

Afrique

ISO/IEC 27001 et la cybersécurité : Une approche unifiée de la sécurité de l'information et de la résilience

PECB REGIONAL WEBINARS

Agenda

1. Panorama de la cybersécurité en Afrique
2. ISO/IEC 27001 et ISO/IEC 27032 dans un contexte de cybermenaces croissantes
3. Convergence entre sécurité de l'information et cybersécurité
4. Stratégies pour bâtir une organisation résiliente & assurer la continuité des activités
5. Approche intégrée pour renforcer la résilience et assurer la continuité des activités
6. Matrice de correspondance (extrait opérationnel)
7. Résilience organisationnelle et opérationnelle dans la défense en profondeur (7 couches)
8. Bonnes pratiques issues des retours d'expérience et des audits

1. Panorama de la cybersécurité en Afrique

1

La menace cyber est plus présente que jamais en Afrique
Près de **50 %** des organisations africaines ont été victimes d'au moins une cyberattaque en 12 mois, avec un impact opérationnel grave dans **100 %** des cas signalés : interruptions d'activités, extorsions, atteinte à la réputation.

2

Les capacités de réponse aux incidents restent insuffisantes
62 % des organisations ne se sentent pas prêtes à gérer une cyberattaque de grande ampleur. Seules **28 %** ont mis en place un programme de cyber-résilience, et plus de la moitié n'ont pas de plan de continuité d'activité testé ou opérationnel.

3

Une pénurie alarmante de talents en cybersécurité
70 % des répondants constatent une pénurie de profils spécialisés en SSI, limitant leur capacité à faire face aux menaces. Le besoin le plus exprimé concerne la gestion des risques et la réponse aux incidents.

4

L'investissement reste faible malgré la prise de conscience
44 % des répondants consacrent moins de **5 %** de leur budget SI à la cybersécurité, bien en dessous des moyennes mondiales. Pourtant, **74 %** prévoient d'acquérir de nouvelles solutions de protection, montrant une volonté de progresser malgré des moyens encore limités.

Source: Baromètre de la cybersécurité en Afrique 2025 5ème édition réalisé par le Club D'experts De La Sécurité De L'information en Afrique (CESIA)

2. ISO/IEC 27001 et ISO/IEC 27032 dans un contexte de cybermenaces croissantes

ISO/IEC 27001 – Pilier de la sécurité de l'information

Objectifs fondamentaux	Piliers et contrôles de sécurité	Amélioration continue et conformité
• Assure la confidentialité, l'intégrité et la disponibilité de l'information sous toutes ses formes au sein des organisations avec une approche basée sur les risques.	• Comprend la définition de la politique de sécurité, l'analyse des risques et les contrôles organisationnels, technologiques, humains et physiques pour réduire les risques.	• Suit le cycle PDCA pour s'améliorer continuellement et assurer la conformité aux exigences légales, réglementaires, contractuelles et normatives en matière de sécurité de l'information.

2. ISO/IEC 27001 et ISO/IEC 27032 dans un contexte de cybermenaces croissantes

ISO/IEC 27032 – La cybersécurité en complément

Complément à la norme ISO/IEC 27001	Collaboration avec les parties prenantes et réponse aux incidents	Couverture des cyber-risques
• complète l'ISO/IEC 27001 en se concentrant spécifiquement sur la protection de l'information numérique contre les cybermenaces.	• met l'accent sur la collaboration, la gestion des vulnérabilités et la réponse aux incidents entre les parties prenantes.	• couvrent les risques opérationnels afin d'améliorer la protection des actifs numériques.

2. ISO/IEC 27001 et ISO/IEC 27032 dans un contexte de cybermenaces croissantes

ISO/IEC 27032 – La cybersécurité en complément

Leadership & gouvernance	Planification basée sur le risque	Support
• Politique sécurité, rôles/responsabilités, alignement stratégique, ressources • **Clauses** : 5.1–5.3 (leadership, politique, rôles)	• identification des risques/opportunités, objectifs sécurité, plans pour les atteindre. • **Clauses** : 6.1 (actions face aux risques/opportunités), 6.2 (objectifs), 6.3 (changements). **Annexe A** pour le traitement des risques (SoA)	• couvrent les risques opérationnels afin d'améliorer la protection des actifs numériques. • compétences, sensibilisation, communication, maîtrise documentaire. **Clauses** : 7.1–7.5

3. Convergence sécurité de l’information & cybersécurité

1. **Approche de sécurité unifiée**
   L’intégration des pratiques de cybersécurité dans la sécurité de l’information fournit une base solide de gouvernance et de conformité technique.

2. **Contrôles de sécurité améliorés**
   Les contrôles ISO/IEC 27001 sont améliorés par la détection des incidents, les outils de réponse, la continuité des activités, le cryptage et les méthodes d’authentification forte.

3. **Alignement des normes**
   L’alignement de l’ISO/IEC 27001 sur les normes ISO/IEC 27032, NIST CSF et CIS Controls renforce la synergie en matière de cybersécurité et la gestion des risques liés à la sécurité de l’information.

4. **Stratégie de sécurité complète**
   La combinaison de la gestion des risques, des contrôles techniques et de la sensibilisation des utilisateurs permet d’atteindre des niveaux de sécurité et de résilience optimaux.

4. Stratégies pour bâtir une organisation résiliente

1. **Leadership et engagement**
   Un leadership fort favorise une culture de sécurité positive et mobilise des ressources pour la résilience.

2. **Développement de la culture de sécurité**
   La sensibilisation et la formation continues favorisent la culture de la sécurité à tous les niveaux de l'organisation.

3. **Gestion proactive des risques**
   Il est essentiel d'identifier et de traiter rapidement les menaces à l'aide d'outils et de processus robustes.

4. **Continuité des activités et collaboration**
   La préparation de plans d'intervention en cas de crise et la coopération avec les partenaires assurent une gestion efficace des incidents.

5. Approche intégrée pour renforcer la résilience et assurer la continuité des activités

1

Résilience au-delà de la sécurité

L'objectif n'est pas seulement d'éviter les attaques, mais de garantir la survie et la continuité de l'organisation.
ISO/IEC 27001 intègre la préparation à l'incident, la réponse et la reprise

2

Continuité et reprise d'activité

PCA (Plan de Continuité d'Activité) : maintien des processus essentiels en cas de perturbation.
PRA (Plan de Reprise après Sinistre) : restauration des systèmes critiques dans un délai défini.
Intégration avec **tests de crise**, exercices réguliers, mises à jour des plans.

3

Les bénéfices concrets pour l'organisation

Réduction des interruptions de service : limitation des pertes financières et opérationnelles.
Réputation protégée : communication maîtrisée avec clients, partenaires, autorités.
Conformité réglementaire : anticipation des exigences de plus en plus strictes (ex. NIS2 obligeant la résilience des opérateurs essentiels).

4

Une approche holistique

Gouvernance : cadre ISO/IEC 27001 qui aligne sécurité et stratégie.
Cybersécurité : technologies défensives, surveillance, réponse.
Culture sécurité : collaborateurs formés comme première ligne de défense.
Gestion de crise : coordination, communication interne/externe, post-mortem

5. Approche intégrée pour renforcer la résilience et assurer la continuité des activités

NIST CSF – Chaîne complète prévention→détection→réponse→reprise

Prévention (PR)	Détection (DE)	Réponse (RS)	Reprise (RC)
• Contrôle d'accès, MFA, durcissement, sauvegardes, segmentation (Annexe A : A.8.*).	• Journalisation, use cases SOC corrélés aux tactiques ATT&CK (A.8.16 Journaux, A.8.17 Surveillance). MITRE ATT&CK	• Plan de réponse aux incidents, gestion de crise, communication (A.5.24 préparation à la gestion des incidents, A.5.25 réponse, A.5.26 apprentissage post-incident).	• PCA/PRA, tests de restauration (A.5.30 continuité, A.5.31 exigences de continuité, A.5.32 planification de la continuité)

Gouvernance & amélioration continue

La boucle PDCA (9.x audits/revue, 10.x amélioration) + NIST CSF 2.0 "GOVERN" pour ancrer le cyber au niveau stratégique (appétence au risque, rôles, politiques, supply-chain).

6. Matrice de correspondance (extrait opérationnel)

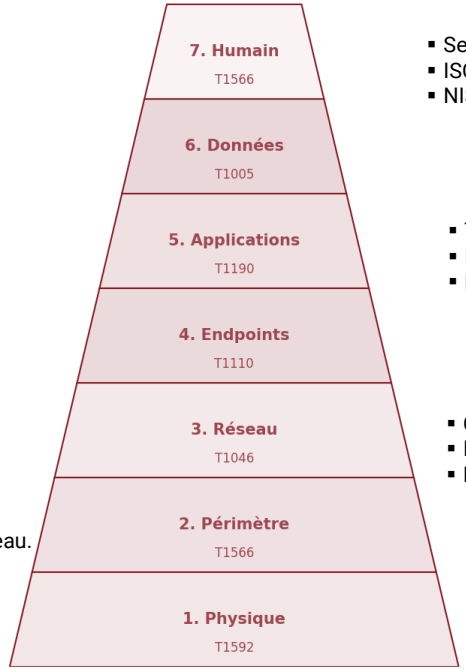
Attention : les mappings sont “meilleurs efforts” et non 1-pour-1. Ils aident à aligner vos politiques/contrôles, vos scénarios de détection et vos playbooks

Thème / Clause ISO 27001:2022	Exemples d’Annexe A	NIST CSF 2.0	CIS v8 (sélection)	MITRE ATT&CK – Tactiques principalement visées
Gouvernance & politique (5.x; 6.x; 7.x; 9–10)	A.5.1 Politique sécu, A.5.2 Rôles, A.5.20 Stratégie cloud, A.5.29 Fournisseurs	GV, ID	17 (Programme de sécurité), 15 (Contrôles fournisseurs)	Cadre global (toutes tactiques) pour orienter détection & réponse. (Publications NIST, CIS)
Gestion des actifs & classification (6.1; 8.2–8.3)	A.5.9 Gestion identités; A.5.23 Classification ; A.8.12 DLP	ID.AM, ID.IM	1 (Assets), 2 (Logiciels), 3 (Data Protection)	Collection, Exfiltration, Impact. (Publications NIST, CIS, MITRE ATT&CK)
Contrôle d’accès & IAM	A.8.2 Gestion identités, A.8.3 Authentification, A.8.4 Gestion des infos d’auth.	PR.AC	6 (Access Control), 5 (Account Management)	Initial Access, Privilege Escalation, Defense Evasion, Credential Access. (Publications NIST, CIS, MITRE ATT&CK)
Sécurité poste/serveurs & configuration	A.8.9 Configurations, A.8.10 Durcissement, A.8.11 Patch mgmt	PR.PS, PR.MA	4 (Configurations sécurisées), 7 (Vuln. Mgmt)	Execution, Persistence, Privilege Escalation. (Publications NIST, CIS)
Journalisation, surveillance & détection	A.8.16 Journaux, A.8.17 Surveillance, A.8.18 Détection	DE.AE, DE.DP	8 (Audit Log Mgmt), 13 (Network Monitoring & Defense)	Discovery, Lateral Movement, Command & Control. (Publications NIST, CIS, MITRE ATT&CK)
Protection réseau & segmentation	A.8.19 Sécurité réseau, A.8.20 Segmentation	PR.PT	12 (Network Infrastructure Mgmt), 13	Initial Access, Lateral Movement, C2. (Publications NIST, CIS)
Chiffrement & protection des données	A.8.24 Chiffrement, A.8.21 Sécurité des services web	PR.DS	3 (Data Protection)	Exfiltration, Impact (ransomware). (Publications NIST, CIS)
Gestion des vulnérabilités	A.8.8 Gestion des vulnérabilités	ID.RA, PR.IP	7 (Vulnerability Mgmt), 16 (Application Software Security)	Exploitation (Execution, PrivEsc). (Publications NIST, CIS)
Sécurité du cycle de vie logiciel	A.8.25 Dev sécurisé, A.8.27 CICD	PR.IP	16 (App Security)	Execution, Defense Evasion. (Publications NIST, CIS)
Fournisseurs & cloud	A.5.29–A.5.30 Tiers/continuité fournisseurs; A.5.20 Cloud	GV.SC, ID.SC	15 (Service Provider Mgmt)	Initial Access via supply chain. (Publications NIST, CIS)
Réponse aux incidents	A.5.24–A.5.26 (préparation, réponse, leçons tirées)	RS	17.8 (IR dans le programme), 11 (Data Recovery) (parties liées)	Toutes tactiques lors de la phase IR. (Publications NIST, CIS)
Continuité & reprise	A.5.30–A.5.32 (continuité IS), tests & restauration	RC	11 (Data Recovery), 14 (Security Awareness soutient la résilience)	Impact (atténuation), Rétablissement post-attaque. (Publications NIST, CIS)
Sensibilisation & RH	A.6.3 Sensibilisation, A.6.1 Process RH	GV.OV, PR.AT	14 (Security Awareness & Skills Training)	Social Engineering (Initial Access). (Publications NIST, CIS)
Sécurité physique	A.7.x Contrôles physiques & environnementaux	PR.PH	14/12 selon périmètres	Initial Access (physique), Impact. (Publications NIST)

7. Résilience organisationnelle et opérationnelle dans la défense en profondeur (7 couches)

La défense en profondeur repose sur l'idée qu'aucune mesure de sécurité unique n'est suffisante. Il faut superposer plusieurs couches de protection: techniques, organisationnelles et humaines, afin de rendre une attaque beaucoup plus difficile.

Pyramide 7 couches



- Sensibilisation, formation, gestion des rôles et responsabilités.
- ISO 27001 : leadership, culture sécurité, PCA.
- NIST CSF : Govern et Respond.

- Chiffrement, sauvegardes, classification des données.
- ISO 27001 : confidentialité, intégrité, disponibilité.
- NIST CSF : Protect et Recover.

- Tests d'intrusion, patching, contrôle du cycle de vie logiciel.
- ISO 27001 : maîtrise des vulnérabilités.
- NIST CSF : Protect et Detect.

- Antivirus, EDR, mises à jour, durcissement des postes.
- ISO 27001 : gestion des actifs, politiques d'usage.
- NIST CSF : Protect et Respond.

- Chiffrement, VLAN, monitoring réseau.
- ISO 27001 : identification des risques de communication.
- NIST CSF : Detect et Protect.

- Pare-feux, IDS/IPS, segmentation réseau.
- ISO 27001 : définition des politiques d'accès et règles réseau.
- NIST CSF : Protect (contrôles réseau).

- Contrôle d'accès aux locaux, surveillance, badges, zones sécurisées
- Lien ISO 27001 : gestion des accès physiques, plans de continuité.
- Lien NIST CSF : Protect (contrôles physiques et environnementaux

8. Bonnes pratiques de gouvernance et opérations (3 recommandations actionnables)

Aligner l’analyse de risque ISO 27001 avec les cas d’usage MITRE	Intégrer NIST CSF dans les procédures opérationnelles	Mettre en place un programme continu de threat hunting & red-team
Lorsque l’analyse identifie un risque élevé (ex. exfiltration de données), mappez-le aux tactiques/techniques MITRE pertinentes pour prioriser les contrôles techniques (journaux, DLP, sauvegardes chiffrées).	Pour chaque objectif ISO (ex. disponibilité d’un service), définir les mesures NISTCSF (Protect → Detect → Respond → Recover) et tests associés (table-top, exercices PRA).	Basé sur MITRE ATT&CK pour tester la robustesse des 7 couches et remonter les gaps à la gouvernance (comité SMSI).

Session de Questions & Réponses



Contact

- Website : www.nktek-holding.com
- Phone : +225 07 57 5039 08
- Email : nicaisekouame@nktek-holding.com

- Website : https://secfonops.fr
- Phone : 06 05 75 22 05
- Email : rodrigue.nsuka@secfonops.fr

Pour toute question ou commentaire, vous pouvez nous contacter ci-dessous :

- support@pecb.com