la pertinence du PCA et du PRA au regard de l'évolution du paysage des cybermenaces décrit à la section 1.1 de ce guide.

9.8 Tests de PRA

Le test du Plan de Reprise d'Activité consiste à vérifier, de manière contrôlée, la capacité effective de l'organisation à restaurer ses systèmes critiques dans les délais et avec le niveau de perte de données fixés par le RTO et le RPO. Ces tests peuvent prendre plusieurs formes, de la simple vérification documentaire jusqu'au test grandeur nature avec bascule effective vers un site de secours, cette dernière modalité, la plus exigeante, étant aussi la seule à révéler véritablement les failles opérationnelles d'un dispositif qui, sur le papier, paraît complet.

La fréquence recommandée de ces tests — généralement annuelle pour les systèmes les plus critiques — doit être proportionnée à l'enjeu que représente chaque système, et chaque test doit donner lieu à un rapport documentant les écarts constatés entre les objectifs fixés et les résultats obtenus, ainsi qu'un plan d'action pour les corriger avant le test suivant.

9.9 Exercices de crise

Complémentaires aux tests techniques du PRA, les exercices de crise, déjà évoqués à la section 8.13 dans le contexte spécifique de la réponse aux incidents, permettent de tester la dimension organisationnelle et décisionnelle de la continuité d'activité : mobilisation de la cellule de crise, communication interne et externe, prise de décision sous contrainte de temps et d'incertitude. Ces exercices, qui gagnent à associer les membres de la Direction générale et non les seules équipes techniques, constituent le meilleur moyen de vérifier que l'organisation dans son ensemble — et pas seulement ses systèmes informatiques — est réellement prête à faire face à une crise majeure.



5

BLOC 5

Piloter

Parties X à XIV

Ce bloc regroupe les leviers de maîtrise transverses et de pilotage : conformité, personnes, tiers, reporting et budget. Les parties XI et XII (personnes et tiers) relèvent aussi de la protection ; elles figurent ici pour respecter l'ordre des parties.

Lecture prioritaire pour : RSSI, DPO, juridique, DRH, achats, direction financière, Direction générale.

Partie	Contenu	Niveau principal
X	Conformité et réglementation (chapitre 10)	Piloter
XI	Le RSSI et les ressources humaines (chapitre 11)	Piloter / Opérer
XII	Le RSSI et les fournisseurs (chapitre 12)	Piloter
XIII	Pilotage et reporting du RSSI (chapitre 13)	Décider / Piloter
XIV	Budget et investissements cybersécurité (chapitre 14)	Décider

X

PARTIE X · CHAPITRE 10

Conformité et réglementation

Le RSSI et les exigences réglementaires

CE QUE LA DIRECTION DOIT SAVOIR

1

La non-conformité réglementaire en matière de sécurité de l'information expose l'organisation à des sanctions financières et administratives, mais aussi à un risque commercial croissant, de nombreux clients et partenaires exigeant désormais des garanties contractuelles de conformité.

2

Le cadre réglementaire africain relatif à la protection des données et à la cybersécurité se développe rapidement : une conformité perçue comme acquise peut devenir obsolète en quelques mois.

3

Une certification (ISO 27001 notamment) est un outil de crédibilisation externe utile, mais ne dispense pas de la démarche de gestion des risques qui doit rester au cœur de l'action du RSSI.

10.1 Pourquoi la conformité fait partie des responsabilités du RSSI

La conformité réglementaire et normative constitue l'une des responsabilités centrales du RSSI, pour une raison simple : la plupart des obligations légales et sectorielles applicables à la sécurité de l'information se traduisent concrètement par des exigences techniques et organisationnelles relevant directement de son périmètre — protection des données personnelles, notification des incidents, mesures de sécurité minimales. Le RSSI n'est cependant généralement pas seul responsable de la conformité de l'organisation dans son ensemble : il collabore étroitement avec la direction juridique et, lorsqu'elle existe, la fonction conformité, chacun apportant son expertise propre — juridique et réglementaire d'un côté, technique et opérationnelle de l'autre.

Cette collaboration doit être structurée dès la phase de veille réglementaire, afin que l'organisation ne découvre pas une nouvelle obligation légale au moment de son entrée en vigueur, mais dispose du temps nécessaire pour s'y préparer. Un défaut de conformité constaté a posteriori, lors d'un contrôle ou à l'occasion d'un incident rendu public, est nettement plus coûteux à corriger, tant financièrement que sur le plan réputationnel, qu'une mise en conformité anticipée et maîtrisée.

10.2 Réglementation nationale

Chaque organisation doit identifier précisément le corpus de textes nationaux qui lui est applicable en matière de sécurité de l'information et de protection des données, ce corpus variant significativement d'un pays à l'autre sur le continent africain selon le degré de maturité législative atteint. Ce travail d'identification, qui relève typiquement de la direction juridique en lien avec le RSSI, doit être documenté et actualisé régulièrement, la production législative dans ce domaine connaissant une accélération notable dans plusieurs pays du continent au cours des dernières années.

CONTEXTE BÉNINOIS — IDENTIFIER LE CORPUS APPLICABLE

Pour une organisation établie au Bénin, le corpus de référence comprend en premier lieu le Code du numérique (loi n° 2017-20 du 20 avril 2018, modifiée par la loi n° 2020-35 du 6 janvier 2021), la PSSIE (décret n° 2021-550) pour les structures de l'État, les règles de protection des infrastructures d'information critiques (décret n° 2023-060) pour les OIIC, ainsi que les textes sectoriels applicables. La liste commentée figure en Annexe 3.

Bonnes pratiques de veille : suivre les publications du Secrétariat général du Gouvernement (textes), de l'ASIN et du bjCSIRT (sécurité numérique), de l'APDP (données personnelles) et des autorités sectorielles, et consigner la date de dernière vérification de chaque texte dans le registre des obligations applicables.

10.3 Protection des données personnelles

La protection des données à caractère personnel constitue le domaine réglementaire le plus structuré et le plus largement adopté à l'échelle du

continent africain, de nombreux pays s'étant dotés de législations inspirées, à des degrés divers, du Règlement général européen sur la protection des données (RGPD) ou de la Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles (Convention de Malabo). Ces textes imposent généralement des obligations de sécurisation des traitements de données personnelles, de notification des violations de données aux autorités compétentes et aux personnes concernées, et de désignation, dans certains cas, d'un responsable dédié — le DPO évoqué à la section 2.9 de ce guide.

Le RSSI joue un rôle déterminant dans la mise en œuvre technique de ces obligations : sécurisation des traitements, contrôle d'accès aux données personnelles, chiffrement, capacité de détection et de notification rapide des violations de données dans les délais impartis par la réglementation applicable, ces délais étant généralement très contraints (souvent 72 heures dans les cadres inspirés du RGPD, alors que le Code du numérique béninois retient la formule « sans délai ») et supposant un dispositif de détection et de qualification des incidents suffisamment réactif, tel que décrit dans la Partie VIII de ce guide.

10.4 Cybercriminalité

Un nombre croissant de pays africains se sont dotés de législations spécifiques réprimant la cybercriminalité — accès frauduleux à un système d'information, altération de données, fraude informatique — qui offrent au RSSI un cadre juridique lui permettant, en cas d'incident avéré résultant d'une action malveillante, d'engager une action pénale en collaboration avec les autorités compétentes. Le RSSI doit connaître l'existence de ce cadre et les modalités pratiques de dépôt de plainte, ainsi que les exigences de préservation de la preuve numérique qui conditionnent la recevabilité d'une telle action, ce qui suppose une coordination étroite avec les équipes d'investigation numérique (forensic) dès les premières heures d'un incident.

10.5 Services numériques

Au-delà de la protection des données, certains textes encadrent spécifiquement la sécurité des services numériques eux-mêmes — services financiers mobiles, plateformes de commerce électronique, services d'administration en ligne — imposant des exigences particulières de sécurité, de disponibilité et parfois d'hébergement local des données. Ces réglementations, souvent sectorielles, se développent rapidement dans plusieurs pays du continent, en cohérence avec l'essor de ces services, et méritent une veille attentive de la part du RSSI dans les organisations concernées.

10.6 Exigences sectorielles

Certains secteurs d'activité — services financiers et bancaires, télécommunications, énergie, santé — sont soumis à des exigences de sécurité spécifiques, imposées par des régulateurs sectoriels (banques centrales, autorités de régulation des

télécommunications) en complément du cadre légal général. Ces exigences sectorielles, souvent plus précises et plus contraignantes que la réglementation générale, imposent fréquemment des obligations de reporting périodique au régulateur, de notification rapide des incidents significatifs, et parfois d'audit de sécurité réalisé par un tiers indépendant, autant d'obligations que le RSSI doit intégrer à son calendrier de conformité.

10.7 Normes internationales : ISO 27001, ISO 27701, NIST CSF, CIS Controls, COBIT

Au-delà des obligations réglementaires proprement dites, plusieurs référentiels normatifs internationaux, d'application volontaire, structurent les pratiques de sécurité reconnues à l'échelle mondiale. La norme ISO/CEI 27001 définit les exigences d'un système de management de la sécurité de l'information et fait l'objet d'une certification reconnue, de plus en plus exigée dans les appels d'offres internationaux et par les grands donneurs d'ordre. La norme ISO/CEI 27701 en constitue l'extension spécifique à la gestion de la vie privée et des données personnelles.

Le NIST Cybersecurity Framework, développé par l'agence américaine de normalisation, propose une structure d'évaluation et de pilotage de la cybersécurité largement adoptée au-delà même des frontières américaines, en raison de sa clarté et de sa souplesse d'application. Les CIS Controls (Center for Internet Security) offrent une liste priorisée de mesures techniques concrètes, particulièrement utile pour les organisations souhaitant structurer rapidement un socle de sécurité minimal sans investissement méthodologique lourd. COBIT (Control Objectives for Information and Related Technologies), enfin, propose un cadre plus large de gouvernance des technologies de l'information, dans lequel la sécurité constitue l'une des dimensions parmi d'autres. Le choix d'un ou plusieurs de ces référentiels dépend des objectifs de l'organisation — certification, structuration interne, ou réponse à des exigences contractuelles spécifiques.

10.8 Audit et certification

La démarche de certification, notamment selon la norme ISO/CEI 27001, constitue pour de nombreuses organisations un objectif structurant qui impose une rigueur méthodologique bénéfique à l'ensemble du dispositif de sécurité, au-delà même de la valeur de crédibilisation externe qu'elle procure auprès des clients, partenaires et investisseurs. Cette démarche suppose la mise en place d'un système de management de la sécurité de l'information documenté, des audits internes réguliers, et un audit de certification réalisé par un organisme accrédité, suivi d'audits de surveillance périodiques pour le maintien de la certification.

Il est essentiel de garder à l'esprit qu'une certification atteste de la conformité à un référentiel de processus, et non d'une absence totale de risque : une organisation certifiée peut malgré tout subir un incident de sécurité, la certification garantissant l'existence d'un système de gestion structuré plutôt qu'une invulnérabilité illusoire. Le RSSI doit veiller à ce que la démarche de certification ne devienne pas une fin en soi déconnectée de la gestion réelle des risques, un écueil parfois observé

lorsque la préparation d'un audit de certification mobilise l'essentiel de l'énergie de l'équipe sécurité au détriment du traitement effectif des risques les plus critiques.

10.9 Gestion des écarts de conformité

Tout exercice d'évaluation de conformité — audit interne, audit de certification, contrôle réglementaire — fait apparaître des écarts, qu'il s'agisse de non-conformités mineures ou d'insuffisances plus significatives. La gestion de ces écarts doit s'appuyer sur un processus structuré : documentation précise de l'écart constaté, analyse de sa cause racine, définition d'un plan d'action correctif avec échéance et responsable désigné, et vérification de son efficacité une fois mis en œuvre.

Un registre des écarts de conformité, distinct mais articulé avec le registre des risques évoqué à la section 6.7, permet de disposer d'une vision consolidée de l'état de conformité de l'organisation et de son évolution dans le temps, un outil particulièrement précieux lors de la préparation d'un nouvel audit ou d'un contrôle réglementaire, et qui témoigne, vis-à-vis d'un régulateur, d'une démarche active de mise en conformité plutôt que d'une négligence.

XI

PARTIE XI · CHAPITRE 11

Le RSSI et les ressources humaines

La dimension humaine de la cybersécurité

CE QUE LA DIRECTION DOIT SAVOIR

1. La grande majorité des incidents de sécurité trouvent leur origine, directe ou indirecte, dans un facteur humain — erreur, négligence ou manipulation — ce qui fait de la dimension humaine un levier au moins aussi important que la technique.

2. La pénurie de compétences cyber, particulièrement aiguë dans plusieurs pays africains, doit être anticipée par une politique active de formation et de fidélisation, plutôt que subie.

3. Les processus d'arrivée et de départ des collaborateurs sont des moments à haut risque pour la sécurité de l'information, trop souvent traités comme de simples formalités administratives.

11.1 Sensibilisation

La sensibilisation à la sécurité de l'information vise à informer l'ensemble des collaborateurs des risques auxquels l'organisation est exposée et des comportements attendus pour les prévenir — reconnaissance des tentatives d'hameçonnage, bonnes pratiques de gestion des mots de passe, signalement des incidents suspects. Pour être efficace, cette sensibilisation doit être récurrente plutôt que ponctuelle, adaptée aux différents profils de collaborateurs plutôt qu'uniforme, et mobiliser des formats variés — sessions présentielles, modules en ligne, campagnes de simulation d'hameçonnage, communications régulières — plutôt qu'un unique support statique rapidement oublié.

L'efficacité d'un programme de sensibilisation se mesure moins à la satisfaction déclarée des participants qu'à des indicateurs comportementaux concrets, tels que le taux de clic lors des campagnes de simulation d'hameçonnage ou le taux de signalement spontané d'emails suspects, développés dans le tableau de bord du RSSI en Partie XIII de ce guide.

11.2 Formation

Distincte de la sensibilisation générale, qui s'adresse à l'ensemble des collaborateurs, la formation vise des publics disposant de responsabilités spécifiques en matière de sécurité — développeurs formés aux pratiques de développement sécurisé, administrateurs systèmes formés au durcissement des configurations, équipe du SOC formée aux techniques de détection et d'investigation. Cette formation ciblée, plus technique et approfondie, constitue un investissement direct dans la réduction du risque, dans la mesure où une part significative des vulnérabilités trouve son origine dans des pratiques inadéquates plutôt que dans une malveillance délibérée.

11.3 Culture de cybersécurité

Au-delà des actions ponctuelles de sensibilisation et de formation, l'enjeu de long terme pour le RSSI est de contribuer à l'instauration d'une véritable culture de la sécurité, c'est-à-dire d'un ensemble de réflexes et de valeurs partagés qui font que la sécurité est intégrée naturellement dans les décisions quotidiennes des collaborateurs, plutôt que perçue comme une contrainte externe imposée. Cette culture se construit dans la durée, par l'exemplarité du management, par une communication positive valorisant les bons comportements plutôt qu'uniquement les sanctions, et par l'implication des directions métier elles-mêmes dans le portage des messages de sécurité, plutôt qu'une communication exclusivement descendante émanant du seul RSSI.

11.4 Gestion des habilitations

La gestion des habilitations, déjà évoquée sous son angle technique à la section 7.1, comporte une dimension humaine et organisationnelle essentielle : elle suppose

un processus clair de demande, de validation et de révocation des droits d'accès, impliquant les responsables hiérarchiques des collaborateurs concernés, ainsi que des revues périodiques permettant de détecter et corriger les habilitations excessives ou obsolètes accumulées au fil du temps, un phénomène connu sous le nom de « dérive des privilèges » et particulièrement fréquent dans les organisations où les mouvements internes de personnel sont nombreux.

11.5 Processus d'arrivée et de départ (Onboarding / Offboarding)

Le processus d'arrivée d'un nouveau collaborateur (onboarding) doit intégrer, dès le premier jour, la création des accès strictement nécessaires à ses fonctions et une sensibilisation initiale aux règles de sécurité de l'organisation, plutôt que de différer ces étapes au profit des seules formalités administratives et opérationnelles. Le processus de départ (offboarding) revêt une importance au moins équivalente, et souvent sous-estimée : il doit garantir la révocation immédiate de l'ensemble des accès du collaborateur sortant, la restitution des équipements et supports contenant des informations de l'organisation, et le cas échéant la réaffectation ou la clôture de ses comptes de messagerie et applicatifs.

11.6 Gestion des comptes des anciens collaborateurs

La persistance de comptes actifs appartenant à d'anciens collaborateurs constitue l'une des vulnérabilités les plus fréquemment constatées lors des audits de sécurité, et l'une des plus simples à exploiter par un attaquant, en particulier lorsque le départ s'est déroulé dans un contexte conflictuel. Le RSSI doit s'assurer de l'existence d'un contrôle croisé régulier entre le registre des ressources humaines et l'annuaire des comptes actifs du système d'information, permettant de détecter systématiquement tout écart entre les collaborateurs effectivement en poste et les comptes demeurant actifs.

11.7 Menaces internes

Les menaces internes, qu'elles résultent d'une malveillance délibérée (collaborateur mécontent, complicité avec un acteur externe) ou d'une simple négligence (erreur de manipulation, non-respect des règles de sécurité), constituent une catégorie de risque spécifique nécessitant une approche dédiée, distincte de celle des menaces externes. Cette approche combine des mesures techniques — surveillance des comportements anormaux, contrôle renforcé sur les accès aux données sensibles, limitation du principe du moindre privilège déjà évoqué — et des mesures organisationnelles, telles qu'une politique claire de sanctions disciplinaires en cas de manquement avéré et un climat social suffisamment sain pour limiter les motivations à la malveillance délibérée.

11.8 Gestion des compétences cyber

La pénurie mondiale de compétences en cybersécurité, particulièrement aiguë dans de nombreux pays africains où les filières de formation spécialisées restent en développement, constitue une contrainte structurelle que le RSSI doit anticiper plutôt que subir. Cette gestion des compétences suppose une cartographie précise des compétences requises au sein de l'équipe sécurité, une identification des écarts par rapport aux besoins de l'organisation, et une stratégie combinant recrutement, formation interne, mobilité depuis d'autres fonctions techniques, et recours ciblé à des prestataires externes pour les compétences les plus rares ou les besoins ponctuels.

11.9 Plan de développement des compétences

Au-delà de la gestion à court terme des besoins en compétences, le RSSI doit construire, en lien avec la direction des ressources humaines, un plan de développement des compétences pluriannuel pour son équipe, intégrant formation continue, certifications professionnelles et participation à des communautés professionnelles ou événements sectoriels permettant de maintenir une veille active sur l'évolution rapide des menaces et des technologies. Ce plan constitue également un levier de fidélisation important dans un marché où la demande de professionnels qualifiés en cybersécurité excède largement l'offre disponible.

11.10 Construire une équipe cybersécurité

La construction d'une équipe cybersécurité doit être pensée en fonction de la taille et de la maturité de l'organisation, plutôt que calquée mécaniquement sur le modèle d'une grande organisation internationale. Dans les organisations de taille modeste, une équipe réduite, voire une personne unique appuyée par des prestataires externes pour les fonctions les plus spécialisées (SOC, tests d'intrusion, investigation numérique), peut constituer un dispositif adapté et efficace. Dans les organisations de plus grande taille, une équipe structurée par domaines de compétence — gouvernance et risques, architecture et technique, opérations et détection, sensibilisation — permet une couverture plus complète des responsabilités décrites dans ce guide.

Dans tous les cas, le RSSI doit veiller à un équilibre entre compétences techniques et compétences de gouvernance au sein de son équipe, un écueil fréquent consistant à ne recruter que des profils techniques, au détriment de la capacité de l'équipe à produire un reporting de qualité, à dialoguer avec les autres directions et à porter une vision stratégique du risque numérique.

XII

PARTIE XII · CHAPITRE 12

Le RSSI et les fournisseurs

Maîtriser le risque lié aux tiers

CE QUE LA DIRECTION DOIT SAVOIR

1. Un nombre croissant d'incidents majeurs trouvent leur origine chez un prestataire ou un fournisseur plutôt que dans le système d'information de l'organisation elle-même.
2. La responsabilité juridique et réputationnelle d'un incident survenu chez un prestataire reste, pour l'essentiel, portée par l'organisation cliente vis-à-vis de ses propres clients et régulateurs.
3. Les exigences de sécurité doivent être intégrées dès la sélection du fournisseur et formalisées contractuellement, et non ajoutées après coup lorsque la relation est déjà engagée.

12.1 Pourquoi les fournisseurs constituent un risque cyber

L'externalisation croissante de fonctions et de systèmes auprès de prestataires — hébergement cloud, développement applicatif, gestion de la paie, support informatique, services de sécurité eux-mêmes — étend le périmètre de risque de l'organisation bien au-delà de ses propres systèmes. Un fournisseur disposant d'un accès aux systèmes ou aux données de l'organisation constitue un point d'entrée potentiel pour un attaquant, comme l'illustrent les attaques par la chaîne d'approvisionnement évoquées à la section 1.1 de ce guide, où la compromission d'un fournisseur permet d'atteindre indirectement l'ensemble de ses clients.

Ce constat impose au RSSI d'étendre sa vision du risque au-delà du seul périmètre interne de l'organisation, et de considérer l'écosystème de fournisseurs et de partenaires comme une composante à part entière de la surface de risque à maîtriser, avec une priorité accordée aux fournisseurs disposant des accès les plus étendus ou traitant les données les plus sensibles.

12.2 Due diligence sécurité

La due diligence sécurité consiste à évaluer, avant la contractualisation, le niveau de maturité en matière de sécurité d'un fournisseur pressenti, au moyen de questionnaires structurés, de demandes de certification (ISO 27001 notamment) ou, pour les prestataires les plus critiques, d'audits sur site. Cette évaluation doit être proportionnée à la criticité de la prestation envisagée : un prestataire disposant d'un accès étendu aux données sensibles de l'organisation justifie un niveau d'exigence nettement supérieur à celui appliqué à un fournisseur de biens ou de services sans lien avec le système d'information.

12.3 Exigences de sécurité dans les contrats

Les exigences de sécurité identifiées lors de la due diligence doivent être traduites en clauses contractuelles explicites et opposables, couvrant notamment les mesures de sécurité minimales attendues, les obligations de notification en cas d'incident affectant les données ou systèmes de l'organisation cliente, le droit d'audit de l'organisation cliente sur le prestataire, et les responsabilités respectives en cas de préjudice résultant d'un manquement à ces exigences. L'implication du RSSI dans la négociation de ces clauses, en lien avec la direction juridique et les équipes achats, est essentielle : des exigences de sécurité définies après la signature du contrat perdent l'essentiel de leur force contraignante.

12.4 SLA et exigences de cybersécurité

Les accords de niveau de service (Service Level Agreement, SLA) conclus avec les prestataires doivent intégrer des engagements spécifiques à la cybersécurité, au-delà des seuls engagements de disponibilité ou de performance habituellement négociés : délais de notification en cas d'incident de sécurité, délais de correction des vulnérabilités identifiées sur les systèmes fournis,

engagements de restauration en cas de sinistre. Ces engagements doivent être assortis de mécanismes de vérification effective — rapports périodiques, indicateurs partagés — plutôt que de rester des déclarations d'intention non mesurées dans la durée.

12.5 Audit des prestataires

Pour les prestataires les plus critiques, un droit d'audit contractuellement établi doit pouvoir être exercé périodiquement, permettant à l'organisation cliente, directement ou via un tiers mandaté, de vérifier la réalité des mesures de sécurité annoncées par le prestataire. Cette pratique, encore peu répandue dans de nombreuses organisations en raison de la complexité perçue de sa mise en œuvre, peut être facilitée par le recours à des certifications reconnues (ISO 27001, rapports d'audit de type SOC 2) qui, sans se substituer totalement à un audit direct, apportent une assurance raisonnable sur le niveau de maturité du prestataire sans nécessiter la mobilisation de ressources d'audit dédiées pour chaque fournisseur.

12.6 Gestion des accès des prestataires

Les accès accordés aux prestataires aux systèmes de l'organisation doivent être encadrés avec la même rigueur que ceux accordés aux collaborateurs internes, selon le principe du moindre privilège déjà évoqué : accès limités au strict périmètre nécessaire à la prestation, limités dans le temps à la durée de la mission, et révoqués systématiquement à l'issue du contrat ou de l'intervention. Une attention particulière doit être portée aux accès à distance des prestataires de maintenance et de support technique, qui constituent, en l'absence d'un encadrement rigoureux, un vecteur d'intrusion régulièrement exploité par des attaquants.

12.7 Cloud et externalisation

Le recours croissant à des services cloud, déjà évoqué à la section 7.7 sous son angle technique, soulève des enjeux contractuels spécifiques : localisation des données, conditions de leur transfert transfrontalier au regard des réglementations de protection des données applicables, garanties offertes par le fournisseur en matière de sécurité et de disponibilité, et réversibilité du service en cas de changement de prestataire. Le RSSI doit être systématiquement associé à l'évaluation de ces enjeux avant tout engagement significatif vers un service cloud, ce choix engageant l'organisation dans la durée et étant souvent coûteux à réviser une fois la migration réalisée.

12.8 Fin de contrat et restitution des données

La fin d'une relation contractuelle avec un fournisseur, qu'elle résulte d'un terme normal ou d'une rupture anticipée, doit faire l'objet d'une procédure formalisée garantissant la restitution ou la destruction sécurisée des données de l'organisation détenues par le prestataire, la révocation de l'ensemble des accès qui lui avaient été accordés, et la vérification que ces engagements ont été effectivement respectés. Cette étape, souvent négligée une fois la relation commerciale terminée et l'attention de l'organisation déjà tournée vers d'autres priorités, constitue pourtant un moment de risque significatif, en particulier lorsque la rupture du contrat s'est déroulée dans un climat conflictuel.

XIII

PARTIE XIII · CHAPITRE 13

Pilotage et reporting du RSSI

Comment rendre compte à la Direction

CE QUE LA DIRECTION DOIT SAVOIR

1. Un reporting sécurité efficace se juge à sa capacité à éclairer une décision, non à sa complétude technique : mieux vaut trois indicateurs compris et actionnables que trente ignorés.
2. Le rythme et le format du reporting doivent être adaptés à chaque destinataire — un tableau de bord opérationnel n'a pas sa place devant un Conseil d'administration.
3. Traduire une vulnérabilité technique en risque business est la compétence la plus déterminante pour qu'un RSSI obtienne l'attention et les arbitrages de sa Direction.

13.1 Pourquoi le reporting est stratégique

Le reporting constitue le principal — parfois l'unique — canal par lequel la Direction générale et les organes de gouvernance prennent connaissance de la réalité du risque numérique de l'organisation. Un dispositif de sécurité par ailleurs solide, mais dont le pilotage reste invisible faute d'un reporting régulier et compréhensible, prive la Direction des éléments nécessaires pour arbitrer en connaissance de cause, et prive symétriquement le RSSI de la légitimité et du soutien que seule cette visibilité peut lui apporter. Le reporting n'est donc pas une formalité administrative annexe à l'action du RSSI : il en est un levier stratégique à part entière.

Un reporting de qualité poursuit simultanément plusieurs objectifs : informer la Direction de l'état réel de l'exposition au risque, démontrer la valeur du travail accompli par la fonction sécurité, alerter suffisamment tôt sur les risques nécessitant un arbitrage, et documenter, à des fins de traçabilité et d'audit, les décisions prises en matière de risque numérique. Un reporting qui ne remplirait que la première de ces fonctions, sans jamais déboucher sur une décision ou une allocation de ressources, finit par perdre de sa valeur perçue aux yeux de ses destinataires.

13.2 Tableau de bord du RSSI

Le tableau de bord du RSSI rassemble, sous une forme synthétique et régulièrement actualisée, les indicateurs clés permettant de suivre la performance du dispositif de sécurité et l'évolution du niveau de risque de l'organisation. Un modèle complet de tableau de bord, structuré autour de neuf domaines (gouvernance, risques, protection technique, incidents, continuité, conformité, sensibilisation, tiers, ressources) est proposé en annexe de ce guide, en Partie XX.

La construction de ce tableau de bord doit résister à la tentation de l'exhaustivité : un tableau de bord surchargé d'indicateurs, aussi rigoureusement documentés soient-ils, perd sa fonction première de pilotage et d'aide à la décision. Le RSSI a intérêt à distinguer un socle réduit d'indicateurs stratégiques, destinés à un reporting régulier auprès de la Direction, d'un ensemble plus large d'indicateurs opérationnels, utiles à son propre pilotage interne mais qui n'ont pas vocation à être systématiquement présentés au-delà de son équipe.

13.3 KPI et KRI

Il est utile de distinguer deux catégories d'indicateurs, dont la confusion est fréquente mais nuit à la clarté du reporting. Les indicateurs de performance (Key Performance Indicators, KPI) mesurent l'efficacité du dispositif de sécurité et de l'action du RSSI — taux de correction des vulnérabilités dans les délais, taux de collaborateurs sensibilisés, délai moyen de réponse aux incidents. Les indicateurs de risque (Key Risk Indicators, KRI), quant à eux, mesurent le niveau d'exposition au risque de l'organisation, indépendamment de la performance du dispositif qui le traite — nombre de vulnérabilités critiques ouvertes, nombre de comptes à privilèges sans authentification forte, ancienneté du registre des risques.

Cette distinction importe car elle éclaire différemment la lecture d'un même chiffre : un nombre élevé d'incidents détectés peut, selon le contexte, traduire un KRI défavorable (l'organisation est fortement exposée) ou, à l'inverse, un KPI favorable (le dispositif de détection fonctionne efficacement), comme développé à la section 4.7 de ce guide. Un tableau de bord équilibré doit combiner ces deux familles d'indicateurs, et le RSSI doit être en mesure d'expliquer à sa Direction laquelle de ces deux lectures s'applique à chaque indicateur présenté.

Les indicateurs gagnent à être classés en quatre familles — KPI opérationnels, KRI, indicateurs de conformité et indicateurs destinés au Comité de direction et au Conseil (voir le tableau de la section 4.5) —, chaque famille ayant ses destinataires, sa fréquence et son niveau de détail. Un même chiffre peut relever de plusieurs familles ; l'essentiel est de savoir, pour chaque présentation, à quelle décision il répond.

13.4 Indicateurs techniques versus indicateurs décisionnels

Un écueil fréquent dans le reporting sécurité consiste à présenter à la Direction des indicateurs formulés dans un langage exclusivement technique — nombre de signatures antivirus mises à jour, nombre de règles de pare-feu revues — qui, bien que légitimes pour un pilotage opérationnel interne, n'apportent que peu d'éclairage à un décideur non spécialiste et ne débouchent sur aucune décision concrète de sa part. Le RSSI doit systématiquement traduire ces indicateurs techniques en indicateurs décisionnels, formulés en termes de risque, de conformité ou d'impact potentiel sur l'activité, seuls réellement porteurs de sens pour une Direction générale.

13.5 Reporting mensuel

Un reporting mensuel, généralement interne à la fonction sécurité et à la DSI, permet un suivi rapproché de l'avancement des plans d'action, du traitement des vulnérabilités et des incidents survenus sur la période. Ce reporting, plus détaillé et plus technique que les reportings destinés à la Direction générale, constitue l'outil de pilotage opérationnel du RSSI et de son équipe, et sert de matière première à l'élaboration des reportings de niveau supérieur, trimestriel et annuel, développés aux sections suivantes.

13.6 Reporting trimestriel à la Direction générale

Le reporting trimestriel à la Direction générale, déjà évoqué à la section 3.6 de ce guide, doit adopter un format synthétique — quelques pages au maximum — structuré autour de l'évolution des principaux indicateurs de risque, des incidents significatifs survenus et de leur traitement, de l'avancement des plans d'action prioritaires, et des décisions ou arbitrages nécessitant l'attention de la Direction. Un modèle de rapport RSSI destiné au comité de direction est proposé en Partie XX de ce guide.

La préparation de ce reporting gagne à être pensée non comme un exercice de reddition de comptes, mais comme un support de dialogue : le RSSI a intérêt à réserver du temps, lors de sa présentation, à l'échange avec les membres du comité de direction sur les arbitrages qu'il attend d'eux, plutôt que de consacrer l'intégralité du temps disponible à une présentation descendante d'indicateurs.

13.7 Reporting au Conseil d'administration

Le reporting au Conseil d'administration ou au Comité d'audit, déjà évoqué à la section 3.7, doit adopter un niveau de synthèse supérieur à celui du reporting trimestriel à la Direction générale : il ne s'agit plus de détailler l'avancement opérationnel du plan de sécurité, mais de donner aux administrateurs une vision consolidée du niveau de risque numérique de l'organisation, de sa trajectoire d'évolution, et des décisions stratégiques ou budgétaires qui pourraient nécessiter leur validation. Un modèle de présentation au Conseil d'administration est également proposé en Partie XX de ce guide.

Ce reporting doit être préparé en lien étroit avec la Direction générale, qui reste l'interlocuteur hiérarchique naturel du RSSI, cette dernière validant généralement le contenu présenté au Conseil avant sa diffusion, sans que cela ne remette en cause l'indépendance de jugement du RSSI dans l'élaboration de son analyse.

13.8 Présenter un risque cyber à un dirigeant non technique

La capacité à présenter un risque cyber de manière compréhensible et actionnable pour un dirigeant non technique constitue l'une des compétences les plus déterminantes, quoique les moins enseignées, du métier de RSSI. Cette capacité suppose d'éviter le jargon technique au profit d'un vocabulaire de risque d'entreprise, de hiérarchiser l'information en commençant par l'essentiel (l'impact potentiel et la décision attendue) plutôt que par le détail technique, et de systématiquement relier chaque risque présenté à une conséquence concrète et mesurable pour l'organisation — perte financière, interruption de service, sanction réglementaire, atteinte à la réputation.

13.9 Transformer une vulnérabilité technique en risque business

La transformation d'une vulnérabilité technique en risque business constitue l'exercice de traduction fondamental que doit maîtriser tout RSSI souhaitant obtenir l'attention et les arbitrages de sa Direction. Cet exercice suit un enchaînement logique reproductible : la vulnérabilité technique identifiée (par exemple, un serveur non corrigé d'une faille connue) conduit à un risque de sécurité (la compromission possible de ce serveur), qui produit un impact opérationnel (l'interruption du service qu'il héberge), lequel se traduit en impact business mesurable (perte de revenus, indisponibilité d'un service public, atteinte à l'image de l'organisation), débouchant enfin sur une décision attendue de la Direction (le financement du plan de remédiation correspondant).

Cette chaîne de traduction, qui peut sembler évidente une fois formulée, est pourtant rarement appliquée de manière systématique dans les organisations, où le reporting sécurité s'arrête trop souvent au premier maillon — la description technique de la vulnérabilité — sans jamais atteindre le dernier, qui est pourtant celui qui déclenche effectivement une décision de la Direction. Le RSSI qui maîtrise cet exercice de traduction transforme sa fonction de simple rapporteur technique en véritable conseiller de la Direction sur les enjeux de risque numérique.

XIV

PARTIE XIV · CHAPITRE 14

Budget et investissements cybersécurité

Construire et défendre le budget cybersécurité

CE QUE LA DIRECTION DOIT SAVOIR

1. Un budget de sécurité construit à partir des risques identifiés est plus robuste et plus facile à défendre qu'un budget fixé arbitrairement en pourcentage du budget informatique.

2. Le coût de l'inaction — pertes potentielles en cas d'incident non prévenu — doit être mis en balance avec le coût des mesures de protection lors de tout arbitrage budgétaire.

3. Un investissement en cybersécurité ne se limite pas à l'achat d'outils : les ressources humaines et les processus représentent souvent une part au moins équivalente, sinon supérieure, de l'effort réellement nécessaire.

14.1 Construire un budget fondé sur les risques

La construction d'un budget de cybersécurité gagne à partir non d'une reconduction historique du budget de l'année précédente, ni d'un pourcentage arbitraire du budget informatique global, mais d'une analyse structurée des risques prioritaires de l'organisation, telle que développée dans la Partie VI de ce guide. Cette approche, dite budgétisation fondée sur le risque, consiste à identifier les scénarios de risque les plus critiques, à évaluer le coût des mesures permettant de les réduire à un niveau acceptable, et à prioriser les investissements en fonction du rapport entre la réduction de risque obtenue et le coût de sa mise en œuvre.

Cette méthode présente un avantage décisif sur le plan de la gouvernance : elle permet au RSSI de justifier chaque ligne budgétaire par un risque identifié et documenté, plutôt que par une référence générique aux bonnes pratiques du secteur, ce qui facilite considérablement l'arbitrage et l'approbation par la Direction générale, particulièrement dans des contextes de ressources contraintes où chaque investissement doit être précisément justifié.

14.2 CAPEX et OPEX

La distinction entre dépenses d'investissement (CAPEX, Capital Expenditure) et dépenses d'exploitation (OPEX, Operating Expenditure) structure la présentation budgétaire attendue par la plupart des directions financières, et le RSSI doit maîtriser cette distinction pour construire un budget lisible et conforme aux pratiques de gestion de son organisation. Les acquisitions d'équipements et de licences pérennes relèvent généralement du CAPEX, tandis que les abonnements à des services (SOC managé, solutions en mode SaaS, prestations récurrentes) et les charges de personnel relèvent de l'OPEX — cette dernière catégorie tendant à croître structurellement avec la généralisation des modèles de services par abonnement dans le secteur de la cybersécurité.

14.3 Priorisation des investissements

Face à des ressources nécessairement limitées, le RSSI doit établir une priorisation explicite entre les différents investissements envisageables, fondée sur des critères objectivés : niveau de criticité du risque adressé, rapport entre le coût de la mesure et la réduction de risque obtenue, dépendances éventuelles entre projets (certains investissements devant précéder d'autres pour être pleinement efficaces), et contraintes de calendrier liées à des obligations réglementaires ou contractuelles. Cette priorisation doit être documentée et présentée à la Direction, qui doit rester l'arbitre final des choix engageant des montants significatifs, le rôle du RSSI étant d'éclairer cette décision par une analyse rigoureuse plutôt que de la prendre seul.

14.4 Construire un business case cybersécurité

Un business case cybersécurité efficace présente, pour chaque investissement significatif proposé, le risque qu'il permet de traiter, formulé en langage de risque d'entreprise conformément aux principes développés à la section 13.9, le coût complet de sa mise en œuvre (acquisition, déploiement, exploitation récurrente), les bénéfices attendus en termes de réduction de risque, et les conséquences d'un renoncement à cet investissement. Cette structuration, proche de celle attendue pour tout projet d'investissement au sein de l'organisation, permet au RSSI de dialoguer avec la Direction financière et la Direction générale dans un cadre familier et rigoureux, plutôt que de solliciter une confiance a priori sur la seule base de son expertise technique.

14.5 Arbitrer entre outils, services et ressources humaines

Un arbitrage récurrent dans la construction du budget de sécurité oppose l'acquisition d'outils technologiques, le recours à des services externalisés, et l'investissement en ressources humaines internes. Aucune de ces trois options n'est intrinsèquement supérieure aux autres : elle dépend du contexte spécifique de l'organisation, de sa capacité à recruter et retenir des compétences internes rares, dans un marché où la pénurie de compétences cyber, développée à la section 11.8, rend cet enjeu particulièrement sensible dans de nombreux pays africains, et de sa capacité à exploiter efficacement des outils technologiques, dont l'acquisition sans les compétences nécessaires à leur exploitation optimale représente un écueil fréquent et coûteux.

Un équilibre réfléchi entre ces trois leviers, réévalué périodiquement à mesure que la maturité de l'organisation évolue, constitue généralement une approche plus robuste qu'une stratégie reposant exclusivement sur l'un d'entre eux — par exemple, l'acquisition d'outils technologiques sophistiqués sans les ressources humaines nécessaires pour les exploiter pleinement, un écueil régulièrement observé et qui conduit à un rendement décevant des investissements réalisés.

14.6 Mesurer le retour sur investissement

La mesure du retour sur investissement (ROI) en matière de cybersécurité présente une difficulté méthodologique propre à ce domaine : contrairement à un investissement générateur de revenus additionnels, un investissement de sécurité vise essentiellement à prévenir des pertes potentielles, dont l'occurrence, par nature incertaine, rend le calcul de retour sur investissement moins direct que dans d'autres domaines de gestion. Le RSSI peut néanmoins s'appuyer sur des approches éprouvées, telles que l'estimation de la perte annuelle attendue (Annual Loss Expectancy), qui combine la probabilité d'occurrence d'un scénario de risque et l'impact financier estimé de sa survenue, permettant de comparer le coût d'une mesure de protection à la réduction de perte attendue qu'elle procure.

14.7 Le coût de l'inaction

Au-delà du seul calcul de retour sur investissement, le RSSI dispose d'un argument souvent plus parlant pour la Direction : le coût de l'inaction, c'est-à-dire les conséquences concrètes et documentées d'un renoncement à l'investissement proposé, en cas de matérialisation du risque qu'il visait à traiter. Ce coût inclut les pertes d'exploitation directes liées à une interruption de service, les coûts de remédiation et d'investigation post-incident, les éventuelles sanctions réglementaires, les coûts juridiques liés à des actions en responsabilité, et les conséquences réputationnelles et commerciales, souvent les plus difficiles à chiffrer mais parfois les plus durables.

La mobilisation d'exemples documentés d'incidents survenus dans des organisations comparables, en termes de secteur ou de taille, s'avère souvent plus convaincante auprès d'une Direction générale qu'une analyse théorique du risque, en donnant une réalité tangible à des conséquences qui, tant qu'elles restent hypothétiques, peinent à justifier un investissement perçu comme une dépense discrétionnaire plutôt que comme une nécessité.

XV

PARTIE XV · CHAPITRE 15

Le RSSI dans les organisations africaines

Enjeux et réalités du contexte africain

CE QUE LA DIRECTION DOIT SAVOIR

1. Les contraintes propres au contexte africain — pénurie de compétences, budgets limités, infrastructures parfois instables — ne dispensent pas de structurer la fonction RSSI : elles imposent au contraire des choix méthodologiques adaptés plutôt qu'un renoncement à la rigueur.

2. Le cadre réglementaire africain de la cybersécurité et de la protection des données progresse rapidement, porté notamment par la Convention de Malabo et les initiatives régionales.

3. Une PME peut structurer une fonction sécurité proportionnée à ses moyens sans nécessairement recruter un RSSI à temps plein.

15.1 Maturité cyber des organisations

La maturité en matière de cybersécurité des organisations africaines est hétérogène, variant fortement selon les secteurs, les tailles et les pays. Certains secteurs — services financiers, télécommunications, grandes entreprises multinationales implantées sur le continent — affichent des niveaux de maturité comparables aux standards internationaux, portés notamment par des exigences réglementaires sectorielles strictes et une exposition directe à des menaces sophistiquées. D'autres secteurs, en particulier les administrations publiques de taille intermédiaire et les petites et moyennes entreprises, restent à un stade plus précoce de structuration de leur dispositif de sécurité, ce qui justifie précisément l'existence de ce guide et l'attention particulière portée, dans cette partie, aux enjeux propres à ces contextes.

15.2 Pénurie de compétences

La pénurie de compétences spécialisées en cybersécurité, phénomène mondial déjà évoqué à la section 11.8, revêt une acuité particulière dans de nombreux pays africains, où les filières de formation spécialisées, bien qu'en développement rapide, restent encore en construction face à une demande croissante. Cette pénurie se traduit par une compétition accrue pour attirer et retenir les profils qualifiés, par des salaires en forte progression sur ce segment de compétences, et par un recours fréquent à des prestataires internationaux pour les expertises les plus rares, avec les enjeux de coût et de souveraineté que cela soulève.

Face à cette contrainte structurelle, les organisations les plus avisées investissent dans la formation de talents locaux plutôt que de s'en remettre exclusivement au marché du recrutement externe, en s'appuyant sur les filières universitaires émergentes, les programmes de certification internationaux accessibles à distance, et des partenariats avec des écoles et centres de formation spécialisés qui se développent progressivement sur le continent.

15.3 Contraintes budgétaires

Les contraintes budgétaires, particulièrement marquées dans les organisations de taille intermédiaire et dans le secteur public, imposent au RSSI une discipline de priorisation encore plus rigoureuse que celle décrite dans la Partie XIV de ce guide : chaque franc investi doit être justifié par une réduction de risque clairement identifiée, et les solutions retenues doivent privilégier un rapport coût-efficacité optimal plutôt qu'une sophistication technologique qui, dans de nombreux cas, excède les besoins réels et la capacité opérationnelle de l'organisation à l'exploiter pleinement.

Dans ce contexte, des mesures de sécurité à faible coût mais à fort impact — authentification forte, gestion rigoureuse des correctifs, sensibilisation des utilisateurs, sauvegardes testées — méritent une priorité particulière, offrant souvent un rapport coût-bénéfice nettement supérieur à des investissements technologiques plus onéreux mais moins immédiatement efficaces sur les scénarios de risque les plus fréquents.

15.4 Dépendance aux prestataires et technologies étrangères

De nombreuses organisations africaines demeurent fortement dépendantes de technologies, d'éditeurs et de prestataires étrangers pour la sécurisation de leurs systèmes d'information, une dépendance qui soulève des enjeux de coût (facturation en devises étrangères, exposée aux fluctuations de change), de continuité (dépendance à des chaînes d'approvisionnement et de support international) et, pour certains secteurs sensibles, de souveraineté des données. Le RSSI doit intégrer cette dimension dans ses choix d'architecture et de sourcing, en évaluant notamment les alternatives régionales émergentes lorsqu'elles offrent un niveau de maturité suffisant, sans pour autant sacrifier la qualité de la protection au nom du seul critère de la souveraineté.

En clair : la souveraineté est un critère parmi d'autres dans l'arbitrage — jamais le critère qui l'emporte automatiquement sur la robustesse de la protection. Un hébergeur local peu mature qui expose l'organisation à un risque plus élevé n'est pas un meilleur choix qu'un hébergeur étranger solide, même si le second pose des questions de souveraineté.

15.5 Infrastructure et connectivité

La fiabilité variable des infrastructures électriques et de connectivité dans certaines zones géographiques constitue une contrainte opérationnelle directe pour le RSSI, qui doit intégrer ces aléas dans sa stratégie de résilience — dispositifs d'alimentation de secours pour les équipements critiques, mécanismes de reprise adaptés à des interruptions de connectivité plus fréquentes que dans d'autres contextes, et architecture technique tolérante aux coupures plutôt que conçue sur l'hypothèse d'une disponibilité continue des infrastructures. Ces contraintes, loin de constituer une excuse à un moindre niveau d'exigence, imposent au contraire une conception plus rigoureuse de la résilience, développée dans la Partie IX de ce guide.

15.6 Gouvernance et culture organisationnelle

La culture managériale de nombreuses organisations, marquée par des structures hiérarchiques fortement verticales, peut compliquer l'exercice du droit d'alerte et de l'indépendance de jugement attendus du RSSI, particulièrement lorsque ses recommandations impliquent de contredire une décision déjà prise par un niveau hiérarchique supérieur. Cette réalité culturelle renforce l'importance des mécanismes de gouvernance formalisés décrits dans la Partie III de ce guide — charte de fonction, lettre de mission, accès direct à la Direction générale — qui offrent au RSSI un cadre institutionnel sur lequel s'appuyer, indépendamment des dynamiques interpersonnelles ou hiérarchiques informelles.

15.7 Sensibilisation des utilisateurs

Les campagnes de sensibilisation à la sécurité, développées à la section 11.1, gagnent à être adaptées aux réalités locales des organisations africaines :

diversité linguistique nécessitant parfois une déclinaison en plusieurs langues, usages numériques spécifiques (forte pénétration du mobile, usage intensif de plateformes de messagerie instantanée dans les échanges professionnels), et exemples de menaces ancrés dans le contexte réel des utilisateurs — fraude aux services financiers mobiles, hameçonnage exploitant l'actualité locale — plutôt que des supports génériques traduits sans adaptation, dont l'efficacité pédagogique s'avère généralement limitée.

5.8 Cadres réglementaires africains

Le cadre réglementaire africain relatif à la cybersécurité et à la protection des données personnelles connaît un développement rapide, porté notamment par la Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles (Convention de Malabo), adoptée en 2014 et progressivement ratifiée par un nombre croissant d'États membres, ainsi que par les législations nationales, de plus en plus nombreuses, qui s'en inspirent ou établissent leurs propres cadres. Ce dynamisme réglementaire, déjà évoqué dans la Partie X de ce guide, impose au RSSI une veille active, le cadre applicable pouvant évoluer significativement en quelques années dans un même pays.

Le cas du Bénin. Le Bénin illustre cette dynamique : doté d'un Code du numérique (loi n° 2017-20 du 20 avril 2018, modifiée en 2021) qui couvre notamment la protection des données personnelles, la sécurité des systèmes d'information et la cybercriminalité, il a ratifié la Convention de Malabo en novembre 2024 et adhéré en 2024 à la Convention de Budapest. Voir l'encadré « Le contexte béninois » de l'Avant-propos, la section 8.14 et l'Annexe 3.

15.9 Coopération régionale

La coopération régionale en matière de cybersécurité se structure progressivement, portée par des initiatives des communautés économiques régionales, des équipes de réponse aux incidents (CERT/CSIRT) nationales et régionales en développement, et des partenariats de partage d'information sur les menaces entre organisations d'un même secteur ou d'une même région. Le RSSI a intérêt à s'informer de l'existence de ces initiatives dans son pays et sa région, et à y participer lorsque cela est possible, ces échanges constituant une source précieuse de veille sur les menaces spécifiquement observées dans le contexte régional, complémentaire des sources internationales généralistes.

15.10 Enjeux spécifiques aux administrations publiques

Les administrations publiques, engagées dans des démarches accélérées de dématérialisation de leurs services aux citoyens, font face à des enjeux de cybersécurité spécifiques : protection de données personnelles sensibles à grande échelle, criticité des services essentiels rendus aux populations, contraintes budgétaires souvent plus strictes que dans le secteur privé, et gouvernance parfois complexe entre différentes entités publiques aux systèmes d'information

interconnectés. La structuration d'une fonction RSSI dans ce contexte gagne à s'appuyer sur des mutualisations possibles entre administrations, ainsi que sur le portage politique au plus haut niveau, indispensable pour surmonter les contraintes budgétaires et organisationnelles propres au secteur public.

15.11 Enjeux spécifiques aux banques et institutions financières

Le secteur financier, généralement soumis à des exigences réglementaires strictes émanant des banques centrales et autorités de régulation, affiche souvent le niveau de maturité cyber le plus élevé du continent, porté par une exposition directe et immédiate à la fraude financière et par des obligations de reporting réglementaire rigoureuses. Le RSSI y opère dans un cadre déjà largement structuré, mais doit faire face à des enjeux spécifiques liés à l'essor des services financiers mobiles et numériques, qui élargissent considérablement la surface d'exposition au risque et exigent une vigilance particulière sur la fraude et la protection des transactions.

15.12 Enjeux des opérateurs de télécommunications

Les opérateurs de télécommunications, en tant qu'infrastructures critiques et acteurs centraux de l'écosystème numérique, sont confrontés à des enjeux de cybersécurité d'une ampleur particulière : volume massif de données personnelles traitées, criticité absolue de la disponibilité de leurs services pour l'ensemble de l'économie numérique, et exposition à des attaques sophistiquées visant à perturber des infrastructures nationales essentielles. Le RSSI dans ce secteur doit généralement disposer de moyens et d'une équipe à la mesure de ces enjeux, avec un dispositif de détection et de réponse aux incidents opérant en continu, au regard de la criticité des services rendus.

15.13 Enjeux des infrastructures critiques

Au-delà des télécommunications, d'autres infrastructures critiques — énergie, transport, eau, systèmes de santé, infrastructure de confiance — connaissent une numérisation croissante de leurs systèmes de contrôle industriel, historiquement isolés mais de plus en plus interconnectés aux systèmes d'information de gestion, ce qui élargit leur surface d'exposition à des menaces auparavant circonscrites aux seuls systèmes informatiques classiques. La sécurisation de ces environnements industriels (technologies opérationnelles, OT) requiert une expertise spécifique, distincte de celle de la sécurité informatique traditionnelle, ces systèmes obéissant à des contraintes de disponibilité et de sécurité physique différentes de celles des systèmes d'information de gestion.

15.14 PME : comment avoir une fonction sécurité avec des moyens limités ?

Les petites et moyennes entreprises, qui ne disposent généralement pas des moyens nécessaires pour recruter un RSSI à temps plein, peuvent néanmoins structurer une fonction sécurité proportionnée à leurs enjeux, selon plusieurs modalités. Un RSSI à temps partagé, mutualisé entre plusieurs organisations ou exercé par un prestataire spécialisé quelques jours par mois, permet d'apporter un pilotage de gouvernance sans le coût d'un poste à temps plein. Un collaborateur existant, désigné comme référent sécurité et formé aux fondamentaux de la fonction, peut également porter cette responsabilité à temps partiel, à condition de bénéficier d'un mandat clair et d'un accès à la Direction, conformément aux principes développés dans la Partie III de ce guide.

Quelle que soit la modalité retenue, une PME a intérêt à concentrer ses efforts sur un socle minimal de mesures à fort impact — sauvegardes régulières et testées, authentification forte sur les comptes sensibles, sensibilisation de base des collaborateurs à l'hameçonnage, mise à jour régulière des systèmes — plutôt que de chercher à reproduire, avec des moyens disproportionnés, l'ensemble du dispositif décrit dans ce guide pour des organisations de plus grande taille. Un référentiel simplifié tel que les CIS Controls, évoqué à la section 10.7, offre un point de départ pragmatique et gradué, adapté à cette réalité.

XVI

PARTIE XVI · CHAPITRE 16

Le RSSI à l'ère de l'intelligence artificielle

Nouveaux défis pour le RSSI

CE QUE LA DIRECTION DOIT SAVOIR

1. L'intelligence artificielle transforme simultanément les capacités des attaquants et celles des défenseurs, sans que l'un de ces effets ne compense mécaniquement l'autre.

2. L'usage non encadré d'outils d'IA générative par les collaborateurs (« Shadow AI ») constitue un risque de fuite de données déjà avéré dans de nombreuses organisations, souvent sans que la Direction en ait pleinement conscience.

3. Le RSSI doit désormais intégrer la gouvernance de l'IA à son périmètre de responsabilité, sans nécessairement en devenir l'unique propriétaire au sein de l'organisation.

16.1 L'IA comme outil d'attaque

L'intelligence artificielle, en particulier générative, est de plus en plus mobilisée par les acteurs malveillants pour industrialiser et sophistiquer leurs attaques : génération de courriels d'hameçonnage grammaticalement irréprochables et personnalisés à grande échelle, création de code malveillant assistée par des modèles de langage, automatisation de la reconnaissance de cibles et de la recherche de vulnérabilités, et production de contenus frauduleux crédibles à des fins d'ingénierie sociale. Cette évolution abaisse significativement la barrière technique nécessaire pour mener des attaques auparavant réservées à des acteurs sophistiqués, élargissant le nombre d'attaquants potentiellement capables de cibler une organisation donnée.

16.2 L'IA comme outil de défense

Symétriquement, l'intelligence artificielle offre des capacités nouvelles aux équipes de défense : détection d'anomalies comportementales à une échelle et une vitesse inatteignables pour une analyse humaine, corrélation automatisée d'événements de sécurité au sein des SIEM de nouvelle génération, assistance à l'investigation et à la réponse aux incidents, et automatisation de tâches répétitives libérant du temps pour les analyses à plus forte valeur ajoutée. Ces capacités, encore en cours de maturation dans de nombreux outils du marché, ne dispensent cependant pas de la supervision humaine, en particulier pour la qualification finale des alertes et les décisions de réponse aux incidents les plus significatifs.

16.3 Shadow AI

Le « Shadow AI » désigne l'usage, par les collaborateurs, d'outils d'intelligence artificielle générative grand public en dehors de tout cadre validé par l'organisation, par analogie avec le phénomène plus ancien du « Shadow IT ». Cette pratique, en forte expansion, expose l'organisation à un risque de fuite de données significatif : des collaborateurs peuvent, sans intention malveillante, soumettre des informations confidentielles ou des données personnelles à des services d'IA externes dans le cadre de leur usage quotidien, ces données pouvant potentiellement être conservées ou réutilisées par le fournisseur du service selon ses propres conditions d'utilisation.

Face à ce risque, le RSSI doit privilégier une approche pragmatique plutôt qu'une interdiction pure et simple, généralement inefficace et contournée : définir un cadre d'usage clair précisant les outils autorisés et les types d'information pouvant y être soumis, sensibiliser spécifiquement les collaborateurs à ce risque, et, lorsque les moyens de l'organisation le permettent, mettre à disposition des alternatives internes ou contractualisées offrant des garanties de confidentialité suffisantes, plutôt que de laisser cet usage se développer de manière totalement incontrôlée.

16.4 Sécurité des modèles d'IA

Les organisations qui développent ou déploient leurs propres modèles d'intelligence artificielle doivent intégrer des risques spécifiques à ce domaine émergent : l'empoisonnement des données d'entraînement, qui consiste à corrompre délibérément les données utilisées pour entraîner un modèle afin d'en biaiser le comportement, les attaques par injection de requêtes malveillantes (prompt injection), qui visent à manipuler le comportement d'un modèle en production par des instructions dissimulées dans les données qu'il traite, et le vol de modèles, consistant à reconstituer ou extraire un modèle propriétaire par des interrogations répétées. Ces risques, encore peu couverts par des référentiels normatifs stabilisés, nécessitent une veille active du RSSI à mesure que ces technologies se généralisent au sein de son organisation.

16.5 Protection des données utilisées par l'IA

Les systèmes d'intelligence artificielle, particulièrement gourmands en données pour leur entraînement et leur fonctionnement, soulèvent des enjeux de protection des données qui recoupent directement les responsabilités du RSSI développées dans la Partie X de ce guide : les données personnelles utilisées pour entraîner ou alimenter un modèle doivent respecter les mêmes exigences de licéité, de minimisation et de sécurisation que tout autre traitement de données personnelles, ces exigences se trouvant parfois complexifiées par l'opacité des mécanismes internes de certains modèles, qui rend plus difficile la démonstration d'une utilisation conforme des données traitées.

16.6 Gouvernance de l'IA

La gouvernance de l'usage de l'intelligence artificielle au sein de l'organisation constitue un enjeu émergent qui dépasse le seul périmètre du RSSI, mobilisant également la direction juridique, la direction des risques et les directions métier utilisatrices de ces technologies. Le RSSI a néanmoins vocation à y jouer un rôle de premier plan sur les dimensions de sécurité et de protection des données, en contribuant à l'élaboration d'une politique d'usage de l'IA au sein de l'organisation, à l'évaluation des risques associés à chaque nouveau cas d'usage envisagé, et à la définition des exigences de sécurité applicables aux outils et modèles déployés.

Au Bénin, une Stratégie nationale pour l'intelligence artificielle et les mégadonnées a été adoptée en 2023 selon les sources consultées ; les organisations ont intérêt à en suivre les orientations. Les outils opérationnels de cette gouvernance (inventaire, procédure d'autorisation, classification des données, grille d'évaluation des fournisseurs, gestion du Shadow AI) sont présentés aux sections 16.11 à 16.15.

16.7 Risques liés à l'IA générative

Au-delà des risques déjà évoqués, l'intelligence artificielle générative soulève des enjeux spécifiques liés à la fiabilité de ses productions : génération de contenus erronés présentés avec une assurance trompeuse (hallucinations), qui peuvent conduire à des décisions fondées sur des informations incorrectes si elles ne sont pas vérifiées, et risques de propriété intellectuelle liés à l'utilisation de contenus générés dont l'origine et les droits associés restent parfois incertains. Le RSSI, en lien avec les directions concernées, doit contribuer à sensibiliser les utilisateurs de ces outils à la nécessité d'une vérification humaine systématique des productions utilisées dans un contexte professionnel à enjeu.

16.8 Deepfakes et fraude

La capacité croissante de l'intelligence artificielle générative à produire des contenus audio et vidéo synthétiques réalistes (deepfakes) ouvre la voie à de nouvelles formes de fraude, en particulier la fraude au président ou au dirigeant, qui exploite l'usurpation de la voix ou de l'image d'un responsable de l'organisation pour ordonner, par exemple, un virement financier frauduleux. Ce risque, déjà matérialisé dans plusieurs incidents documentés à l'échelle internationale, impose au RSSI de renforcer la sensibilisation des collaborateurs disposant d'un pouvoir de décision financière, et de promouvoir des procédures de vérification systématique par un canal alternatif pour toute instruction sensible reçue de manière inhabituelle, quelle que soit l'apparente légitimité de son origine.

16.9 Automatisation de la cybersécurité

L'automatisation croissante des tâches de sécurité, portée par des solutions d'orchestration et de réponse automatisée (SOAR, Security Orchestration, Automation and Response), permet d'accélérer significativement le traitement des alertes de premier niveau et d'appliquer des mesures de réponse standardisées sans intervention humaine systématique, un atout précieux dans un contexte de pénurie de compétences déjà évoqué à plusieurs reprises dans ce guide. Cette automatisation doit cependant rester encadrée par une supervision humaine appropriée, en particulier pour les décisions les plus impactantes, afin d'éviter qu'une automatisation mal calibrée ne produise elle-même des perturbations opérationnelles non désirées.

16.10 Nouvelles compétences du RSSI

L'essor de l'intelligence artificielle impose au RSSI d'élargir son socle de compétences, développé plus largement dans la Partie XVII de ce guide : une compréhension suffisante des principes de fonctionnement des systèmes d'IA pour en évaluer les risques sans nécessairement en maîtriser les aspects les plus techniques, une capacité à dialoguer avec les équipes data science et les directions métier sur les enjeux de gouvernance de ces technologies, et une veille active sur un domaine dont les usages, les risques et les référentiels normatifs

évoluent à un rythme nettement plus rapide que dans la plupart des autres domaines couverts par ce guide.

16.11 Inventaire des usages de l'IA

On ne protège pas ce que l'on ne connaît pas. La première mesure consiste à tenir un inventaire des usages de l'IA, couvrant les outils autorisés, les fonctionnalités d'IA intégrées dans des logiciels existants, les développements internes et les usages individuels découverts. Chaque entrée précise : l'usage et son propriétaire métier, l'outil et son fournisseur, la nature des données traitées (selon la classification de la section 16.13), les utilisateurs concernés, l'hébergement et les transferts de données, le niveau de risque, le statut d'autorisation et la date de dernière revue.

L'inventaire est alimenté par trois sources : les déclarations des directions, l'analyse des flux sortants et des applications SaaS, et des campagnes de recensement. Il est revu au moins une fois par an, à titre indicatif.

16.12 Procédure d'autorisation d'un usage de l'IA

Une procédure légère, graduée selon le niveau de risque, évite à la fois le blocage et la dérive. Le tableau suivant en décrit les étapes.

Étape	Action	Qui	Résultat
1. Demande	Le métier décrit l'usage, l'objectif et les données concernées	Direction métier (demandeur)	Fiche de demande
2. Qualification	Classification des données ; niveau de risque (faible, moyen, élevé) ; vérification que l'usage n'est pas interdit	RSSI et DPO	Niveau de risque retenu
3. Évaluation du fournisseur	Application de la grille de la section 16.14	RSSI, juridique, achats	Score et réserves
4. Décision	Risque faible : RSSI ; risque moyen : comité de sécurité ; risque élevé ou données sensibles : Direction générale	Instance compétente	Autorisation, refus ou autorisation conditionnelle
5. Conditions	Configuration, formation, désactivation de la réutilisation des données, journalisation, clauses contractuelles	DSI, juridique	Conditions de mise en service
6. Enregistrement	Inscription à l'inventaire des usages	RSSI ou DSI	Registre à jour
7. Revue	Revue périodique et à chaque changement significatif (nouvelle version, nouveau fournisseur, nouvelles données)	RSSI	Décision maintenue, adaptée ou retirée

16.13 Classification des données utilisables avec l'IA

La règle d'usage dépend de la sensibilité des données. La grille suivante s'appuie sur la classification des informations de l'organisation ; à défaut, établir cette classification est un préalable.

Classe	Exemples	Règle d'usage avec des outils d'IA
Publique	Communiqués, contenus publiés	Autorisée avec tout outil validé, y compris grand public
Interne	Notes de service, procédures non sensibles	Autorisée uniquement avec des outils validés par l'organisation (contrat, absence de réutilisation des données)
Confidentielle	Données financières non publiées, contrats, dossiers clients, secrets d'affaires	Uniquement avec des outils ou instances contractualisés offrant des garanties (hébergement, non-réutilisation, journalisation), après autorisation
Sensible ou réglementée	Données de santé, données de paiement, données de sécurité (identifiants, configurations), informations classifiées	Interdite avec des services externes non maîtrisés ; usage uniquement sur des environnements internes validés, avec analyse d'impact et avis du DPO

16.14 Grille d'évaluation des fournisseurs d'IA

Chaque critère est noté de 0 (non satisfait) à 2 (pleinement satisfait, preuve à l'appui). À titre indicatif, un score supérieur à 80 % du maximum permet une autorisation, entre 60 % et 80 % une autorisation conditionnelle, en dessous un refus ou un recours à une alternative.

Domaine	Question à poser au fournisseur	Preuve attendue	Score (0 à 2)
Gouvernance	Le fournisseur dispose-t-il de certifications ou d'attestations de sécurité (ISO/CEI 27001, ISO/CEI 42001 ou équivalent) ?	Certificats, périmètre, dates	
Gouvernance	Une politique d'IA responsable et un processus de gestion des incidents sont-ils documentés ?	Politique, procédure	
Données	Les données saisies sont-elles utilisées pour entraîner les modèles du fournisseur ? Peut-on l'interdire contractuellement ?	Conditions d'utilisation, clause	
Données	Quelles sont les durées de conservation, les modalités de suppression et la localisation de l'hébergement ?	Documentation, accord de traitement	
Sécurité	Chiffrement en transit et au repos, authentification forte et SSO, gestion des rôles ?	Fiche technique, tests	
Sécurité	Journalisation et export des journaux pour le SIEM de l'organisation ?	Capacités de journalisation	
Sécurité	Délai et modalités de notification des incidents de sécurité au client ?	Clause contractuelle	
Modèle	Mesures contre l'injection de requêtes, les fuites et les contenus nuisibles ; tests réguliers ?	Rapports de test	
Contrat	Propriété des productions, garanties relatives à la propriété intellectuelle, sous-traitants ultérieurs listés ?	Contrat, annexes	

Domaine	Question à poser au fournisseur	Preuve attendue	Score (0 à 2)
Contrat	Réversibilité, restitution et suppression des données en fin de contrat ?	Clause de réversibilité	
Données personnelles	Rôle du fournisseur (sous-traitant), accord de traitement, transferts hors du pays encadrés, appui à l'exercice des droits ?	Accord de traitement	
Continuité	Engagements de disponibilité, plan de continuité, dépendance à un sous-traitant unique ?	SLA, plan de continuité	

16.15 Gestion du Shadow AI

Le Shadow AI se gère par le cycle suivant plutôt que par l'interdiction pure et simple :

- Détecter : analyse des flux sortants et des applications SaaS, déclarations spontanées, enquêtes auprès des directions ;
- Évaluer : appliquer la procédure d'autorisation (16.12) aux usages découverts, en privilégiant la régularisation à la sanction ;
- Régulariser ou bloquer : autoriser sous conditions, ou bloquer lorsque le risque est inacceptable et qu'aucune alternative n'existe ;
- Offrir une alternative : mettre à disposition un outil validé répondant au besoin réel ;
- Sensibiliser : expliquer les règles d'usage par classe de données et les raisons de ces règles ;
- Mesurer : nombre d'outils d'IA non autorisés détectés, part des usages inventoriés, délai de traitement des demandes, incidents liés à l'IA.

XVII

PARTIE XVII · CHAPITRE 17

Profil, compétences et carrière du RSSI

Devenir un RSSI performant

CE QUE LA DIRECTION DOIT SAVOIR

1

Un bon RSSI n'est pas nécessairement le meilleur technicien de l'organisation : c'est avant tout un professionnel capable de conjuguer compréhension du risque, gouvernance et communication avec la Direction.

2

Les compétences de leadership, de communication et de compréhension du business pèsent au moins autant que les compétences techniques dans la réussite d'un RSSI.

3

Investir dans le développement de carrière du RSSI et de son équipe est un facteur direct de rétention, dans un marché où la concurrence pour ces profils est intense.

17.1 Compétences techniques

Un socle de compétences techniques reste nécessaire à l'exercice de la fonction RSSI, ne serait-ce que pour dialoguer avec crédibilité avec les équipes techniques et évaluer la pertinence des solutions proposées. Ce socle couvre une compréhension générale des architectures réseau et systèmes, des principes de la cryptographie, des mécanismes d'authentification et de contrôle d'accès, et des grands domaines techniques détaillés dans la Partie VII de ce guide. Il ne s'agit toutefois pas d'une expertise de spécialiste sur chacun de ces domaines : comme rappelé au début de cette même partie, le RSSI doit comprendre les

17.2 Compétences en gouvernance

Les compétences en gouvernance permettent au RSSI de structurer les instances, politiques et processus décrits dans la Partie V de ce guide, et de faire vivre un dispositif de pilotage cohérent avec les pratiques de gouvernance globales de son organisation. Cette compétence suppose une compréhension des principes de contrôle interne, du modèle des trois lignes de défense, et des mécanismes de reddition de comptes attendus par une Direction générale et un Conseil d'administration.

17.3 Compétences en gestion des risques

La maîtrise des méthodologies de gestion des risques, développées dans la Partie VI de ce guide, constitue une compétence distinctive du RSSI par rapport à un profil purement technique : elle suppose la capacité à conduire une analyse de risque rigoureuse, à dialoguer avec les métiers pour évaluer des impacts business, et à prioriser objectivement des investissements de sécurité sur la base de cette analyse plutôt que sur la seule base de préférences technologiques personnelles.

17.4 Compétences en gestion financière

La capacité à construire, défendre et piloter un budget, développée dans la Partie XIV de ce guide, constitue une compétence de plus en plus déterminante pour un RSSI appelé à dialoguer avec la Direction financière et à justifier ses arbitrages en termes de retour sur investissement et de coût de l'inaction. Un RSSI dépourvu de cette compétence, aussi brillant soit-il techniquement, se trouve souvent en difficulté pour obtenir les ressources nécessaires à la mise en œuvre de sa stratégie.

17.5 Compétences en management

Dès lors qu'il encadre une équipe, le RSSI doit mobiliser des compétences de management classiques — organisation du travail, évaluation de la performance,

développement des collaborateurs — mais également des compétences spécifiques à l'animation d'une fonction souvent en tension permanente, entre l'urgence de la gestion d'incidents et le temps long de la construction d'un dispositif de sécurité durable. Savoir protéger son équipe d'un rythme d'alerte permanent, tout en maintenant sa réactivité face aux situations réellement critiques, constitue un exercice managérial spécifique à cette fonction.

17.6 Compétences en communication

Déjà largement développée dans la Partie XIII de ce guide consacrée au reporting, la compétence de communication conditionne directement la capacité du RSSI à faire comprendre les enjeux de risque numérique à des publics très divers — dirigeants, collaborateurs, techniciens, partenaires externes — chacun nécessitant un registre et un niveau de détail différents. Cette compétence s'apprend et se travaille, notamment par la pratique répétée de la prise de parole devant des instances de direction et par la recherche systématique de retours sur la clarté de ses présentations.

17.7 Leadership

Le leadership du RSSI se mesure moins à son autorité hiérarchique formelle, souvent limitée en dehors de sa propre équipe, qu'à sa capacité d'influence sur des acteurs qu'il ne dirige pas directement — direction informatique, directions métier, collaborateurs de l'ensemble de l'organisation. Ce leadership d'influence, qui s'appuie sur la crédibilité de l'expertise, la qualité de la relation construite avec les parties prenantes et la constance de l'exemplarité personnelle en matière de sécurité, est souvent ce qui distingue un RSSI dont les recommandations sont suivies d'un RSSI dont l'autorité reste purement théorique.

17.8 Négociation

La négociation intervient dans de nombreuses dimensions de l'activité du RSSI : arbitrage budgétaire avec la Direction financière, négociation de clauses de sécurité avec des fournisseurs, dans le cadre développé à la Partie XII de ce guide, ou encore recherche de compromis avec une direction métier réticente à l'application d'une mesure de sécurité perçue comme contraignante. Cette compétence suppose la capacité à identifier des solutions alternatives préservant l'essentiel de l'exigence de sécurité tout en tenant compte des contraintes légitimes de l'interlocuteur, plutôt qu'une posture rigide qui, à terme, isole le RSSI plutôt qu'elle ne renforce sa position.

17.9 Compréhension du business

Un RSSI qui ne comprend pas en profondeur le modèle économique, les processus métier essentiels et les enjeux stratégiques de son organisation ne peut pas, par

construction, prioriser correctement les risques ni traduire efficacement les enjeux techniques en langage de risque business, tel que développé à la section 13.9 de ce guide. Cette compréhension du business ne s'acquiert pas uniquement par la lecture de documents internes : elle suppose un investissement actif du RSSI dans la connaissance directe des métiers de son organisation, par l'échange régulier avec les directions opérationnelles et, lorsque cela est possible, une immersion dans leurs activités quotidiennes.

17.10 Éthique et déontologie

Le RSSI accède, dans l'exercice de ses fonctions, à des informations sensibles sur les vulnérabilités de l'organisation, sur les comportements individuels des collaborateurs, et parfois sur des situations personnelles délicates révélées à l'occasion d'une investigation. Cette position impose une exigence déontologique particulière : discrétion sur les informations sensibles dont il a connaissance, usage strictement proportionné des pouvoirs d'investigation qui lui sont confiés, et impartialité dans le traitement des situations, y compris lorsqu'elles impliquent des collaborateurs occupant des positions hiérarchiques élevées. Un manquement à ces exigences déontologiques, au-delà de ses conséquences individuelles, peut durablement fragiliser la confiance nécessaire à l'exercice de la fonction dans l'ensemble de l'organisation.

17.11 Certifications pertinentes : CISSP, CISM, CRISC, ISO 27001, etc.

Plusieurs certifications professionnelles reconnues à l'échelle internationale permettent au RSSI de valider et de faire reconnaître son niveau de compétence. La certification CISSP (Certified Information Systems Security Professional) offre une reconnaissance large des compétences techniques et managériales en sécurité de l'information. La certification CISM (Certified Information Security Manager), plus orientée vers la gouvernance et le management de la sécurité, est souvent considérée comme particulièrement adaptée au profil spécifique du RSSI. La certification CRISC (Certified in Risk and Information Systems Control) valorise une expertise approfondie en gestion des risques informatiques.

La certification de formation aux exigences de la norme ISO/CEI 27001 (auditeur ou responsable de mise en œuvre) constitue également une référence reconnue, particulièrement utile pour les RSSI engagés dans une démarche de certification de leur organisation. Au-delà de la reconnaissance qu'elles procurent, ces certifications présentent l'intérêt d'imposer un parcours de formation structuré, couvrant l'ensemble des domaines développés dans ce guide, et de maintenir les compétences à jour grâce aux exigences de formation continue qu'elles imposent généralement pour leur renouvellement.

17.12 Plan de carrière du RSSI

La fonction de RSSI, encore récente dans de nombreuses organisations, ne dispose pas toujours d'un parcours de carrière clairement balisé, contrairement à des fonctions plus anciennes. Plusieurs trajectoires sont néanmoins observées : évolution vers des fonctions de direction plus larges intégrant l'ensemble du risque numérique et technologique (Chief Risk Officer, Chief Digital Officer), spécialisation accrue dans des organisations de plus grande taille ou à enjeux plus critiques, ou orientation vers le conseil et l'accompagnement d'autres organisations, valorisant l'expérience accumulée.

Pour les organisations elles-mêmes, offrir une perspective de carrière crédible à leur RSSI et à son équipe constitue un enjeu de rétention majeur, dans un contexte de pénurie de compétences déjà développé à la section 15.2 de ce guide : un RSSI qui perçoit un plafond de carrière rapide au sein de son organisation sera naturellement plus enclin à répondre favorablement aux sollicitations, nombreuses sur ce marché, d'organisations concurrentes ou de cabinets de conseil spécialisés.

XVIII

PARTIE XVIII · CHAPITRE 18

Les 100 premiers jours du RSSI

Prendre ses fonctions efficacement

CE QUE LA DIRECTION DOIT SAVOIR

1. Les cent premiers jours d'un RSSI nouvellement nommé conditionnent largement sa crédibilité et son efficacité ultérieure : une phase de compréhension bâclée au profit d'une action précipitée se paie généralement plus tard.

2. La Direction doit faciliter, dès l'arrivée du RSSI, l'accès à l'information et aux interlocuteurs nécessaires à cette phase de prise de connaissance.

3. Des livrables concrets doivent être attendus à l'issue de cette période, matérialisant la transition entre la phase de découverte et la phase d'action.

La prise de fonction d'un RSSI, qu'il s'agisse d'une première nomination dans l'organisation ou de l'arrivée d'un nouveau titulaire, mérite une approche structurée, généralement organisée en trois phases successives sur les cent premiers jours : comprendre, diagnostiquer, puis transformer. Cette progression, qui peut sembler évidente une fois énoncée, est pourtant fréquemment négligée au profit d'une action immédiate, avec le risque de mettre en œuvre des mesures mal calibrées faute d'une compréhension suffisante du contexte propre à l'organisation.

Jours 1 à 30 — Comprendre

La première phase doit être consacrée à la compréhension approfondie du contexte dans lequel le RSSI prend ses fonctions, avant toute action corrective. Cette compréhension couvre l'organisation elle-même — sa stratégie, sa culture, ses processus de décision, ses rapports de force internes —, le système d'information dans ses grandes lignes, les actifs critiques déjà identifiés le cas échéant, l'historique des risques et incidents déjà survenus, les contrats en cours avec les prestataires significatifs, le cadre réglementaire applicable, et enfin l'équipe déjà en place, ses compétences et sa dynamique.

Cette phase suppose une série d'entretiens structurés avec l'ensemble des parties prenantes clés — Direction générale, DSI, directions métier principales, équipe sécurité existante, auditeurs internes le cas échéant — davantage qu'une revue documentaire isolée, les entretiens permettant de recueillir des informations souvent absentes des documents formels, notamment sur les dynamiques informelles et les points de friction existants.

Jours 31 à 60 — Diagnostiquer

La deuxième phase consiste à transformer les informations recueillies durant la phase de compréhension en un diagnostic structuré : évaluation de la maturité globale du dispositif de sécurité, selon le modèle développé dans la Partie XIX de ce guide, cartographie initiale des risques prioritaires, identification des vulnérabilités techniques et organisationnelles les plus significatives, évaluation de la gouvernance existante, revue de l'architecture technique en place, et évaluation des ressources humaines et budgétaires disponibles au regard des enjeux identifiés.

Ce diagnostic, même s'il reste nécessairement provisoire à ce stade précoce, doit être suffisamment étayé pour servir de socle à la feuille de route élaborée durant la troisième phase, et suffisamment documenté pour pouvoir être présenté et validé, au moins dans ses grandes lignes, par la Direction générale.

Jours 61 à 100 — Transformer

La troisième phase consiste à engager les premières actions concrètes, en combinant des « quick wins » — mesures à impact rapide et à coût limité, permettant de démontrer une valeur ajoutée tangible dès les premiers mois — et l'élaboration d'une feuille de route de moyen terme, structurée autour des

priorités identifiées lors du diagnostic. Cette phase doit également poser les fondations de gouvernance nécessaires à l'action durable du RSSI : proposition de budget pour la période suivante, mise en place ou consolidation des instances de gouvernance décrites dans la Partie V de ce guide, et définition des premiers indicateurs de pilotage.

Livrables attendus au terme des cent jours

- Un diagnostic de maturité documenté, présenté à la Direction générale ;
- Une cartographie initiale des risques prioritaires ;
- Une feuille de route de sécurité à horizon de douze à vingt-quatre mois, assortie d'une proposition budgétaire ;
- Une première proposition de gouvernance (comité de sécurité, politique de sécurité si elle n'existe pas encore) ;
- Un plan d'action pour les « quick wins » déjà identifiés et, si possible, déjà engagés ;
- Une proposition de charte de fonction et de lettre de mission, si ces documents n'existent pas encore, conformément aux principes développés dans la Partie III de ce guide.

XIX

PARTIE XIX · CHAPITRE 19

Modèle de maturité de la fonction RSSI

Évaluer la maturité de son organisation

CE QUE LA DIRECTION DOIT SAVOIR

1

Un modèle de maturité permet de situer objectivement l'organisation sur une échelle reconnue, et de fixer une trajectoire de progression réaliste plutôt qu'un objectif abstrait de « sécurité totale ».

2

Il n'est ni nécessaire ni toujours souhaitable de viser le niveau de maturité le plus élevé sur l'ensemble des dimensions : le niveau cible doit être proportionné au profil de risque de l'organisation.

3

Une auto-évaluation régulière, même simplifiée, permet d'objectiver les progrès réalisés d'une année sur l'autre et de justifier la poursuite des investissements engagés.

Un modèle de maturité permet d'évaluer, sur une échelle progressive, le niveau de structuration du dispositif de sécurité d'une organisation, indépendamment de son secteur ou de sa taille. Ce type de modèle, largement utilisé dans les démarches d'audit et d'auto-évaluation, structure généralement l'évaluation en cinq niveaux croissants, appliqués à un ensemble de dimensions couvrant l'intégralité du périmètre de la fonction RSSI.

Niveau 1 — Initial / Réactif

À ce niveau, la sécurité de l'information n'est pas gérée de manière structurée : les actions entreprises le sont en réaction à des incidents déjà survenus, sans anticipation ni méthode formalisée. Aucune fonction RSSI n'est clairement identifiée, ou cette fonction est exercée de manière informelle et secondaire par un collaborateur par ailleurs chargé d'autres responsabilités. Ce niveau, encore fréquent dans de nombreuses organisations n'ayant pas encore engagé de démarche structurée, expose à un risque significatif et largement non maîtrisé.

Niveau 2 — Sensibilisé

À ce niveau, l'organisation a pris conscience de l'importance du risque numérique, généralement à la suite d'un incident significatif ou d'une exigence externe (client, régulateur, partenaire), mais les actions entreprises restent ponctuelles et peu coordonnées. Une fonction RSSI a été identifiée, mais dispose de moyens et d'une autorité encore limités, et ne bénéficie pas toujours du positionnement organisationnel décrit dans la Partie III de ce guide.

Niveau 3 — Structuré

Ce niveau marque un basculement significatif : l'organisation dispose d'une politique de sécurité formalisée, d'un registre des risques régulièrement actualisé, d'instances de gouvernance fonctionnelles (comité de sécurité notamment), et d'un socle de mesures techniques couvrant les domaines essentiels décrits dans la Partie VII de ce guide. Le RSSI dispose d'un mandat clair et d'un accès régulier à la Direction générale. La plupart des organisations de taille intermédiaire ayant engagé une démarche structurée se situent à ce niveau, qui constitue un objectif raisonnable à moyen terme pour les organisations encore aux niveaux 1 ou 2.

Niveau 4 — Maîtrisé

À ce niveau, le dispositif de sécurité est non seulement structuré mais mesuré : des indicateurs de performance et de risque sont suivis régulièrement, comme développé dans la Partie XIII de ce guide, les processus sont documentés et appliqués de manière cohérente à l'échelle de l'organisation, et une démarche d'amélioration continue est engagée sur la base des enseignements tirés des incidents et des audits. Ce niveau, généralement associé à une certification

reconnue (ISO 27001 notamment), caractérise les organisations les plus matures du continent, souvent dans les secteurs soumis aux exigences réglementaires les plus strictes.

Niveau 5 — Optimisé

Ce niveau, le plus avancé, caractérise des organisations où la sécurité est pleinement intégrée à la culture et aux processus de décision, où l'innovation en matière de sécurité (automatisation avancée, usage de l'intelligence artificielle en défense, anticipation proactive des menaces émergentes) est activement recherchée, et où le dispositif fait l'objet d'une amélioration continue rigoureusement pilotée par la donnée. Peu d'organisations, y compris à l'échelle internationale, atteignent effectivement ce niveau sur l'ensemble des dimensions simultanément, et il ne constitue pas nécessairement un objectif pertinent pour toute organisation, le niveau cible devant rester proportionné à son profil de risque réel.

Dimensions à évaluer

L'évaluation de la maturité doit être conduite séparément sur chacune des grandes dimensions de la fonction RSSI décrites dans ce guide, une organisation pouvant afficher des niveaux de maturité sensiblement différents d'une dimension à l'autre : gouvernance, organisation et positionnement, gestion des risques, politique de sécurité, gestion des identités et des accès, infrastructure et protection technique, capacités du centre des opérations de sécurité, gestion des incidents, continuité d'activité, conformité réglementaire, ressources humaines et sensibilisation, gestion des fournisseurs, et capacité d'innovation.

Un modèle simplifié d'auto-évaluation de la maturité, reprenant ces dimensions, est proposé en Annexe 7 de ce guide, permettant à une organisation de conduire un premier exercice d'auto-positionnement sans recourir nécessairement à un audit externe, ce dernier restant néanmoins recommandé pour objectiver et approfondir les résultats d'une auto-évaluation initiale.

Critères objectivables et preuves attendues

Une auto-évaluation purement déclarative tend à surestimer le niveau de maturité. Pour la rendre objective, chaque niveau est associé à des critères vérifiables et à des preuves attendues. Quatre règles s'appliquent : (1) un niveau n'est acquis que si tous ses critères sont satisfaits sur la dimension considérée ; (2) chaque critère s'appuie sur au moins une preuve datée ; (3) une preuve absente ou périmée ramène au niveau inférieur ; (4) pour les niveaux 4 et 5, une revue par une personne extérieure à la fonction sécurité (audit interne ou tiers) est recommandée.

Niveau	Critères objectivables	Preuves attendues
1 — Initial / Réactif	Aucune politique approuvée ; pas de RSSI désigné ou rôle informel ; incidents traités au cas par cas	Absence constatée de documents ; incidents passés sans compte rendu
2 — Sensibilisé	RSSI ou référent désigné par écrit ; inventaire, même partiel, des actifs critiques ; au moins une action de sensibilisation ; sauvegardes existantes	Décision de désignation ; liste d'actifs ; support et liste d'émargement de la sensibilisation ; rapport de sauvegarde
3 — Structuré	PSSI approuvée par la Direction générale depuis moins de 24 mois ; charte et lettre de mission signées ; registre des risques actualisé depuis moins de 6 mois ; comité de sécurité réuni au moins deux fois dans l'année ; authentification forte sur les comptes à privilèges ; plan de réponse aux incidents rédigé ; au moins un test de restauration réalisé	PSSI datée et signée ; comptes rendus de comités ; extrait du registre avec dates ; rapport de configuration de l'authentification forte ; plan de réponse ; procès-verbal de test de restauration
4 — Maîtrisé	Indicateurs de performance et de risque suivis trimestriellement avec cibles ; plan de réponse testé au moins une fois en douze mois avec retour d'expérience ; audit interne ou externe réalisé et plan d'actions suivi ; fournisseurs critiques évalués ; actifs critiques couverts par une analyse de risque à jour à 90 % ou plus	Tableaux de bord datés ; rapports d'exercice et retours d'expérience ; rapport d'audit et suivi des recommandations ; grilles d'évaluation des fournisseurs ; registre des risques
5 — Optimisé	Amélioration continue pilotée par la donnée sur plusieurs cycles consécutifs ; détection et réponse avancées mesurées ; exercices de crise impliquant la Direction et des tiers ; certification ou revue externe maintenue ; absence d'écarts majeurs répétitifs	Séries d'indicateurs sur au moins trois périodes ; rapports d'exercices ; certificats et rapports de surveillance ; analyses de tendance

Les seuils chiffrés (24 mois, 6 mois, 90 %) sont des repères à adapter au contexte de l'organisation.



6

BLOC 6

Se professionnaliser et s'adapter

Parties XV à XX

Ce dernier bloc replace la fonction dans son contexte (africain et béninois), traite les nouveaux défis (intelligence artificielle), décrit le profil du RSSI, ses cent premiers jours, le modèle de maturité et présente la boîte à outils du RSSI.

Lecture prioritaire pour : RSSI en poste ou futurs RSSI, Direction générale, organismes de formation.

Partie	Contenu	Niveau principal
XV	Le RSSI dans les organisations africaines (chapitre 15)	Décider / Piloter
XVI	Le RSSI à l'ère de l'intelligence artificielle (chapitre 16)	Piloter
XVII	Profil, compétences et carrière du RSSI (chapitre 17)	Piloter
XVIII	Les 100 premiers jours du RSSI (chapitre 18)	Piloter
XIX	Modèle de maturité de la fonction RSSI (chapitre 19)	Décider / Piloter
XX	Boîte à outils du RSSI (chapitre 20)	Piloter / Opérer

XX

PARTIE XX · CHAPITRE 20

Boîte à outils du RSSI

Modèles et outils pratiques

CE QUE LA DIRECTION DOIT SAVOIR

1

Cette boîte à outils rassemble les modèles-cadres correspondant aux principaux livrables évoqués tout au long de ce guide, à adapter au contexte propre de chaque organisation.

2

Le tableau de bord RSSI fait l'objet d'un développement complet, disponible en Annexe 9 de ce guide.

3

L'existence de ces modèles ne dispense pas d'une appropriation réelle par l'organisation : un document copié sans adaptation au contexte perd l'essentiel de sa valeur.

Cette boîte à outils recense les principaux modèles et supports pratiques évoqués tout au long de ce guide, destinés à faciliter leur mise en œuvre concrète par le RSSI. Chaque modèle est décrit ci-dessous avec son objectif et son contenu attendu ; les organisations souhaitant disposer de ces documents entièrement rédigés et prêts à compléter peuvent solliciter leur élaboration détaillée, sur le modèle du Tableau de bord RSSI déjà intégré en Annexe 9 de ce guide.

A. LETTRE DE MISSION DU RSSI

Document individuel adressé au titulaire du poste, précisant les objectifs assignés pour la période, les moyens alloués et les modalités d'évaluation (voir section 3.9).

B. CHARTE DE LA FONCTION RSSI

Document de gouvernance pérenne formalisant le mandat, le rattachement, l'autorité et les prérogatives de la fonction (voir section 3.8).

C. ORGANIGRAMME TYPE DE LA FONCTION SÉCURITÉ

Représentation des rattachements hiérarchiques et fonctionnels recommandés, déclinée selon la taille de l'organisation (voir Partie III et Annexe 4).

D. POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION (PSSI)

Modèle de document-cadre énonçant les principes directeurs de sécurité applicables à l'ensemble de l'organisation (voir section 5.2).

E. REGISTRE DES RISQUES

Modèle tabulaire recensant les scénarios de risque, leur évaluation, leur traitement et leur suivi (voir section 6.7).

F. CARTOGRAPHIE DES RISQUES

Modèle de matrice probabilité / impact pour la représentation visuelle synthétique des risques (voir section 6.8).

G. TABLEAU DE BORD RSSI

Modèle complet d'indicateurs de pilotage par domaine, intégré en Annexe 9 de ce guide (voir section 13.2).

H. MATRICE KPI / KRI

Grille de distinction et de suivi séparé des indicateurs de performance et des indicateurs de risque (voir section 13.3).

I. PLAN D'ACTION CYBERSÉCURITÉ

Modèle de suivi des actions issues de la stratégie de sécurité, avec propriétaires et échéances.

J. PLAN DE TRAITEMENT DES RISQUES

Modèle de suivi détaillé des mesures de traitement associées à chaque risque identifié (voir section 6.10).

K. FICHE DE DÉCLARATION D'INCIDENT

Support standardisé permettant à tout collaborateur de signaler un incident suspecté (voir section 8.1).

L. PROCÉDURE DE GESTION DES INCIDENTS

Document opérationnel détaillant les étapes de qualification, containment, éradication et restauration (voir Partie VIII).

M. PLAN DE COMMUNICATION DE CRISE

Modèle d'éléments de langage et de plan de diffusion pour la communication interne et externe en cas d'incident majeur (voir section 8.9).

N. QUESTIONNAIRE D'ÉVALUATION D'UN FOURNISSEUR

Grille de due diligence sécurité à utiliser avant contractualisation avec un prestataire (voir section 12.2).

O. CHECKLIST D'AUDIT DE SÉCURITÉ

Liste de contrôle couvrant les principaux domaines à examiner lors d'un audit interne ou externe.

P. CHECKLIST D'ARRIVÉE D'UN NOUVEAU COLLABORATEUR

Liste des actions de sécurité à réaliser lors de l'intégration d'un collaborateur (voir section 11.5).

Q. CHECKLIST DE DÉPART D'UN COLLABORATEUR

Liste des actions de sécurité à réaliser lors du départ d'un collaborateur, notamment la révocation des accès (voir section 11.6).

R. MODÈLE DE RAPPORT RSSI MENSUEL

Support de reporting opérationnel interne à la fonction sécurité et à la DSI (voir section 13.5).

S. MODÈLE DE RAPPORT RSSI AU COMITÉ DE DIRECTION

Support de reporting trimestriel synthétique destiné à la Direction générale (voir section 13.6).

T. MODÈLE DE PRÉSENTATION AU CONSEIL D'ADMINISTRATION

Support de reporting annuel ou semestriel destiné aux administrateurs (voir section 13.7).

U. MODÈLE DE BUDGET CYBERSÉCURITÉ

Grille de construction budgétaire structurée par domaine de risque, distinguant CAPEX et OPEX (voir Partie XIV).

V. MATRICE RACI CYBERSÉCURITÉ

Tableau de répartition des responsabilités (Responsable, Approbateur, Consulté, Informé) par processus de sécurité (voir section 5.6).

W. TABLEAU DE SUIVI DES VULNÉRABILITÉS

Registre opérationnel des vulnérabilités identifiées, de leur criticité et de leur statut de correction (voir section 7.16).

X. TABLEAU DE SUIVI DES INCIDENTS

Registre consolidé des incidents survenus, de leur qualification et de leur traitement (voir Partie VIII).

A

ANNEXES 1 À 10

Annexes

Annexe 1 — Glossaire cybersécurité

Ce glossaire rassemble les principaux acronymes utilisés tout au long de ce guide.

RSSI : Responsable de la Sécurité des Systèmes d'Information (CISO en anglais)

DSI : Direction / Directeur des Systèmes d'Information

SOC : Security Operations Center — Centre des Opérations de Sécurité (voir 7.15)

SIEM : Security Information and Event Management — gestion des informations et événements de sécurité (voir 7.14)

IAM : Identity and Access Management — gestion des identités et des accès (voir 7.1)

PAM : Privileged Access Management — gestion des accès privilégiés (voir 7.3)

EDR : Endpoint Detection and Response — détection et réponse sur les postes de travail

XDR : Extended Detection and Response — détection et réponse étendue, au-delà du seul poste de travail

PKI : Public Key Infrastructure — infrastructure à clés publiques (voir 7.12)

HSM : Hardware Security Module — module matériel de sécurité pour la gestion des clés cryptographiques

MFA : Multi-Factor Authentication — authentification multifacteurs (voir 7.2)

BIA : Business Impact Analysis — analyse d'impact sur l'activité (voir 9.1)

PCA : Plan de Continuité d'Activité (voir 9.2)

PRA : Plan de Reprise d'Activité (voir 9.3)

RTO : Recovery Time Objective — délai de reprise cible (voir 9.4)

RPO : Recovery Point Objective — perte de données maximale tolérée (voir 9.4)

KPI : Key Performance Indicator — indicateur de performance (voir 13.3)

KRI : Key Risk Indicator — indicateur de risque (voir 13.3)

DPO : Data Protection Officer — Délégué à la Protection des Données (voir 2.9)

SOAR : Security Orchestration, Automation and Response — orchestration et automatisation de la réponse de sécurité (voir 16.9)

MTTD / **MTTR** : Mean Time To Detect / Mean Time To Respond — délais moyens de détection et de réponse à un incident (voir 8.3, 13.3)

ASIN : Agence des Systèmes d'Information et du Numérique (Bénin, créée en 2022)

APDP : Autorité de Protection des Données à caractère Personnel (Bénin)

bjCSIRT : équipe nationale béninoise de réponse aux incidents de sécurité informatique (voir 8.14)

OIIC : Opérateur d'Infrastructure d'Information Critique

PSSIE : Politique de Sécurité des Systèmes d'Information de l'État (Bénin)

PPIIC : règles de Politique de Protection des Infrastructures d'Information Critiques (Bénin)

SNSN : Stratégie Nationale de Sécurité Numérique (Bénin)

OCRC : Office Central de Répression de la Cybercriminalité (Bénin)

PRIC : Plan de Réponse aux Incidents de Cybersécurité (voir 8.12)

CSIRT : Computer Security Incident Response Team — équipe de réponse aux incidents de sécurité informatique

CVSS : Common Vulnerability Scoring System — système de notation de la sévérité des vulnérabilités (voir 7.16)

EPSS : Exploit Prediction Scoring System — probabilité d'exploitation d'une vulnérabilité

DLP : Data Loss Prevention — prévention des fuites de données

RACI : Responsible, Accountable, Consulted, Informed — matrice de répartition des responsabilités (Annexe 10)

DIC : disponibilité, intégrité, confidentialité

Annexe 2 — Référentiels et normes

Cette annexe recense les principaux référentiels et normes cités dans ce guide, avec pour chacun l'éditeur, la version et l'année de référence, l'objet, le caractère obligatoire ou recommandé et le lien officiel.

Référentiel	Éditeur	Version / année	Objet	Statut	Lien officiel
ISO/CEI 27001	ISO/IEC	2022 (+ Amd 1:2024)	Exigences d'un système de management de la sécurité de l'information (SMSI)	Volontaire ; certifiable ; peut être exigé par des clients, partenaires ou régulateurs	iso.org/standard/27001
ISO/CEI 27002	ISO/IEC	2022	Mesures de sécurité de l'information (93 mesures)	Recommandé	iso.org/standard/75652.html
ISO/CEI 27005	ISO/IEC	2022	Gestion des risques liés à la sécurité de l'information	Recommandé	iso.org/standard/80585.html
ISO/CEI 27701	ISO/IEC	2025 (remplace l'édition 2019)	Système de management de la protection de la vie privée ; désormais norme autonome, certifiable sans ISO 27001	Volontaire ; certifiable	iso.org (rechercher « 27701 »)
ISO/CEI 27035-1	ISO/IEC	2023	Gestion des incidents de sécurité de l'information	Recommandé	iso.org (rechercher « 27035 »)
ISO 22301	ISO	2019	Systèmes de management de la continuité d'activité	Volontaire ; certifiable	iso.org/standard/75106.html
ISO 31000	ISO	2018	Lignes directrices de management du risque	Recommandé	iso.org/standard/65694.html
ISO/CEI 42001	ISO/IEC	2023	Système de management de l'intelligence artificielle	Volontaire ; certifiable	iso.org/standard/81230.html
NIST Cybersecurity Framework	NIST (États-Unis)	2.0 — février 2024	Cadre de gestion des risques cyber (gouverner, identifier, protéger, détecter, répondre, rétablir)	Volontaire	nist.gov/cyberframework

Référentiel	Éditeur	Version / année	Objet	Statut	Lien officiel
NIST RMF (SP 800-37)	NIST	Révision 2 — 2018	Cadre de gestion des risques et d'autorisation des systèmes	Obligatoire pour les agences fédérales américaines ; recommandé ailleurs	csrc.nist.gov/pubs/sp/800/37/r2/final
NIST AI RMF	NIST	1.0 — janvier 2023	Gestion des risques liés à l'intelligence artificielle	Volontaire	nist.gov/itl/ai-risk-management-framework
CIS Controls	Center for Internet Security	v8.1 — 2024	Dix-huit mesures de sécurité priorisées, groupes de mise en œuvre IG1 à IG3	Recommandé	cisecurity.org/controls
COBIT	ISACA	COBIT 2019	Gouvernance et management des technologies de l'information	Recommandé	isaca.org/resources/cobit
EBIOS Risk Manager	ANSSI (France), Club EBIOS	Méthode 2018 ; guide v1.5 (2024)	Appréciation et traitement du risque numérique en cinq ateliers	Recommandé ; obligatoire seulement dans certains cadres français	cyber.gouv.fr/la-methode-ebios-risk-manager
OCTAVE Allegro	SEI, Carnegie Mellon	2007	Auto-évaluation des risques centrée sur les actifs informationnels	Recommandé	sei.cmu.edu (rechercher « OCTAVE Allegro »)

Vérification des versions : octobre 2026.

Annexe 3 — Principales réglementations africaines et cadre béninois

A. Panorama africain et international

Cette annexe rappelle, à titre de repère général, les principaux textes et initiatives structurant le cadre réglementaire africain en matière de cybersécurité et de protection des données, déjà développés à la section 15.8 de ce guide.

- Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles (Convention de Malabo, 2014), progressivement ratifiée par les États membres ;
- Législations nationales de protection des données personnelles, en développement rapide dans un nombre croissant de pays du continent ;

- Réglementations sectorielles émanant des banques centrales et autorités de régulation financière, imposant des exigences de sécurité renforcées au secteur bancaire et financier ;
- Réglementations des autorités de régulation des télécommunications, encadrant la sécurité et la protection des données des opérateurs ;
- Initiatives régionales de coopération en cybersécurité, portées par les communautés économiques régionales et les équipes de réponse aux incidents (CERT/CSIRT) nationales.

Ce panorama général doit impérativement être complété par une vérification précise, auprès de la direction juridique de chaque organisation, du cadre réglementaire effectivement applicable dans le ou les pays où elle opère, ce cadre évoluant rapidement et variant significativement d'un pays à l'autre.

B. Cadre légal et réglementaire du Bénin

Cette section recense, à titre de repère, les principaux textes et institutions du cadre béninois cités dans ce guide. Elle a été établie à partir de sources publiques consultées en octobre 2026. Elle ne remplace pas la lecture des textes eux-mêmes ni l'avis de la Direction juridique : chaque texte doit être validé auprès de l'autorité compétente (Secrétariat général du Gouvernement, ASIN, APDP) avant toute décision de conformité.

Texte	Référence	Objet et pertinence pour le RSSI	Source
Code du numérique	Loi n° 2017-20 du 20 avril 2018, modifiée par la loi n° 2020-35 du 6 janvier 2021	Cadre général : services de confiance, protection des données personnelles (Livre V, dont l'article 427 sur la notification des violations), sécurité des systèmes d'information (Livre VI), cybercriminalité	sgg.gouv.bj/doc/loi-2017-20
PSSIE	Décret n° 2021-550 du 27 octobre 2021	Politique de sécurité des systèmes d'information de l'État ; déclaration des incidents au bjCSIRT par les institutions de l'État	asin.bj (documentation)
Protection des infrastructures d'information critiques	Décret n° 2023-060 du 22 février 2023	Règles applicables aux opérateurs d'infrastructures d'information critiques : détection et réponse aux incidents, continuité, coordination, sanctions	numerique.gouv.bj (règles de politique de protection des infrastructures d'information critiques)
Stratégie nationale de sécurité numérique (SNSN)	Première version 2019 ; mise à jour 2023-2026	Orientations de l'État en matière de sécurité numérique	asin.bj (documentation)
Stratégie nationale IA et mégadonnées	Adoptée en 2023 selon les sources consultées	Orientations de l'État sur l'intelligence artificielle	numerique.gouv.bj
Convention de Malabo	Signée en 2015 ; ratifiée le 26 novembre 2024	Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel	au.int (traités)

Texte	Référence	Objet et pertinence pour le RSSI	Source
Convention de Budapest	Adhésion en 2024	Convention du Conseil de l'Europe sur la cybercriminalité et ses protocoles	coe.int (cybercriminalité)

Institutions et autorités

Institution	Description	Rôle pour le RSSI	Site
ASIN	Agence des systèmes d'information et du numérique, créée en 2022 par fusion de plusieurs agences dont l'ANSSI	Sécurité des systèmes d'information, transformation numérique	asin.bj
bjCSIRT	Équipe nationale de réponse aux incidents de sécurité informatique, opérationnelle depuis 2017	Déclaration et assistance en cas d'incident ; bulletins d'alerte	csirt.gouv.bj
APDP	Autorité de protection des données à caractère personnel	Formalités préalables, contrôle, sanctions, notification des violations	apdp.bj
CININ	Centre central de répression de la cybercriminalité (Ministère de l'Intérieur)	Enquêtes et dépôt de plainte	cnin.bj
Autorités sectorielles	Banque centrale et Commission bancaire de l'UMOA ; ARCEP Bénin ; autres régulateurs	Exigences prudentielles, de continuité et de notification propres aux secteurs régulés	À confirmer pour chaque secteur

Annexe 4 — Exemple d'organigramme cybersécurité

Cette annexe illustre, à titre d'exemple, une organisation type de la fonction sécurité pour une organisation de taille intermédiaire à grande, conforme aux principes de positionnement développés dans la Partie III de ce guide : un RSSI rattaché à la Direction générale ou à la Direction des risques, animant une équipe structurée autour de trois pôles complémentaires — un pôle gouvernance, risques et conformité, chargé notamment de la gestion des risques et du reporting ; un pôle architecture et protection technique, chargé de la définition des exigences techniques et du pilotage de leur mise en œuvre par la DSI ; et un pôle opérations et réponse aux incidents, animant le lien avec le SOC, interne ou externalisé, et pilotant la gestion des incidents.

Pour les organisations de taille plus modeste, cette structure peut être considérablement simplifiée, ainsi qu'évoqué à la section 15.14 de ce guide

consacrée aux PME, jusqu'à se réduire à un référent sécurité unique, appuyé par des prestataires externes pour les compétences les plus spécialisées.

Annexe 5 — Exemple de tableau de bord RSSI

Un modèle complet de tableau de bord RSSI, structuré en neuf domaines (gouvernance, gestion des risques, protection et vulnérabilités, gestion des incidents, continuité d'activité, conformité réglementaire, sensibilisation, tiers et fournisseurs, ressources et budget) et comprenant une quarantaine d'indicateurs prêts à être complétés, est intégré en Annexe 9 de ce guide.

Annexe 6 — Auto-évaluation du RSSI

Cette auto-évaluation permet à tout titulaire de la fonction RSSI de faire un point personnel sur l'exercice de ses responsabilités, en répondant honnêtement aux questions suivantes.

- Ai-je un accès régulier et direct à la Direction générale, conformément aux principes développés à la section 3.6 ?
- Ma charte de fonction et ma lettre de mission sont-elles à jour et formellement approuvées ?
- Mon registre des risques a-t-il été actualisé au cours des six derniers mois ?
- Ai-je présenté un reporting structuré à la Direction Générale au cours du dernier trimestre ?
- Mon plan de réponse aux incidents de cybersécurité a-t-il été testé au cours des douze derniers mois ?
- Suis-je en mesure de répondre avec précision aux dix questions listées à la section 4.9 de ce guide, si elles m'étaient posées par ma Direction ?
- Ai-je consacré du temps, au cours de la dernière année, au développement de mes propres compétences, telles que décrites dans la Partie XVII de ce guide ?
- Mon équipe dispose-t-elle d'un plan de développement des compétences documenté ?

Annexe 7 — Auto-évaluation de l'organisation

Cette auto-évaluation simplifiée, fondée sur le modèle de maturité présenté dans la Partie XIX de ce guide, permet à une organisation de situer approximativement son niveau de maturité sur chacune des dimensions suivantes, en s'attribuant un niveau de 1 (Initial) à 5 (Optimisé) : gouvernance de la sécurité ; positionnement et autorité de la fonction RSSI ; gestion des risques ; corpus documentaire de politiques et procédures ; gestion des identités et des accès ; protection technique de l'infrastructure ; capacités de détection et de réponse aux incidents ; continuité d'activité et résilience ; conformité réglementaire ; sensibilisation et culture de sécurité ; gestion du risque fournisseurs ; budget et ressources.

Une organisation affichant des niveaux hétérogènes selon les dimensions — par exemple un niveau élevé en protection technique mais un niveau faible en gouvernance — devrait prioriser le renforcement des dimensions les plus faibles, ces dernières constituant généralement le facteur limitant de la maturité globale du dispositif, indépendamment des progrès réalisés sur les autres dimensions.

Annexe 8 — Checklist « Mon organisation est-elle réellement sécurisée ? »

Cette checklist, destinée en priorité aux dirigeants, reprend et complète les dix questions présentées à la section 4.9 de ce guide, sous une forme permettant une réponse rapide par oui ou par non.

Un RSSI est-il formellement désigné, avec une charte de fonction et une lettre de mission approuvées ?

Le RSSI dispose-t-il d'un accès direct et régulier à la Direction générale ?

Un registre des risques cyber existe-t-il et est-il actualisé au moins semestriellement ?

Une politique de sécurité de l'information a-t-elle été formellement approuvée par la Direction ?

L'authentification forte est-elle déployée sur l'ensemble des comptes à privilèges ?

Les sauvegardes critiques sont-elles isolées et testées en restauration au moins annuellement ?

Un plan de réponse aux incidents de cybersécurité existe-t-il et a-t-il été testé au cours des douze derniers mois ?

Les collaborateurs bénéficient-ils d'une sensibilisation à la sécurité au moins une fois par an ?

Les fournisseurs critiques ont-ils fait l'objet d'une évaluation de sécurité ?

Un budget de sécurité dédié, distinct du budget informatique général, est-il alloué chaque année ?

Un nombre significatif de réponses négatives à cette checklist ne signifie pas nécessairement que l'organisation est en situation de danger immédiat, mais indique de manière fiable l'existence de lacunes de gouvernance qui méritent une attention prioritaire de la Direction, dans l'esprit développé tout au long de ce guide.

Annexe 9 — Tableau de bord RSSI

Ce tableau de bord rassemble les indicateurs clés (KPI) permettant au RSSI de piloter dans la durée la maîtrise du risque numérique de l'organisation, déjà présenté en principe à la section 13.2 de ce guide. Il est organisé en neuf domaines, correspondant aux grandes responsabilités du RSSI décrites tout au long de cet ouvrage.

Pour chaque indicateur, les colonnes « Fréquence », « Cible » et « Mode de calcul » sont pré-renseignées à titre de référence et doivent être ajustées selon le contexte de l'organisation. Les colonnes « Valeur actuelle », « Statut » et « Commentaire » sont laissées vierges, à compléter à chaque cycle de reporting par le RSSI, selon le code couleur ci-dessous.

	Vert — Maîtrisé	Indicateur conforme à la cible ; aucune action requise au-delà du suivi courant.
	Orange — Sous surveillance	Écart à la cible constaté ; un plan d'action est engagé ou à engager.
	Rouge — Critique	Écart significatif ou risque avéré ; alerte et arbitrage de la Direction requis.

Synthèse exécutive de la période

À compléter par le RSSI avant présentation à la Direction générale / au Comité d'audit.

Période couverte	
Nombre d'indicateurs au statut Vert / Orange / Rouge	
Principaux risques ou alertes de la période	
Principales actions engagées	
Décisions ou arbitrages attendus de la Direction	

1 Gouvernance et pilotage

Indicateurs mesurant l'existence, l'actualisation et le fonctionnement effectif du dispositif de gouvernance de la sécurité.

Indicateur	Fréquence	Cible de référence	Mode de calcul / unité	Valeur actuelle	Statut	Commentaire
Existence d'une politique de sécurité approuvée par la Direction	Annuelle	Oui, à jour (< 12 mois)	Oui / Non + date de dernière révision			
Nombre de réunions du Comité de sécurité tenues sur la période	Trimestrielle	100 % des réunions planifiées tenues	Nombre / Nombre prévu			
Présentation du RSSI au Comité de direction	Trimestrielle	Au moins 1 fois par trimestre	Nombre de présentations			
Présentation au Conseil d'administration / Comité d'audit	Annuelle ou semestrielle	Au moins 1 fois par an	Oui / Non			
Existence d'une charte de fonction RSSI et d'une lettre de mission à jour	Annuelle	Oui, signées et à jour	Oui / Non			
Taux d'avancement du plan de traitement des risques	Trimestrielle	≥ 80 % des actions dans les délais	% d'actions réalisées dans les délais			

2 Gestion des risques

Ces valeurs cibles sont indicatives : chaque entité les ajuste selon ses risques, son secteur et ses obligations.

Indicateur	Fréquence	Cible de référence	Mode de calcul / unité	Valeur actuelle	Statut	Commentaire
Taux de couverture des actifs critiques par une analyse de risque à jour	Semestrielle	≥ 90 %	% des actifs critiques couverts			
Nombre de risques majeurs identifiés et non traités	Mensuelle	0 sans plan d'action validé	Nombre			
Ancienneté moyenne du registre des risques	Semestrielle	< 6 mois	Mois depuis dernière mise à jour			
Nombre de risques formellement acceptés par la Direction	Trimestrielle	Suivi et traçabilité à 100 %	Nombre + % documentés			
Niveau de maturité global du dispositif de sécurité (référentiel utilisé)	Annuelle	Progression continue vers la cible fixée	Score / échelle du référentiel			

3 Protection et vulnérabilités

Indicateurs mesurant l'exposition technique de l'organisation et la rapidité de remédiation.

Indicateur	Fréquence	Cible de référence	Mode de calcul / unité	Valeur actuelle	Statut	Commentaire
Nombre de vulnérabilités critiques ouvertes	Mensuelle	0 non traitée au-delà du délai cible	Nombre			
Délai moyen de correction des vulnérabilités critiques	Mensuelle	≤ 15 jours (critiques), ≤ 30 jours (élevées)	Jours			
Taux de couverture du parc par un antivirus / EDR à jour	Mensuelle	≥ 98 %	% du parc couvert			
Taux de comptes à privilèges protégés par authentification forte (MFA)	Trimestrielle	100 %	% des comptes			
Taux de systèmes critiques sauvegardés et testés en restauration	Trimestrielle	100 %	% testé avec succès			
Nombre de tests d'intrusion / scans réalisés sur la période	Annuelle	Au moins 1 par an sur le périmètre critique	Nombre			

4 Gestion des incidents

Indicateurs mesurant la capacité de détection et de réponse aux incidents de sécurité (à interpréter en tendance et en qualité de traitement, jamais en volume brut seul — voir Partie IV du guide).

Indicateur	Fréquence	Cible de référence	Mode de calcul / unité	Valeur actuelle	Statut	Commentaire
Nombre d'incidents de sécurité détectés sur la période	Mensuelle	Suivi de tendance (pas de cible en valeur absolue)	Nombre, par niveau de gravité			
Délai moyen de détection d'un incident (MTTD)	Mensuelle	En réduction continue	Heures			
Délai moyen de réponse et de résolution (MTTR)	Mensuelle	En réduction continue	Heures			
Nombre d'incidents ayant impacté la continuité d'activité	Trimestrielle	0 non anticipé dans le PCA	Nombre			
Taux d'incidents ayant fait l'objet d'un retour d'expérience formalisé	Trimestrielle	100 % des incidents majeurs	%			
Existence et test du plan de réponse à incident	Annuelle	Testé au moins 1 fois par an	Oui / Non + date du dernier test			

5 Continuité d'activité

Indicateurs mesurant la préparation de l'organisation face à un scénario de crise cyber majeure.

Indicateur	Fréquence	Cible de référence	Mode de calcul / unité	Valeur actuelle	Statut	Commentaire
Existence d'un PCA / PRA intégrant des scénarios de crise cyber	Annuelle	Oui, à jour	Oui / Non			
Nombre d'exercices de simulation de crise cyber réalisés	Annuelle	Au moins 1 par an	Nombre			
RTO (délai de reprise cible) atteint lors du dernier test	Annuelle	Conforme à l'objectif fixé	Oui / Non + écart			
RPO (perte de données maximale tolérée) atteint lors du dernier test	Annuelle	Conforme à l'objectif fixé	Oui / Non + écart			

6 Conformité réglementaire

Indicateurs mesurant le respect des obligations légales, réglementaires, sectorielles et contractuelles applicables.

Indicateur	Fréquence	Cible de référence	Mode de calcul / unité	Valeur actuelle	Statut	Commentaire
Taux de conformité aux obligations réglementaires applicables	Semestrielle	100 % ou plan de mise en conformité daté	%			
Nombre d'écarts de conformité majeurs ouverts	Trimestrielle	0 sans plan d'action	Nombre			
Nombre d'audits (internes/externes) réalisés sur la période	Annuelle	Selon plan d'audit validé	Nombre			
Taux de recommandations d'audit sécurité clôturées dans les délais	Trimestrielle	≥ 90 %	%			

7 Sensibilisation et culture sécurité

Indicateurs mesurant le niveau d'appropriation de la sécurité par les collaborateurs.

Indicateur	Fréquence	Cible de référence	Mode de calcul / unité	Valeur actuelle	Statut	Commentaire
Taux de collaborateurs ayant suivi une sensibilisation sur la période	Annuelle	≥ 90 %	%			

Indicateur	Fréquence	Cible de référence	Mode de calcul / unité	Valeur actuelle	Statut	Commentaire
Taux de clics lors des campagnes de simulation d'hameçonnage	Trimestrielle	En réduction continue	%			
Taux de signalement spontané d'emails suspects par les collaborateurs	Trimestrielle	En progression continue	%			
Nombre de campagnes de sensibilisation menées sur la période	Annuelle	Au moins 2 par an	Nombre			

8 Tiers et fournisseurs

Indicateurs mesurant la maîtrise du risque cyber lié à l'écosystème de partenaires et prestataires.

Indicateur	Fréquence	Cible de référence	Mode de calcul / unité	Valeur actuelle	Statut	Commentaire
Taux de fournisseurs critiques évalués sur le plan de la sécurité	Annuelle	100 %	%			
Nombre de fournisseurs critiques sans clause de sécurité contractuelle	Annuelle	0	Nombre			
Taux de fournisseurs critiques disposant d'un plan de continuité connu	Annuelle	≥ 90 %	%			

9 Ressources et budget

Indicateurs mesurant l'adéquation des moyens alloués à la fonction sécurité.

Indicateur	Fréquence	Cible de référence	Mode de calcul / unité	Valeur actuelle	Statut	Commentaire
Budget sécurité rapporté au budget informatique global	Annuelle	Benchmark sectoriel (à documenter)	%			
Taux d'exécution budgétaire du plan de sécurité	Trimestrielle	≥ 90 %	%			
Taux de postes sécurité pourvus vs. effectif cible	Semestrielle	≥ 90 %	%			
Nombre de jours de formation suivis par l'équipe sécurité	Annuelle	Selon plan de formation validé	Jours / personne			

Annexe 10 — Matrices RACI de la sécurité de l'information

DG : Direction générale · RSSI · DM : Directions métier · DSI · COL : Collaborateurs · PREST : Prestataires

Processus	Nature	DG	RSSI	DSI	DM	Audit interne	COL	PREST
Approbation de la stratégie de cybersécurité	Décision	A	R	C	C	I		
Approbation de la PSSI et des politiques thématiques	Décision	A	R	C	C	I	I	
Acceptation formelle d'un risque majeur	Décision	A	R	C	C	I		
Validation du budget de sécurité	Décision	A	R	C	C			
Qualification et classification d'un incident	Décision	I	A/R	C	I			
Décision de communication de crise	Décision	A/R	C		C			
Réalisation et actualisation de la cartographie des risques	Pilotage	I	A/R	C	R	I		
Définition des exigences de sécurité techniques	Pilotage	I	A/R	C	C			C
Sensibilisation et formation à la sécurité	Pilotage	I	A/R	C	C		R	
Intégration des exigences de sécurité dans les contrats fournisseurs	Pilotage	I	A	C	R			C
Pilotage opérationnel de la réponse à un incident majeur	Pilotage	A	R	R	C	I		C
Reporting sécurité au Comité de direction et au Conseil	Pilotage	I	A/R			I		
Mise en œuvre des mesures de sécurité techniques	Exécution	I	C	A/R	C			R
Gestion des demandes et attribution des accès	Exécution		C	R	A		I	
Signalement d'un incident suspecté	Exécution		A	R	I		R	R

Processus	Nature	DG	RSSI	DSI	DM	Audit interne	COL	PREST
Respect quotidien des règles de sécurité	Exécution	I	C	C	A		R	R
Respect des exigences de sécurité contractuelles	Exécution		C	I	I			A/R
Test du plan de continuité et de reprise d'activité	Exécution	I	A	R	C			C
Revue périodique des habilitations	Contrôle		A	C	R		I	
Contrôle de conformité du dispositif — deuxième ligne (revues, tests, vérifications)	Contrôle	I	A/R	C	C	I		C
Audit indépendant du dispositif de sécurité — troisième ligne	Contrôle	I	C	C	C	A/R		I

R	**Responsible**	Exécute — réalise concrètement l'activité
A	**Accountable**	Rend compte — valide en dernier ressort et porte la responsabilité du résultat (un seul A par ligne)
C	**Consulted**	Consulté — sollicité pour avis avant décision ou action
I	**Informed**	Informé — tenu au courant du résultat ou de la décision

Guide du Responsable de la sécurité des systèmes d'information (RSSI)

Gouvernance, responsabilités et pilotage de la cybersécurité dans les organisations

Suivez-nous sur nos canaux digitaux

@asinbenin