



DOCUMENT GRC COMPLET

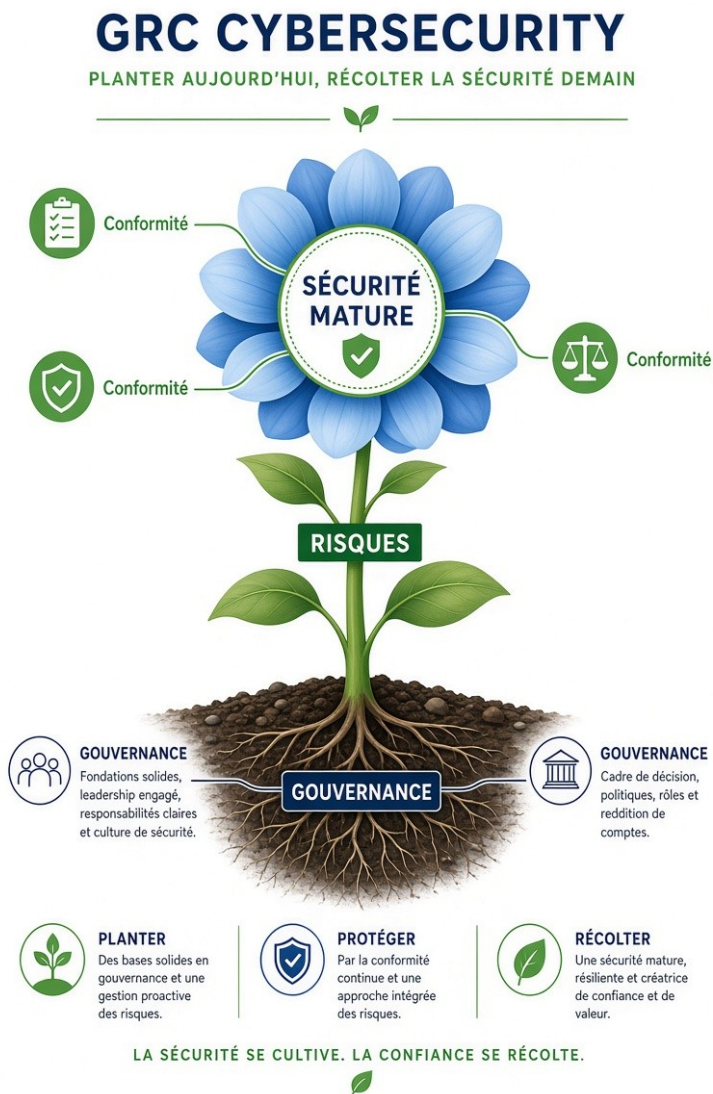
Gouvernance • Risques • Conformité

La sécurité qui se cultive et se récolte durablement

« Tu récoltes ce que tu sèmes »

Table des matières

01	Vision d'ensemble du GRC	2	05	Niveaux d'accompagnement GRC	7
02	Gouvernance SSI : Préparer le sol	4	06	Intégration GRC dans vos équipements	8
03	Gestion des Risques : Protéger la récolte	5	07	Offres modulaires	9
04	Conformité : Respecter les règles	6	08	Conclusion	10



Vision d'ensemble du GRC

Métaphore visuelle : La Fleur du GRC

Racines = Gouvernance • Tige = Risques • Pétales = Conformité • Fleur = Sécurité mature

Philosophie DIEUF-DIEUL Secure SN

Une sécurité durable commence par de petits gestes répétés avec constance. Comme une terre cultivée, un système d'information a besoin d'attention, de règles claires et d'entretien. Nous semons des pratiques simples, nous les cultivons avec les équipes et nous récoltons une protection durable.

Chez DIEUF-DIEUL Secure SN, nous croyons fermement que vous récoltez ce que vous semez. La cybersécurité n'est pas un produit : c'est une culture.

Nous semons les bonnes graines de sécurité (politiques, contrôles, sensibilisation) pour que nos clients récoltent une protection durable, une confiance renforcée et une conformité sereine.

Les 3 piliers interconnectés du GRC



Gouvernance

Préparer le sol et définir le cadre



Risques

Protéger la récolte contre les menaces



Conformité

Respecter les règles du village numérique

Approche par maturité

Les niveaux d'accompagnement sont déterminés après le questionnaire de maturité SSI. Selon le résultat, nous proposons :

Tàggat

Semer les premières graines

Jëf

Cultiver et renforcer

Bu Mat

Récolter une sécurité mature

Gouvernance SSI : Préparer le sol

Définition

La gouvernance SSI, c'est préparer le sol avant de semer. Elle pose les fondations : rôles, responsabilités, politiques et objectifs long terme. Sans un sol fertile, aucune graine de sécurité ne peut bien pousser.

Ce que nous définissons ensemble

Préparer le sol, c'est donner à chacun un rôle clair et une direction commune. Les responsabilités, les politiques et les décisions doivent rester compréhensibles et vivantes pour que la sécurité puisse réellement prendre racine dans l'organisation.

- Rôles et responsabilités (RACI)
- Politiques SSI et chartes d'usage
- Objectifs stratégiques de sécurité alignés sur le métier
- Cadre de décision et de reporting

Gouvernance SSI Préparer le sol



Gouvernance SSI

Définir la stratégie, les rôles et les responsabilités pour une cybersécurité durable.



Engagement
Des parties prenantes alignées



Politiques & Standards
Clairs, applicables et mesurables



Pilotage & Amélioration
Mesurer, suivre et s'adapter



Un sol fertile

Culture de sécurité, compétences, processus et technologies saines pour faire face aux menaces.



Culture & Sensibilisation



Compétences & Connaissances



Processus & Contrôles



Outils & Technologies



Racines solides

Confiance, résilience et anticipation prennent racine dans un sol bien préparé.



Dieuf-Dieul Secure

Sécuriser aujourd'hui, cultiver la confiance demain.



"tu récoltes ce que tu sèmes"

La sécurité est une culture, pas une clôture.



Gestion des Risques - Protéger la récolte



ANTICIPER • ÉVALUER • PROTÉGER • RÉCOLTER



IDENTIFIER LES RISQUES

Connaître les menaces
pour mieux les anticiper



METTRE EN PLACE DES BARRIÈRES

Contrôles, accès et solutions
de sécurité adaptées



DÉTECTER ET SURVEILLER

Surveillance continue
pour repérer tôt



RÉAGIR ET RENFORCER

Réponse rapide et amélioration
continue



DIEUF-DIEUL Secure

PHILOSOPHIE • PRÉVENTION • PATRIMOINE • PERPÉTUITÉ

Protéger aujourd'hui pour récolter demain.



Gestion des Risques : Protéger la récolte

Définition

La gestion des risques protège votre champ contre les menaces. Nous identifions, évaluons et traitons les risques pour que votre récolte (données, activité, réputation) reste en sécurité.

Menaces principales

Une menace ignorée peut devenir un risque qui se propage. Notre approche consiste à observer le terrain, reconnaître les signes de faiblesse et agir avant que la récolte — données, activité ou réputation — ne soit compromise.

- Ransomware et malwares
- Phishing et ingénierie sociale
- Fuite de données et violation de la vie privée
- DDoS et indisponibilité
- Menaces internes (insider threat)

Notre démarche

Protéger la récolte ne signifie pas supprimer tous les risques. Il s'agit de les connaître, de mesurer leurs conséquences et de réduire ceux qui peuvent réellement affecter l'organisation, avec des mesures proportionnées et suivies dans le temps.



Conformité : Respecter les règles

Définition

La conformité, c'est respecter les règles du village numérique. Elle transforme les exigences réglementaires en mesures concrètes et vérifiables, pour que la culture de la sécurité soit acceptée et durable.

Référentiels principaux

Les référentiels sont des repères pour cultiver une sécurité cohérente et vérifiable. Ils transforment les exigences en pratiques concrètes, adaptées au terrain et au niveau de maturité de chaque organisation.

- ISO 27001 / ISO 27005
- RGPD (pour les flux internationaux)
- Loi sénégalaise 2008-12 sur la protection des données personnelles
- Bonnes pratiques ANSSI, NIST CSF, COBIT

Conformité – Respecter les règles du village numérique

La cybersécurité, cultivée chaque jour,
protège notre village numérique.



✓ CHECKLIST – BONNES PRATIQUES

- ✓ Identités vérifiées et protégées
- ✓ Accès maîtrisé selon le principe du moindre privilège
- ✓ Données chiffrées et sauvegardées
- ✓ Sensibilisation et vigilance de tous les acteurs
- ✓ Incidents détectés, consignés et traités

LES RÈGLES DU VILLAGE NUMÉRIQUE



COMMUNAUTÉ
On se protège ensemble, on agit avec responsabilité.



ÉQUITÉ
Chaque acteur respecte les règles pour le bien collectif.



TRANSPARENCE
On agit avec clarté, on rend des comptes.



CONFIANCE
La confiance se cultive chaque jour, elle est notre bien commun.



PHILOSOPHIE DIEUF-DIEUL SECURE
“ tu récoltes ce que tu sèmes ”

Semons aujourd'hui les bonnes pratiques, pour récolter un village numérique sûr, résilient et durable.



Niveaux d'accompagnement GRC (Tàggat / Jëf / Bu Mat)

Important : Ces trois niveaux sont déterminés après le remplissage du questionnaire de maturité SSI. Le résultat du questionnaire permet de proposer l'accompagnement le plus adapté.

Niveau 1 – Tàggat

(Premiers Semis)

Tàggat, c'est semer l'essentiel. On commence par identifier les failles prioritaires et poser les premières protections afin de créer un terrain favorable à la suite du parcours.

Objectif : Identifier les failles essentielles et planter les premières graines de sécurité.

Métaphore : La graine.

- Diagnostic flash / analyse de risques légère
- Premières politiques et chartes
- Sensibilisation de base

Niveau 2 – Jëf

(Culture Sécuritaire)

Jëf, c'est cultiver la sécurité au quotidien. Les pratiques deviennent plus structurées, les utilisateurs prennent leur place et les protections gagnent en profondeur.

Objectif : Renforcer les protections, structurer les pratiques et cultiver la sécurité.

Métaphore : La jeune plante.

- Analyse de risques simplifiée
- Politiques SSI structurées
- Formation des utilisateurs et plan d'actions

Niveau 3 – Bu Mat

(Sécurité Durable)

Bu Mat, c'est récolter les fruits d'une culture de sécurité mature : une gouvernance solide, des risques mieux maîtrisés et une amélioration continue capable de s'adapter aux nouvelles menaces.

Objectif : Construire une gouvernance solide et récolter les bénéfices d'une sécurité mature.

Métaphore : La fleur mature.

- Analyse de risques approfondie
- PSSI complète + déclinaison des politiques de domaine
- Tableau de bord, suivi et amélioration continue

Intégration GRC dans vos équipements

Nous appliquons la même logique de maturité (Tàggat / Jëf / Bu Mat) directement sur les équipements que vous achetez ou que vous utilisez déjà. Le niveau est également guidé par le questionnaire de maturité.

● Niveau 1 – Tàggat

(Équipements)

Objectif : Mettre en place les premières protections essentielles.

- Chiffrement du disque
- Mots de passe forts + verrouillage automatique
- Mises à jour système automatiques

● Niveau 2 – Jëf

(Équipements)

Objectif : Renforcer la sécurité et structurer les usages.

- Sauvegarde chiffrée
- MFA (authentification multi-facteurs)
- Gestion des accès et formation des utilisateurs

● Niveau 3 – Bu Mat

(Équipements)

Objectif : Atteindre une sécurité mature, durable et supervisée.

- Audit de configuration
- Politique d'usage formalisée
- Supervision et plan de réponse aux incidents

Offres modulaires

Offre Gouvernance

Préparation du sol : politiques, rôles, chartes et cadre de décision.

Offre Risques

Protection de la récolte : analyse de risques, plan de traitement et suivi.

Offre Conformité

Respect des règles : cartographie des exigences, contrôles et preuves.

Offre GRC Complet

Une sécurité équilibrée ne repose pas sur un seul pilier. Comme une plante a besoin de racines, d'une tige et de feuilles, l'organisation doit relier gouvernance, risques et conformité pour faire grandir une protection cohérente.

Accompagnement intégré sur les trois piliers selon le niveau de maturité issu du questionnaire.

Offre Mix & Match

Chaque organisation possède son propre terrain. Nous adaptons donc l'accompagnement à votre contexte et à votre maturité, afin de semer les bonnes graines au bon moment, sans démarche inutilement lourde.

Composez votre accompagnement GRC selon vos besoins. DIEUF-DIEUL Secure SN assemble l'accompagnement selon votre contexte.

08 — CONCLUSION

La sécurité n'est pas une destination : c'est un chemin.

Tu ne récolteras pas seulement un outil.

Tu récolteras une compétence et une protection durable.

« *Tu récoltes ce que tu sèmes* »

DIEUF-DIEUL Secure SN

Semer les bonnes graines d'une sécurité numérique accessible et intelligible pour tous.

