Cybersécurité

Renforcement du dispositif de maîtrise des risques informatiques des établissements de crédit et de microfinance en zone CEMAC

Notre offre

pwc

Le contexte

Par une lettre circulaire, LC-COB/04 du 21 janvier 2022, avec en objet le «renforcement du dispositif de maîtrise des risques informatiques notamment la sécurité des systèmes d'information et la cybersécurité », le Secrétaire général de la Commission bancaire d'Afrique Centrale (COBAC) «incite fortement » établissement de crédit, de microfinance et de paiement de la zone CEMAC à faire auditer, au plus tard le 30 juin 2022, leur système d'information par des experts indépendants de la sécurité et/ou de l'audit informatiques afin d'en établir un diagnostic approfondi retraçant les points de vulnérabilité. Les résultats des audits effectués devront lui être adressés au plus tard, le 15 juillet 2022 accompagnés des mesures de rémédiation prises par les établissements de crédit, de microfinance et de paiement. A défaut, ces derniers s'exposent aux sanctions prévues par la réglementation en vigueur.

Par la même correspondance, il recommande, en plus, la mise en place d'un dispositif spécifique de lutte contre la fraude, de procéder à une identification et à une évaluation adéquate des risques opérationnels auxquels les établissements sont exposés notamment en ce qui concerne les cyberattaques. L'objectif recherché étant, d'une part, de les prévenir, et d'autre part de renforcer la capacité des établissements de crédit et de microfinance à assurer la continuité de leurs activités en cas d'incident majeur. Dans cette perspective, la mise en place de mesures de détection des opérations non autorisées, de réponse aux attaques et de rétablissement du fonctionnement des systèmes d'information occupent une place centrale.

Autre demande contenue dans la lettre-circulaire, c'est l'invitation faite aux établissements de crédit et de microfinance de se doter d'une politique de sécurité informatique en phase avec les bonnes pratiques et les standards internationaux en la matière, notamment les normes ISO/CEI 27001-02, la norme de sécurité de l'industrie des cartes de paiement (Payment Card Industry Data Security Standard, PCI-DSS).

Ces demandes font suite à un constat qui découle de l'impact de la crise sanitaire de Covid-19 sur le secteur financier qui, du fait des restrictions observées dans les déplacements et les mesures de distanciation, a conduit les établissement de crédit et de microfinance à accélérer leur plan de transformation digitale en ligne avec le règlement n°04/18/CEMAC/UMAC/COBAC relatif aux services de paiement dans la CEMAC, et d'autre part pour mieux répondre à l'évolution des attentes du marché.
Toutefois, bien que ces évolutions technologiques et les dispositions réglementaires mise en place par la COBAC permettent de réduire certains risques opérationnels, notamment les risques d'erreurs d'exécution, l'expansion des réseaux et des technologies, l'ouverture des systèmes d'information aux échanges extérieurs et la croissance des transactions électroniques, contribuent à accroître de façon substantielle les risques liés à la cybercriminalité.

Cette ouverture expose de façon importante les établissements de crédit et de microfinance du fait du développement soutenu de la dématérialisation de leurs produits et services bancaires qu'ils rendent accessibles au travers des canaux proposés (site internet, applications mobiles). D'ailleurs la lettre du secrétaire général fait le constat que de nombreux établissements de crédit ont fait l'objet de plusieurs cyber-attaques de plus en plus sophistiquées ayant entraîné des pertes financières importantes. Ces pertes qui au regard de la fréquence et de l'ampleur pourraient mettre en péril le système bancaire et financier en zone CEMAC.
Dans sa lettre-circulaire, le secrétaire général de la COBAC énumère quelques une des négligences mises en lumière par des missions conduites par son organisme lors des contrôles sur site qui accentuent la menace :

- Absence de politique de gestion des mots de passe et des droits d'accès.
- Non réalisation des tests d'intrusion qui permettraient d'apprécier la vulnérabilité des systèmes d'information face à de potentielles attaques;
- Absence de séparation entre les environnements de systèmes de développement de test et de production.

Notre compréhension des enjeux

Les principaux enjeux de la lettre circulaire de la COBAC

- Réalisation de l'audit indépendant de sécurité des SI et transmettre le rapport d'audit à la COBAC dans les délais
- Adoption d'un référentiel international unique pour l'audit indépendant de sécurité des SI
- Définition du périmètre et de l'étendue des travaux à réaliser dans le cadre de l'audit indépendant de sécurité des SI

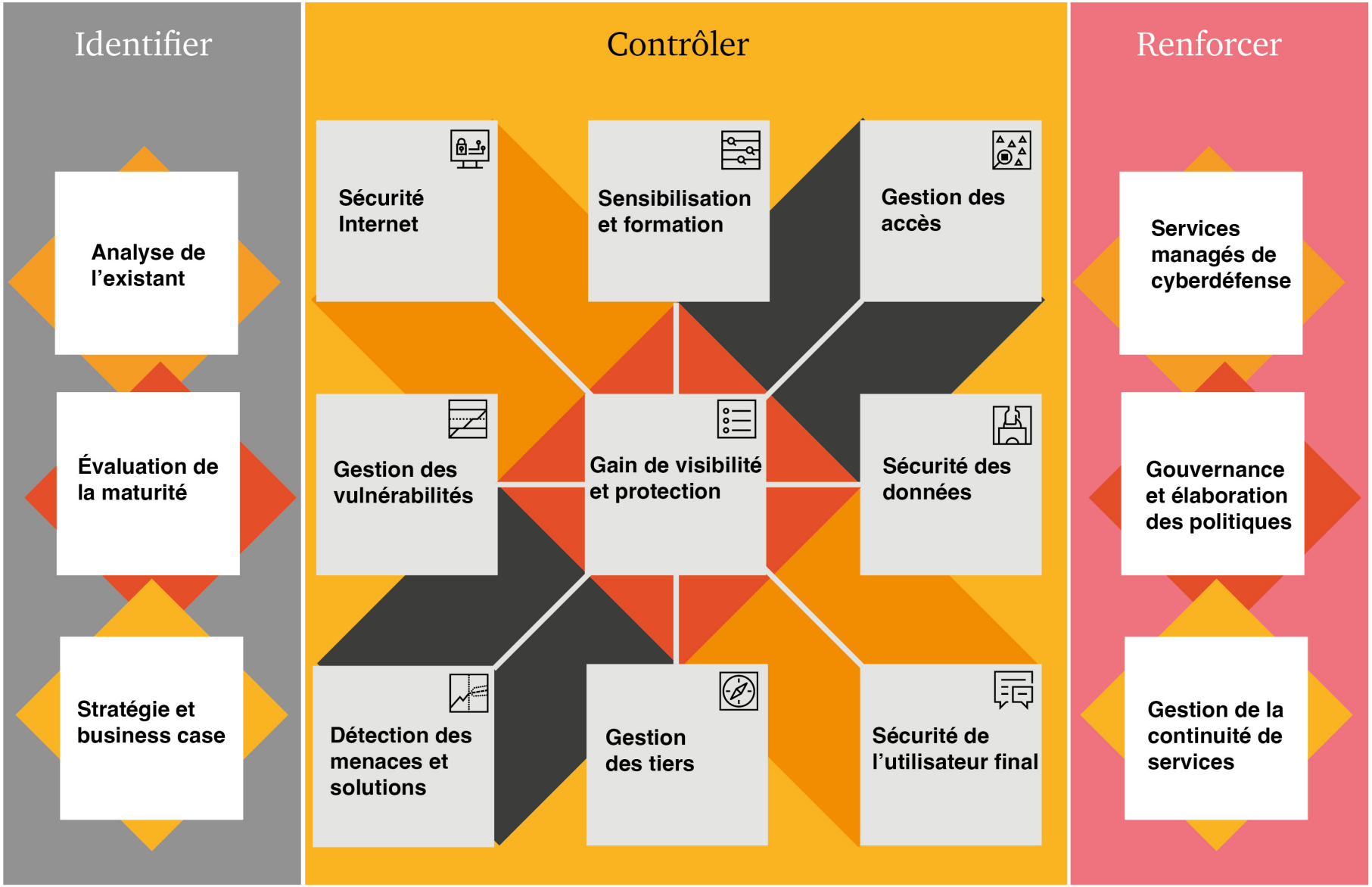
Comment PwC peut aider?

Notre rôle est de vous aider à créer la confiance et à générer des résultats durables. Ainsi, PwC se positionne comme votre partenaire de confiance pour vous accompagner dans l'atteinte de vos objectifs de cybersécurité
Nous vous accompagnons dans:

- la sélection d'un Cabinet indépendant dans le respect des procédures de passation des marchés et contractualiser dès que possible compte tenu de l'échéance et des délais de validation des livrables
- L'adoption de la norme ISO 27001 comme référentiel international pour réaliser l'audit indépendant de sécurité des SI
- L'inclusion dans le périmètre des travaux l'ensemble des systèmes, processus et données critiques
- La prise en compte de l'ensemble des entités concernées y compris les centres des services partagés

L'offre de PwC en matière de cybersécurité

Une approche basée sur trois grands axes : identifier, contrôler, renforcer pour vous aider à faire face à vos enjeux de cybersécurité.



Par où commencer? 8 actions clés à prendre

Déterminer votre degré de tolérance aux risques cyber
1

Faire une analyse de l'existant/ Audit
2

Recruter/ former un RSSI
3

Développer un plan de conformité et une stratégie de sécurité informatique
4

Former une équipe de pilotage et de gestion de crise cyber
5

Créer des guides tactiques d'intervention sur incidents
6

Sensibiliser/ former le comité de direction et l'ensemble du personnel
7

Développer des tableaux de bord pour les différents comités de suivi
8

Contact

Valéry Kapnang
Associé
valery.kapnang@pwc.com
+237 677 50 29 80