

OPÉRATIONS • GOUVERNANCE • RISQUE • CONFORMITÉ

Nommé RSSI. Et maintenant ?

Vous maîtrisez l'infra, les systèmes, le réseau. Mais la **gouvernance**, l'**analyse de risques** et la **conformité** ? Vous avancez à l'aveugle — sans cadre, sans méthode, sans mode d'emploi.



LA SOLUTION

RSSI — Le Manuel de Terrain

De la sécurité opérationnelle au pilotage par les risques.

41
modules

Débutant →
Confirmé

Programme
complet

Télécharger le manuel



PRIX

5 990 F CFA

→ sqwwjzbu.mychariow.market

Ignace Yao Expert en cybersécurité · Auditeur des SI

ISO 27001 Lead Auditor · ISO 27005 Lead Implementer · Aspirant CISA

RSSI | Le Manuel de Terrain

De la sécurité opérationnelle au pilotage par les risques · Édition 2025

Le Livre Bleu de la cybersécurité est maintenant disponible !

Devenez le RSSI capable de **protéger votre entreprise**, **d'influencer les décideurs** et de **piloter les risques**.

La plupart des livres de cybersécurité vous expliquent ce qu'il faut **savoir**.
Celui-ci vous montre ce qu'il faut **faire**.

Que vous débutiez dans la cybersécurité, que vous preniez vos fonctions de RSSI ou que vous souhaitiez évoluer vers un poste de CISO, ce manuel vous accompagne à chaque étape de votre progression. Il transforme les référentiels, les méthodes et les bonnes pratiques en **décisions concrètes**, en **plans d'action** et en **résultats mesurables**.

Surnommé « **Le Livre Bleu de la cybersécurité** », cet ouvrage est conçu pour répondre à une réalité simple : le métier de RSSI ne consiste plus seulement à sécuriser des systèmes. Il faut désormais protéger les actifs critiques, maîtriser les risques, accompagner la transformation numérique, convaincre les dirigeants et créer de la confiance.

Ce manuel vous prépare à relever ces défis.

Plus de 700 pages, 41 modules et 1 000+ chapitres composent un parcours progressif qui vous permet de développer les compétences attendues d'un RSSI moderne. Pensé pour les **organisations africaines et francophones**, il s'appuie sur des situations opérationnelles, des méthodes directement applicables et une approche centrée sur le risque métier.

Ce que vous allez apprendre :

► Partie I — Construire des bases solides

MODULES 01 → 10 | DÉBUTANT · RECONVERSION

Avant de piloter la cybersécurité, il faut comprendre le système d'information.

Vous apprendrez à :

- Analyser un environnement informatique ;
- Classifier les actifs et les informations sensibles ;
- Sécuriser les postes de travail, les serveurs et les réseaux ;
- Mettre en œuvre IAM et PAM ;
- Réussir vos cent premiers jours dans une fonction RSSI.

À l'issue de cette première partie, vous disposerez des fondamentaux indispensables pour dialoguer avec les équipes techniques et prendre des décisions éclairées.

► Partie II — Maîtriser les opérations de cybersécurité

MODULES 11 → 26 | RSSI OPÉRATIONNEL

Une stratégie ne vaut que si elle résiste aux attaques.

Vous apprendrez à :

- Détecter les menaces et accélérer leur traitement grâce aux plateformes SIEM, SOAR, EDR/XDR et SOC ;
- Gérer les vulnérabilités avant qu'elles ne deviennent des incidents ;
- Organiser la réponse aux cyberattaques ;
- Intégrer la sécurité dans le Cloud, les projets DevSecOps et la Supply Chain ;
- Exploiter la Threat Intelligence ;
- Sécuriser les nouveaux usages de l'intelligence artificielle.

Vous développerez les réflexes opérationnels qui permettent de réduire l'exposition au risque tout en améliorant la résilience de l'entreprise.

► Partie III — Passer du RSSI au leader stratégique

MODULES 27 → 41 | RSSI SENIOR · CISO

La crédibilité d'un RSSI se mesure autant dans une salle serveur que dans une salle de conseil.

Cette dernière partie vous apprend à :

- Construire une gouvernance cyber durable ;
- Aligner les investissements sécurité sur les priorités métiers ;
- Mesurer la performance grâce à des indicateurs réellement utiles ;
- Produire des tableaux de bord destinés aux dirigeants ;
- Communiquer avec un COMEX ;
- Défendre un budget, justifier les investissements et transformer la cybersécurité en levier de création de valeur.

Vous développerez les compétences qui permettent à un responsable cybersécurité de devenir un véritable partenaire de la Direction Générale.

Ce manuel s'appuie sur les référentiels qui structurent aujourd'hui la cybersécurité :

ISO/IEC 27001:2022

NIST CSF 2.0

CIS Controls v8

MITRE ATT&CK

RGSSI 2025 (ANSSI-CI)

Mais connaître un référentiel ne suffit pas.

Vous apprendrez à l'interpréter, à l'adapter à votre organisation, à le traduire en **politiques, procédures, contrôles, tableaux de bord et plans d'action** capables de réduire concrètement le risque.

Parce qu'au final, une norme ne protège aucune entreprise. Ce sont **les décisions que vous prenez** et **les actions que vous déployez** qui font la différence.

Ce manuel a été écrit par un praticien.

Chaque chapitre s'appuie sur **plus de quinze années d'expérience** en audit des systèmes d'information, gouvernance, gestion des risques, conformité réglementaire et sécurité opérationnelle.

L'objectif n'est pas de vous transmettre des connaissances supplémentaires. C'est plutôt de vous donner les méthodes, les outils et les réflexes qui vous permettront d'exercer votre métier avec davantage d'**impact**, de **crédibilité** et de **confiance**.

Profitez de la période promotionnelle pour l'acheter à 5990F au lieu de 7990F !

Pour tout besoin d'information, merci de me contacter :

contact@ignaceyao.org

yaopointcom@gmail.com