Projet d’audit technique - Cybersécurité

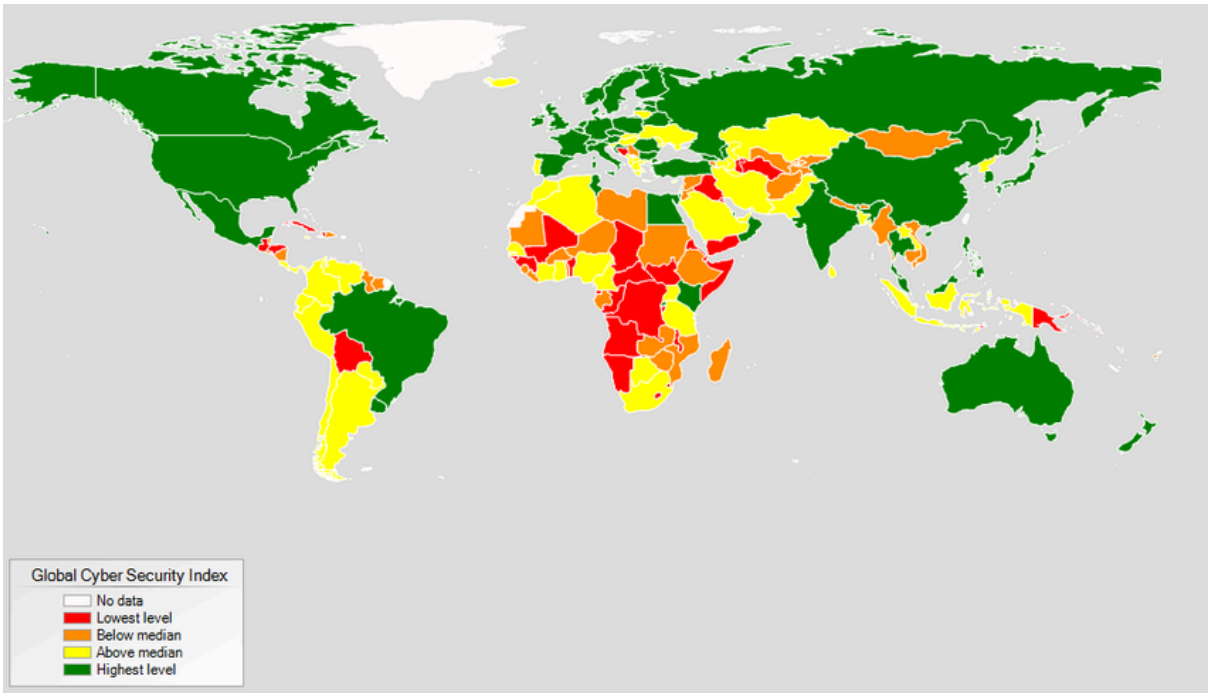
Termes de Référence

Audit technique des institutions financières en conformité vis-à-vis de la cybersécurité

1. Contexte

1.1. Notation de Madagascar

Le Global Cybersecurity Index 2025 (GCI) de Madagascar est évalué à 3,4/10 par l’Unité internationale des télécommunications (UIT)



Source : https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

1.2. Economie nationale

Le secteur financier national subit une transformation numérique accélérée, cette modernisation expose l'économie à un risque systémique majeur.

- **Risque systémique :** Si une seule grande banque primaire, un Mobile Banking ou une microfinance est bloquée par un *ransomware*, c'est toute l'économie du pays qui s'arrête (blocage des salaires, des importations, de la compensation).
- **Souveraineté numérique :** l'État s'appuie sur des compétences locales certifiées au plus haut niveau international plutôt que de dépendre uniquement de cabinets étrangers hors de prix.

2. Faiblesses constatées

À ce jour, le cadre réglementaire en vigueur laisse une trop grande latitude aux institutions financières dans l'évaluation discrétionnaire de leurs propres dispositifs de sécurité. Cette gouvernance passive engendre deux biais structurels majeurs :

- **Le conflit d'intérêt du contrôle interne :** Les Responsables de la Sécurité des Systèmes d'Information (RSSI) internes se retrouvent structurellement juges et parties. Leurs rapports de conformité, soumis à de fortes contraintes budgétaires ou à des pressions hiérarchiques internes, ne reflètent pas systématiquement la réalité opérationnelle des vulnérabilités.

3. Objectif

Sous l'impulsion de la Commission des Finances et du Budget, et en parfaite concertation avec la Primature et le Ministère de l'Economie et des Finances, il est impératif d'amener la CSBF au niveau de la Banky Foiben'i Madagasikara à émettre une instruction sectorielle contraignante et d'application immédiate visant à articuler trois piliers :

1. Instaurer un audit de cybersécurité externe obligatoire : Imposer de manière stricte à chaque institution financière (Banques, Assurances, IMF) un audit technique, organisationnel et de gouvernance approfondi, réalisé sur un rythme annuel ou bisannuel.

2. Exiger la tierce maintenance de confiance (Indépendance) : Interdire formellement que cet audit soit exécuté par des équipes internes ou par le fournisseur/intégrateur principal des infrastructures de l'institution. L'évaluation doit obligatoirement être menée par un Cabinet Indépendant dûment agréé par la CSBF.

3. Sanctionner le non-respect de la conformité : Introduire un régime de sanctions financières dissuasives et de mesures administratives coercitives (allant jusqu'à la suspension conservatoire de l'agrément d'exploitation) pour les entités ne se soumettant pas à l'obligation ou échouant à corriger les failles critiques dans un délai strict imparti.

4. Proposition de Feuille de route législative et exécutive

Nr	Projet	Echéance	Responsable	Etat
1	Lancer officiellement l'atelier de constitution de la Stratégie Nationale de Cybersécurité	Déc. 2025	CIRT MDG	Fait
2	Initier un atelier interne sur l'analyse des risques et les mesures d'atténuation des institutions financières vis-à-vis de la cybersécurité	Mois 1	CERTIM et Expert national	Fait
3	Consulter les avis des autorités compétences sur l'élaboration du note de cadrage en matière de l'obligation à réaliser un audit indépendant auprès des institutions financières vis-à-vis de la cybersécurité	Mois 2	CERTIM	En cours
4	Valider la résolution de l'atelier et la consultation des autorités sur l'analyse des risques et les mesures d'atténuation des institutions financières vis-à-vis de la cybersécurité	Mois 3	Autorité	
5	Créer un task-force sur l'état des lieux du 1er rapport d'évaluation des institutions financières pilotes vis-à-vis de la cybersécurité	Mois 3	Task-force	
6	Elaborer une lettre de politique sectorielle sur les mesures d'atténuation des risques de cyberattaques envers les institutions financières	Mois 4	MEF	
7	Emettre un texte réglementaire sur l'obligation de réaliser un audit indépendant en cybersécurité	Mois 5	MEF/BFM	

	pour la sécurité des consommateurs en paiement électronique			
8	Mettre à jour la politique de sécurité du système d'information en précisant l'obligation de réaliser un audit indépendant	Mois 5	Institutions financières pilotes	
9	Réaliser un audit indépendant auprès des institutions financières pilotes vis-à-vis de la cybersécurité	Mois 6	Cabinet d'Expert pilote	
10	Valider le 1er rapport d'évaluation des institutions financières pilotes vis-à-vis de la cybersécurité	Mois 9	Task-force	
11	Transmettre le 1er rapport d'évaluation aux autorités compétentes, autorités de régulation, aux institutions financières et à UIT	Mois 10	Task-force	
12	Effectuer le 2nd cycle d'évaluation	Mois 12	Cabinet d'expertise	