1KOSMOS

Additional Factors of Authentication (AFA)

Impacts and Implications of The Bank Negara Malaysia's advise on managing cyber threats and strengthening defense

Whitepaper

Executive Overview

To strengthen the resilience of financial services and enhance cyber defense, Bank Negara Malaysia has issued an Exposure Draft outlining updated requirements for managing technology and cyber risks. The policy aims to elevate industry-wide cybersecurity standards, improve customer protection, and facilitate the secure adoption of emerging technologies. Grounded in both local and global risk insights, past incident analysis, and evolving best practices, the framework requires financial institutions to:

Invest in skilled expertise and robust IT controls to prevent operational disruptions.

Strengthen defenses against sophisticated cyber threats.

Ensure strong oversight of third-party providers.

Adopt ethical, inclusive, and responsible technology practices.

The policy adopts a proportionate approach—larger, more digitized institutions must implement more comprehensive safeguards. Enforcement actions may include third-party reviews, remediation plans, additional capital requirements, or other corrective measures for non-compliance with key provisions.

1Kosmos, with its **privacy-by-design** platform, is well-positioned to help financial institutions comply with these requirements. By delivering **verified identity assurance, passwordless and multi-factor authentication**, and seamless **user control over personal data**, 1Kosmos enhances security while improving customer experience. Its solutions support institutions in building operational resilience, reducing fraud risk, and maintaining regulatory compliance.

Ultimately, this revision is intended to bolster institutional and system-wide resilience, ensure secure digital innovation, and maintain public trust in Malaysia's financial ecosystem.

BNM's Framework – An Overview

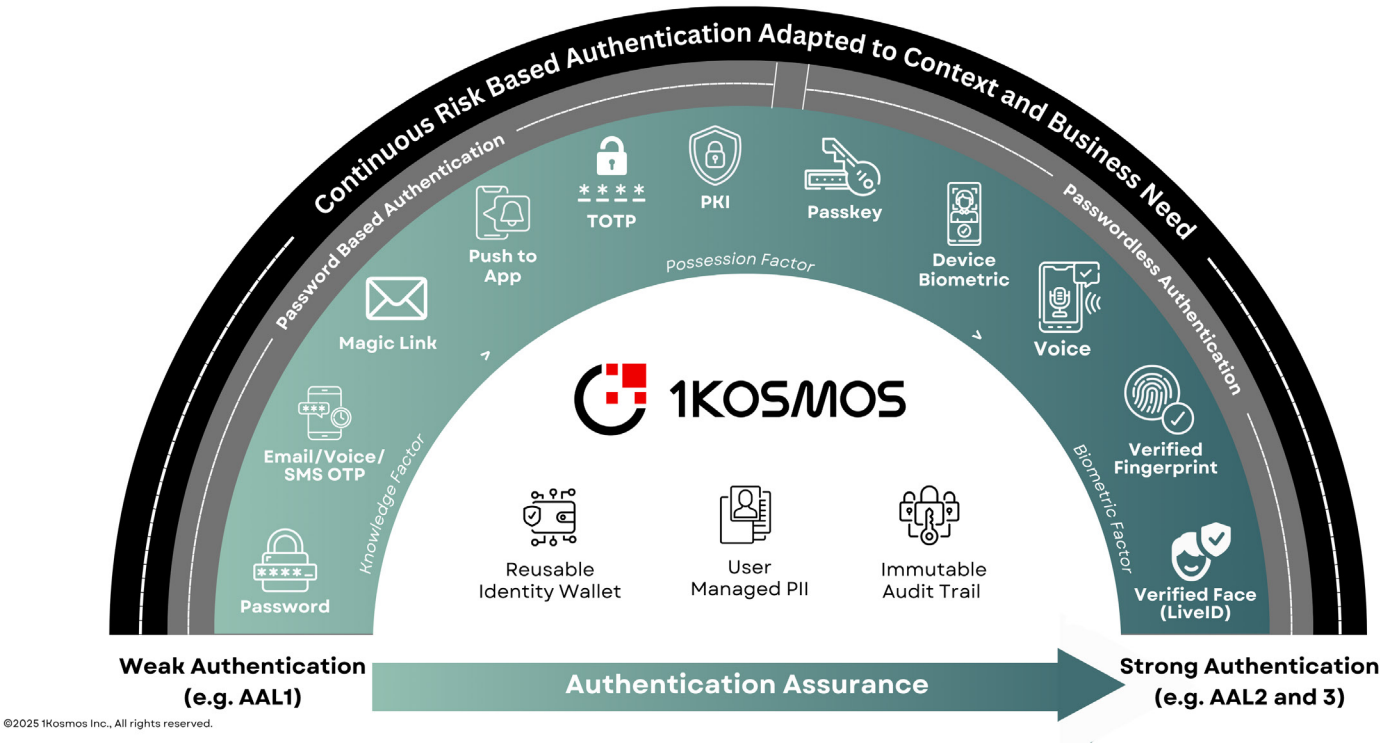
BNM's RMiT The November 2024 Exposure Draft significantly raises the cybersecurity benchmark for Malaysian financial institutions—transforming from periodic compliance to continuous, proactive cyber defense.

A brief overview of the guidelines, as advised for financial institutions by BNM include the following:

- **Financial institutions must implement an access control policy that ensures proper identification, authentication, and authorization of all users, with controls tailored to the level of risk**
- **Robust user authentication must align with asset criticality, and multi-factor authentication (MFA) should resist social engineering by combining at least two factors such as knowledge, inherence, or possession. MFA must be securely activated after user verification, with customer notifications for any activation or changes, and must avoid unencrypted SMS channels.**
- **A Cyber Risk Framework (CRF) should define governance, resilience objectives, and risk tolerance, supporting effective identification, protection, detection, response, and recovery across all systems, while adopting zero-trust principles, real-time monitoring, strong incident response, automated asset tracking, and dedicated cyber risk management functions.**
- **Strong identity verification and credential binding must be enforced to prevent impersonation and fraud. Technology risks should be classified by impact and likelihood, monitored continuously, and overseen independently.**
- **Before adopting cloud services, a comprehensive risk assessment must address deployment sophistication, migration, geopolitical and legal risks, multi-tenancy, vendor lock-in, security configurations, cyber exposure, termination processes, responsibility demarcation, and compliance with regulations.**
- **Institutions must retain full control of encryption keys, store public keys in certificates from recognized authorities, and protect private keys to remain legally binding. For third-party vendors, due diligence, clear SLAs, and continuous risk monitoring are essential.**
- **Finally, institutions must ensure digital services are secure, with device-level security and fraud detection in place to prevent unauthorized access and malicious activities.**

The 1Kosmos Platform

The 1Kosmos platform exhibits flexibility which allows service providers and their users to choose the authentication method that best suits their needs, thereby increasing the adoption of digital payments while maintaining high security standards with minimal friction to the user experience.



©2025 1Kosmos Inc., All rights reserved.

The platform is attested for Authentication Assurance Level 1, 2, and 3 as per NIST 800-63 standards. This allows 1Kosmos to enforce multiple factors of authentication via various authentication methods in a single platform.

It also leverages **adaptive authentication** to adjust the required factors based on risk signals, ensures secure transmission and storage of authentication data, and provides convenient user management and recovery options. This approach helps to protect against unauthorized access while maintaining a user-friendly experience.

1Kosmos customers are able to leverage this in multiple ways, for example, by this global banking customer.

Adopting MFA

Notably, among other guidelines, The BNM exposure draft recommends that the adoption of MFA for financial and high-risk non-financial transactions.

The 1Kosmos platform fully supports the adoption of Multi-Factor Authentication (MFA) for financial and high-risk non-financial transactions and for performing subsequent funds transfers to that beneficiary, through the following methods.

1. Biometric Authentication

Advanced biometrics such as facial recognition, fingerprint scanning, and liveness detection are supported. These methods are identity-bound, ensuring authentication is tied to a verified individual.

2. Passwordless MFA

The platform eliminates passwords by combining biometrics with cryptographic keys, providing a seamless and secure user experience.

3. Cryptographic Authenticators

Public-private key pairs are used for secure authentication, ensuring credentials cannot be intercepted or reused.

4. Push Notifications

Users can authenticate by approving push notifications sent to their registered devices.

5. Hardware Tokens

The platform supports FIDO2-compliant security keys and other hardware-based authenticators for high-assurance authentication.

6. Device Biometrics

Users can authenticate using device-native biometrics, such as Apple Face ID or Android Fingerprint.

7. One-Time Passcodes (OTPs)

OTPs delivered via SMS, email, or authenticator apps are supported as a fallback authentication method.

8. Magic Links

Users can authenticate by clicking on a secure, time-sensitive link sent to their email or mobile device.

9. TOTP (Time-Based One-Time Password)

The platform supports TOTP for scenarios requiring time-sensitive, app-generated codes.

10. Passkeys

The platform supports passkeys, which are cryptographic credentials stored on devices, enabling secure and passwordless authentication

Managing Cyber Risk

In addition to adopting MFA, another key guideline as highlighted in the Exposure draft is that institutions must develop a Cyber Risk Framework (CRF) that defines governance, cyber resilience objectives, and risk tolerance, considering the evolving threat landscape. The CRF should ensure operational resilience against extreme but plausible cyber-attacks and support effective identification, protection, detection, response, and recovery (IPDRR) for systems and data, whether hosted on-premises or by third-party providers.

1Kosmos Alignment with Cyber Risk Framework (CRF) Requirements:

1. Comprehensive Understanding of Cyber Risks

1Kosmos enhances cyber risk visibility by verifying identities through government ID proofing and biometric authentication.

It provides identity-related telemetry and analytics that help organizations assess and mitigate identity-based risks.

2. Classification & Prioritization of Critical Assets

By enforcing role-based access policies, 1Kosmos ensures that only authorized, verified users can access critical applications and data.

Integrates with IAM and SIEM platforms to map access patterns and secure high-value assets.

3. Threat Identification & Countermeasures

Real-time behavioral risk analysis, device fingerprinting, and geolocation help detect and respond to threats.

Allow step-up authentication or blocks access when anomalies are detected.

4. Adoption of Zero Trust Architecture

Built on Zero Trust principles: no user or device is trusted by default until users are verified by biometrics.

Enforces identity verification.

5. Real-Time Monitoring

Provides monitoring APIs for integration with third-party SIEM tools.

Enables real-time tracking of authentication events and access attempts in audit logs.

6. Robust Incident Response Support

Maintains detailed audit logs and verification trails.

Facilitates forensic investigations by recording who accessed what, when, and how.

7. Secure Collaboration Enablement

Enables secure, passwordless access to enterprise and collaboration tools.

Prevents unauthorized sharing or misuse of credentials.

8. Automated Asset Tracking Support

1Kosmos supports tracking of identity access to systems and services. 1Kosmos binds a user identity to a FIDO2 compliant security device which enables organizations to track which assets (devices or endpoints) are being authenticated by users.

9. Dedicated Cyber Risk Management Function

Supports ongoing cyber risk management with continuous identity assurance.

1Kosmos Platform Helps Meet Global Privacy Standards

1) Enhanced Security

Passwords are susceptible to breaches, phishing, and other attacks. The diverse and flexible methods (e.g., biometrics, device-based authentication, and one-time codes) offered by 1Kosmos reduce the risk of unauthorized access, aligning with Global Data Privacy requirements for strong data protection.

2) Compliance

Adhering to industry standards and certifications such as the NIST 800-63-3 identity proofing and access management, FIDO2 for passwordless authentication and iBeta for biometric authentication.

3) Privacy by Design

The state-of-the-art approach of 1Kosmos solution encourages a ''privacy by design'' approach. This approach inherently reduces the data footprint and enhances user security, which is built into the authentication mechanism from the start.

4) Improved User Control and Transparency

The reliable mechanisms, particularly those that use biometrics or device-based factors, help comply with the Global Data Privacy Acts and regulations that emphasis on user rights by giving individuals more control over their data (e.g., biometric data stored locally on their device rather than a central server).

5) Reduced Risk of Data Breaches

With fewer stored passwords, the organization's risk of exposure from data breaches decreases, which helps in meeting the data security and breach reporting standards.

Conclusion

The 1Kosmos platform offers a comprehensive suite of features that directly address and fulfill the compliance requirements outlined in the RMiT 2024 Exposure Draft. With advanced identity proofing, strong authentication, cryptographic security, and robust governance tools, 1Kosmos empowers financial institutions to build secure, compliant, and customer-centric digital ecosystems. The platform's risk-based approach, customer consent mechanisms, and real-time transaction alerts further align with the BNM's requirements. Additionally, 1Kosmos' commitment to compliance and standardization ensures that its solutions are secure, interoperable, and reliable, making it an ideal choice for issuers looking to meet the BNM's guidelines.

Breakdown Chart

To read further in depth about how 1Kosmos complies with the The Bank Negara Malaysia's advise on managing cyber threats and strengthening defense, kindly refer to our section wise breakdown

Read Here

About 1Kosmos
1Kosmos enables remote identity verification and passwordless multi-factor authentication for workers, customers and residents to securely transact with digital services. By unifying identity proofing, credential verification and strong authentication, the 1Kosmos platform prevents identity impersonation, account takeover and fraud while delivering frictionless user experiences and preserving the privacy of users' personal information. 1Kosmos performs millions of authentications daily for government agencies and some of the largest banks, telecommunications, higher education, and healthcare organizations in the world.

1KOSMOS

©2025 One Kosmos Inc., All rights reserved.