ANSSI
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
CÔTE D'IVOIRE

CYBEREX 2026

TERMES DE RÉFÉRENCE (TDR)

1ère édition CYBEREX 2026

Premier exercice national de simulation de crise cyber

28 et 29 octobre 2026

Radisson Blu, Abidjan

SOMMAIRE

1. CONTEXTE ET JUSTIFICATION

L'accélération de la transformation numérique en Côte d'Ivoire expose désormais les administrations, les entreprises et les citoyens à des cybermenaces de plus en plus fréquentes, sophistiquées et coûteuses. La résilience numérique n'est plus un simple enjeu technique : elle constitue une condition de souveraineté nationale, de continuité économique et de confiance des usagers.

Face à ce constat, **l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI)** initie la **1ère édition du CYBEREX 2026**, premier exercice national de simulation de crise cyber, destiné à renforcer la préparation, la coordination et la résilience des acteurs publics et privés face aux cybermenaces, sous le thème : **« Résilience numérique nationale : Anticiper, réagir, rebondir ensemble pour garantir la sécurité des infrastructures critiques»**.

À travers des scénarios réalistes inspirés des meilleures pratiques internationales, cette première édition met l'accent sur trois secteurs stratégiques que sont **l'énergie, les technologies de l'information et de la communication (TIC) et les finances** afin de tester les capacités de détection, de réponse, de gestion de crise et de continuité des activités, tout en consolidant la coopération entre les parties prenantes de l'écosystème national de cybersécurité.

Le présent document constitue les **Termes De Référence de cette 1ère édition**. Il en précise le contexte, les objectifs, le public visé, le contenu, l'organisation, le plan de communication, le budget prévisionnel ainsi que le calendrier de mise en œuvre. Il propose également une thématique fédératrice destinée à porter l'identité de l'événement.

2. OBJET DE L'ÉVÈNEMENT

CYBEREX 2026 est le premier exercice national de simulation de crise cyber, organisé par l'ANSSI. Deux jours durant, il réunit décideurs, responsables métiers, experts techniques, étudiants et acteurs de l'écosystème numérique ivoirien autour d'un programme immersif et opérationnel.

Cette première édition cible trois secteurs stratégiques : l'énergie, les technologies de l'information et de la communication (TIC) et la finance pour éprouver, en conditions réalistes, les capacités nationales de détection, de réponse, de gestion de crise et de continuité d'activité.

Il ne s'agit pas d'une conférence de plus : c'est un espace rare où les dirigeants vivent une cyberattaque de l'intérieur, où les experts éprouvent leurs réflexes en conditions réelles et où les jeunes talents se révèlent. Un véritable rendez-vous de transformation collective.

Cette édition fondatrice du CYBEREX 2026 a vocation à devenir le rendez-vous national de référence de la cybersécurité opérationnelle et de la résilience numérique, appelé à rayonner à l'échelle sous-régionale.

- **Thématique proposée pour la 1ère édition :**

Résilience numérique nationale : Anticiper, réagir, rebondir ensemble pour garantir la sécurité des infrastructures critiques.

- **Justification**

Cette thématique reprend les trois piliers énoncés dans le contexte de l'événement : la souveraineté nationale, la continuité économique et la confiance des usagers. Elle place la résilience, plutôt que la seule dimension technique au centre du discours. Ce choix permet de parler à la fois aux décideurs (enjeu de gouvernance et de souveraineté), aux experts techniques (enjeu opérationnel de détection et de réponse) et au grand public notamment les étudiants (enjeu de confiance et de mobilisation collective).

Le triptyque « Anticiper, réagir, rebondir ensemble. » traduit fidèlement, sous une forme mémorisable et facilement déclinable en signature visuelle, les trois (03) capacités testées pendant l'exercice (détection, réponse, gestion de crise et continuité d'activité).

Le mot « ensemble » rappelle que les trois secteurs stratégiques ciblés (énergie, TIC, finance) ainsi que les acteurs publics et privés ne peuvent atteindre une résilience réelle que de manière collective et coordonnée. Ce message est cohérent avec l'objectif de renforcement de la coordination inter-organisationnelle poursuivi par l'Objectif stratégique 2 « Protéger le cyberespace » de la stratégie Nationale de Cybersécurité.

3. OBJECTIFS

- **Objectif général**

Renforcer la résilience cyber nationale en faisant vivre aux acteurs publics et privés une crise cyber réaliste, dans un cadre coordonné et mesurable.

- **Objectifs spécifiques**
  - Faire vivre aux décideurs publics et privés une crise cyber réaliste, pour transformer leur perception du risque en réflexe de décision ;
  - Éprouver les capacités de détection, de réponse, de gestion de crise et de continuité d'activité à travers des scénarios de simulation en conditions réelles ;
  - Donner à voir, par la démonstration, les menaces d'aujourd'hui et les solutions concrètes pour s'en protéger ;
  - Repérer, valoriser et fédérer les talents nationaux de la cybersécurité, de l'étudiant au professionnel confirmé ;

- Renforcer la coordination entre les acteurs des secteurs stratégiques et l'ensemble de l'écosystème cybersécurité.

4. RÉSULTATS ATTENDUS

À l'issue des deux journées d'exercice, les résultats concrets et mesurables suivants sont attendus :

- Renforcer la préparation nationale face aux cyberattaques affectant les secteurs critiques ciblé pour cette édition (Energie, TIC et Finances).
- Tester l'efficacité des dispositifs de gestion de crise cyber des organisations participantes, notamment leurs capacités de détection, d'analyse, de décision, de réponse et de reprise d'activité.
- Évaluer les mécanismes de coordination entre l'ANSSI, les administrations, les opérateurs d'infrastructures critiques, les entreprises et les autres acteurs de l'écosystème.

5. PUBLIC CIBLE ET ACTEURS CONCERNÉS

- Profils de participants

CYBEREX 2026 s'adresse à trois grandes familles de profils :

DÉCIDEURS	EXPERTS TECHNIQUES	ENSEIGNEMENT SUPÉRIEUR
• PCA & membres de COMEX • DG & DGA • Responsables Risques & Conformité	• RSSI & DSI • Équipes SOC & experts cyber • Consultants sécurité & Auditeurs • Analystes & ingénieurs SI	• ESATIC, INP-HB • Universités & Grandes Écoles • Centres de formation spécialisés • Étudiants en informatique & SSI

Cette première édition cible prioritairement les opérateurs de l'Énergie, des TIC et de la Finance, au sein d'une audience nationale élargie, répartie entre secteur public et secteur privé :

Secteur public

- Ministères et Institutions publiques
- Collectivités territoriales et services déconcentrés de l'État
- Sociétés d'État et établissements publics à caractère stratégique

Secteur privé

- Établissements bancaires et financiers
- Opérateurs de télécommunications (TIC)
- Acteurs du secteur de l'énergie
- Compagnies d'assurance, industrie, PME et grandes entreprises

Acteurs ciblés pour l'édition 2026

CYBEREX 2026 est destiné à l'ensemble des secteurs d'activités du pays, avec une priorité accordée aux acteurs des secteurs stratégiques de l'Énergie, des TIC et de la Finance. Le tableau suivant recense les principales organisations choisies pour participer aux exercices cyber.

ÉNERGIE	TIC	FINANCE
– Autorité Nationale de Régulation du Secteur de l'électricité de Côte d'Ivoire (ANARE-CI) – Compagnie Ivoirienne d'Électricité (CIE) – Côte d'Ivoire Énergie (CI-ENERGIE) – FOXTROT International – Société de Gestion des Stocks Pétroliers de Côte d'Ivoire (GESTOCI) – Société Ivoirienne de Raffinage (SIR) – Compagnie Ivoirienne de Production d'Électricité (CIPREL)	– Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI) – Orange CI – MTN CI – Moov Africa – MainOne Solutions by Equinix – KAYDAN Technologie – VIP NET	– Ministère de l'Économie, des Finances et du Budget – Banque Centrale des États d'Afrique de l'Ouest (BCEAO) – Direction Générale des Impôts (DGI) – Direction Générale des Douanes de Côte d'Ivoire – Direction Générale du Trésor Public et de la Comptabilité publique – Banque Nationale d'Investissements (BNI) – Djamo Côte d'Ivoire – Wave Côte d'Ivoire – Push CI

6. FORMAT DE L'ÉVÈNEMENT

Dates	28 et 29 octobre 2026
Lieu	Radisson Blu, Abidjan
Format	Présentiel 2 jours
Participants attendus	800 participants
Cibles principales	Décideurs (PCA, DG, DGA, DAF, DAJC), Experts Techniques (RSSI, DSI, SOC, CERT, équipe IT), Étudiants

7. AXES D'ANIMATION

Le programme de CYBEREX 2026 s'articule autour de sept axes d'animation complémentaires, combinant simulation de crise, démonstrations techniques, montée en compétences et valorisation des talents.

- **Axe 1 : Cyber Crise Exécutive**

Simulation immersive de gestion de crise cyber destinée aux dirigeants. Dans un environnement reconstitué, ils prennent sous pression des décisions critiques face à une cyberattaque majeure visant leurs organisations.

Participants cibles : PCA, DG, DAF, DAJC, DRH, DIRCOM

Objectif : Faire vivre aux décideurs une crise cyber de l'intérieur, pour qu'ils comprennent les enjeux et l'importance de leur capacité à prendre les décisions pour limiter les impacts sur l'organisation.

- **Axe 2 : Cyber Drill**

Exercice national de simulation d'incident cyber multi-organisations. Administrations, banques, opérateurs télécoms et énergéticiens collaborent sur un scénario coordonné touchant les secteurs de l'Énergie, des TIC et de la Finance.

Participants cibles : RSSI, DSI, équipes SOC, auditeurs cybersécurité, consultants sécurité, analystes cybersécurité, ingénieurs systèmes et réseaux.

Objectif : Tester et renforcer les mécanismes de coordination intra-organisationnelle et les réflexes de réponse à incident à l'échelle nationale.

- **Axe 3 : Audit express & Durcissement d’un système critique**

Exercice pratique de cybersécurité permettant aux participants d'évaluer, dans un temps limité, le niveau de sécurité d'un système d'information représentatif d'une infrastructure critique. À travers une démarche méthodique d'audit technique, ils identifient les vulnérabilités, évaluent leur criticité et mettent en œuvre les principales mesures de durcissement afin de réduire la surface d'attaque et d'améliorer la résilience du système.

Participants cibles : RSSI, équipes SOC, auditeurs cybersécurité, consultants sécurité, analystes cybersécurité, ingénieurs systèmes et réseaux, DSI.

Objectif : Développer les compétences opérationnelles des experts en matière d'audit de sécurité, de réduction de la surface d'attaque et de sécurisation des systèmes critiques, conformément aux bonnes pratiques et aux standards nationaux internationaux de cybersécurité.

Axe 4 : MasterClass Environnement institutionnel et juridique de la Côte d'Ivoire

Session consacrée à la compréhension de l'architecture nationale de cybersécurité, du cadre juridique applicable et de la gouvernance institutionnelle en Côte d'Ivoire. À travers des présentations interactives et des échanges d'expérience, les participants appréhendent les responsabilités des principaux acteurs, les mécanismes de coordination et les fondements légaux de la prévention, de la gestion et de la réponse aux incidents cyber.

Participants cibles : Universités & Grandes Écoles, Centres de formation spécialisés, Étudiants en informatique & SSI.

Objectif : Susciter des vocations, renforcer la culture cyber des étudiants et leur donner les clés de compréhension des enjeux institutionnels, juridiques et opérationnels de la cybersécurité en Côte d'Ivoire.

- **Axe 5 : Cyber Village**

Espace d'exposition dédié aux solutions de cybersécurité, aux innovations locales, aux services de l'ANSSI et aux démonstrations technologiques des partenaires de l'écosystème.

Participants cibles : Partenaires, exposants, porteurs de solutions et visiteurs professionnels.

Objectif : Créer un espace de rencontres techniques, de découverte et de business entre les acteurs de l'offre et de la demande en cybersécurité.

- **Axe 6 : Épreuves Capture The Flag (CTF)**

Compétition technique de cybersécurité destinée à évaluer les connaissances et les aptitudes opérationnelles des participants au travers de défis progressifs inspirés de situations réelles. Les équipes s'affrontent sur des épreuves de **Capture The Flag (CTF)** couvrant l'investigation numérique, l'OSINT, la cryptographie, l'exploitation de vulnérabilités, la sécurité des réseaux, des systèmes et des applications.

Participants cibles : Étudiants, élèves-ingénieurs, jeunes professionnels, universités, grandes écoles, centres de formation et communautés cyber.

Objectif : Promouvoir l'excellence technique, renforcer les compétences pratiques en cybersécurité, détecter les talents émergents et contribuer à la constitution d'un vivier national d'experts capables de répondre aux enjeux de souveraineté numérique et de résilience cyber de la Côte d'Ivoire.

- **Axe 7 : Cyber RETEX**

Sessions de retour d'expérience (RETEX) au cours desquelles des organisations ayant traversé un incident cyber majeur partagent, sans tabou, le déroulé de la crise, les décisions prises et les enseignements tirés. Des témoignages concrets d'acteurs publics et privés ayant résisté à une crise majeure.

Participants cibles : PCA, DG, DAF, RSSI , DSI ,DAJC, DRH, DIRCOM en séance restreinte.

Objectif : Apprendre du vécu réel plutôt que de la théorie : diffuser les bonnes pratiques, dédramatiser la parole autour des incidents et renforcer la préparation collective grâce aux leçons apprises.

8. PROGRAMME PRÉVISIONNEL

- **Jour 1 : 28/10/2026**

Horaire	Activité	Profil
08h00 – 08h45	Accueil & enregistrement des participants	
08h45 – 09h30	Cérémonie officielle d'ouverture et Allocutions institutionnelles	Officiels
09h30 – 09h45	Keynote d'ouverture : « L'état de la menace cyber en Côte d'Ivoire : Bilan et perspectives »	DG
09h45– 10h15	Visite des officiels du Cyber Village et Pause-café	
10h15 – 12h00 (simultanée)	Cyber Crise Executive : Simulation de gestion de crise pour dirigeants : attaque par rançongiciel (Salle 01)	Décideurs
	Cyber Drill (Salle 02)	Experts
	MasterClass : environnement institutionnel et juridique de la CI (Salle 03)	Étudiants
12h00 – 14h00	Déjeuner	
14h00 – 16h30	Audit express & durcissement d'un système critique (Salle 02)	Experts
	Lancement du CTF (Capture The Flag) (Salle 03)	Etudiants
16h30 – 16h45	Pause-café	
16h45 – 20h00	CTF (Capture The Flag) (Salle 03)	Etudiants

- **Jour 2 : 29/10/2026**

Horaire	Activité	Profil
08h00 – 09h00	Accueil & enregistrement des participants	
09h00– 10h15	Cyber RETEX	Décideurs
10h15 – 10h30	Pause-café & networking	
10h30 – 12h30	Formation RSSI (Salle 01 et Salle 02)	RSSI & DSI
	CTF (Capture The Flag) (Salle 03) (suite)	Etudiants
11h30 – 12h30	Visite du Cyber Solutions Village	
12h30 – 14h00	Déjeuner	
14h00 – 16h30	Formation RSSI	RSSI & DSI
16h30 – 16h35	Clôture du CTF (Capture The Flag) (Salle 03)	Etudiants
16h35 – 17h30	Cérémonie de clôture et distinction	Tout public
17h30 – 19h00	Networking & cocktail de fin	Tout public

9. DISTINCTIONS ET PRIX

Parce que la cybersécurité est d'abord une affaire d'hommes et de femmes, CYBEREX 2026 célèbre l'excellence à travers cinq distinctions officielles, remises lors de la cérémonie de clôture, en présence des plus hautes autorités de l'État.

Prix	Description
Prix de la Résilience Numérique	Récompense l'organisation la plus exemplaire en matière de préparation et de gestion des cybermenaces.
Meilleure Équipe Cyber Défis CTF	Couronne l'équipe victorieuse du Cyber Défis CTF
Prix Innovation Cybersécurité	Valorise la solution ou l'approche la plus innovante présentée au Cyber Solutions Village.
Prix Partenaire Cyber 2026	Reconnaît la contribution exceptionnelle d'un partenaire à l'écosystème cyber national.

10. CONCLUSION

CYBEREX 2026 représente une étape fondatrice pour l'écosystème national de cybersécurité. En réunissant sur deux journées décideurs, experts techniques et jeunes talents autour d'une thématique fédératrice **« Résilience numérique nationale : Cybermenaces Anticiper, réagir, rebondir ensemble»** , cette 1ère édition doit poser les bases d'un rendez-vous annuel de référence, capable de rayonner au-delà des frontières nationales.