Additional Factors of Authentication (AFA) Section Wise Breakdown

Section Wise Breakdown - How 1Kosmos complies with The Bank Negara Malaysia's advise on managing cyber threats and strengthening defense

Whitepaper

Intro

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. Below you shall find a section-wise breakdown on how 1Kosmos complies with The Bank Negara Malaysia's advise.

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.**

Section	Compliance Points	1Kosmos Compliance Features
10.53	A financial institution must implement an access control policy for the identification, authentication, and authorization of all users to its IT assets and data. The level of granularity defined in the access control policy shall be commensurate with the level of risk of unauthorized access to its IT assets.	**Access Control:** 1Kosmos enables role-based policies, allowing institutions to define user permissions based on identity assurance level, device, location, and behavior—ensuring access aligns with risk. **Strong Identity Verification & Authentication:** Through passwordless, biometric-based authentication and identity proofing (including government ID verification), 1Kosmos ensures only verified users can access sensitive IT assets. **Audit & Compliance:** 1Kosmos maintains detailed logs and audit trails for authentication events and policy enforcement, helping financial institutions demonstrate adherence to access control policies.
10.54	A financial institution must implement a default "deny all" access policy, enforce least privilege and time-bound access, and segregate incompatible functions to prevent conflicts of interest. Dual authorization should be required for sensitive activities. Robust user authentication must be applied based on asset criticality, ensuring strong identity verification, especially for high-risk access.	1Kosmos enforces authentication using Zero Trust principles where access is not granted until the user is verified using biometrics or strong MFA and the user's device and identity are authenticated and authorized by enabling strong identity proofing and binding so roles cannot be impersonated or misused. 1Kosmos grant the required access or privilege by giving strong and verified identity assurance before granting access.

Section	Compliance Points	1Kosmos Compliance Features
10.55	A financial institution must employ multi-factor authentication (MFA) that can defend against social engineering attacks for authenticating user access, to critical systems. The MFA must combine two or more of knowledge factors, inherent factors (e.g. biometric characteristics) or possession factors (e.g. security keys, tokens).	MFA Compliance 1Kosmos fully supports Multi-Factor Authentication (MFA) using the three key authentication factors: • Knowledge – such as a PIN or gesture. • Possession – typically a registered mobile device. • Inherence – biometric traits like fingerprint or facial recognition. This ensures strong identity assurance, satisfying regulatory requirements such as PCI DSS, ISO 27001 and NIST while offering seamless, passwordless access through layered protection.
10.57	A financial institution must ensure— (a) access controls to enterprise-wide systems are effectively managed and monitored; (b) anomalies are flagged for prompt investigations to contain any cyber incidents; and (c) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained	1Kosmos helps financial institutions comply by enabling centralized access control, detects real time anomalies and detailed user activity logging. It integrates with SIEM tools to monitor access across systems and maintains audit logs to support compliance and incident response.

Section	Compliance Points	1Kosmos Compliance Features
10.57	investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner.	
11.2	A financial institution must develop a CRF which clearly articulates the institution's governance for managing cyber risks, its cyber resilience objectives and its risk tolerance, with due regard to the evolving cyber threat environment. Objectives of the CRF shall include ensuring operational resilience against extreme but plausible cyber-attacks. The framework must be able to support the effective identification, protection, detection, response, and recovery (IPDRR) of systems and data hosted on-premises or by third party service providers from internal and external cyber-attacks.	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.

Section	Compliance Points	1Kosmos Compliance Features
11.3	The Cyber Risk Framework (CRF) must ensure a comprehensive understanding of cyber risks, classify and prioritize critical assets, and identify threats and countermeasures. It should adopt global best practices like zero-trust, enable real-time monitoring, have robust incident response plans, promote secure collaboration, maintain automated asset tracking, and establish a dedicated cyber risk management function for ongoing threat analysis and escalation.	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.

Section	Compliance Points	1Kosmos Compliance Features
11.3		-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.

Cybersecurity Controls and Monitoring

Section	Compliance Points	1Kosmos Compliance Features
11.1 to 11.17, Appendix 5	To maintain a resilient security posture, organizations must implement continuous threat detection and monitoring, conduct regular red team simulations and penetration testing, and establish robust systems for detecting anomalies and security incidents in real time	**Behavioral Biometrics** 1Kosmos continuously monitors and analyzes user behavior—such as keystroke dynamics. Any deviation from this established pattern triggers a step-up authentication, enabling early detection of credential misuse or insider threats. **Audit Trails** The platform maintains comprehensive, tamper-proof audit logs that record every authentication attempt, user activity, and system access event. These logs are vital for compliance reporting, incident investigation, and forensic analysis, helping organizations quickly trace and respond to suspicious activity. **Geolocation Monitoring** 1Kosmos captures and assesses the user's geographical location at the time of login. If access is attempted from unusual or high-risk locations, the system can automatically block the attempt or require additional authentication, adding a strong contextual layer of security. **Adaptive Authentication** Leveraging risk-based analytics, 1Kosmos dynamically adjusts authentication requirements based on contextual signals such as device trust, location, login time, and behavioral patterns.

User Identity Verification & Credential Binding

Section	Compliance Points	1Kosmos Compliance Features
10.21, 10.55, 11.3C	Organizations must ensure strong identity verification and credential binding to authenticate users accurately, implement measures to prevent impersonation and fraud, and enforce secure authentication methods to protect access to digital services	Live Identity Proofing Live identity proofing combines biometric liveness detection with real-time document verification to confirm that the user is physically present, and their identity is genuine. It uses liveness checks to detect spoofing attempts and matches the live image with government-issued IDs. This ensures secure onboarding and eliminates the risk of identity fraud during user registration or access. Blockchain Ledger A blockchain ledger provides an immutable and decentralized way to store identity bindings and credentials. By recording cryptographically hashed identity data on the blockchain, any tampering or unauthorized changes become virtually impossible. This approach enhances trust, transparency, and security in identity verification processes while giving users more control over their data. Verifiable Credentials 1Kosmos supports Verifiable Credentials through its platform, which leverages W3C-compliant verifiable credential standards. It allows organizations to issue digitally signed credentials to users after identity verification. These credentials are stored in the user's self-sovereign identity wallet, and users can control what attributes to share. Third-party verifiers can instantly validate the credentials' authenticity using cryptographic proofs, enabling trust without centralized data access—ideal for privacy, compliance, and decentralized identity ecosystems.

Section	Compliance Points	1Kosmos Compliance Features
9.1 to 9.5, 10.1 to 10.3	Organizations must classify technology risks based on their impact and likelihood, implement continuous monitoring to detect emerging threats, and establish independent oversight functions to ensure objective assessment and governance of technology-related risks	Configurable Risk Tiers 1Kosmos allows administrators to define risk levels for users based on their authentication strength—such as biometric, passwordless, or legacy credentials—ensuring adaptive access control. Real-time Risk Analysis 1Kosmos captures the user activity to detect anomalies or suspicious patterns to enforce step-up authentication when needed. Admin Dashboard 1Kosmos provides a centralized dashboard for real-time visibility into identity audit logs.

Cloud Adoption & Cryptography

Section	Compliance Points	1Kosmos Compliance Features
10.20 to 10.22, 10.50	Organizations must maintain full control over encryption keys to safeguard sensitive information and ensure that cloud services are used securely, with clear policies in place to uphold data ownership and accountability.	1Kosmos supports the management of cryptographic keys, enabling secure user authentication through passkeys. Customer Data Sovereignty With 1Kosmos, customers retain full ownership and control of their identity data, aligning with privacy and regulatory requirements. SHA-2 Compliant Encryption 1Kosmos employs SHA-2 certified encryption standards to ensure secure data handling and compliance with government and industry regulations.

Section	Compliance Points	1Kosmos Compliance Features
10.5	A financial institution must fully understand the inherent risk of adopting cloud services. In this regard, a financial institution is required to conduct a comprehensive risk assessment prior to cloud adoption which considers the inherent architecture of cloud services that leverages on the sharing of resources and services across multiple tenants over the Internet. The assessment must specifically address risks associated with the following: (a) sophistication of the deployment model; (b) migration of existing systems to cloud infrastructure; (c) location of cloud infrastructure including potential geopolitical risks and legal risks that may impede compliance with any legal or regulatory requirements; (d) multi-tenancy or data co-mingling; (e) vendor lock-in and application portability or interoperability; (f) ability to customise security configurations of the cloud infrastructure to ensure a high level of data and technology system protection; (g) exposure to cyber-attacks via cloud service providers; (h) termination of a cloud service provider including the ability to secure the financial institution's data following the termination; (i) demarcation of responsibilities, limitations and liability of the cloud	The 1Kosmos platform mitigates cloud adoption risks for financial institutions through its single-tenant deployment model for resource isolation, robust API framework for seamless migration, and compliance with GDPR, SOC2, and ISO 27001. It leverages Google Cloud with multiple data centers for redundancy and disaster recovery, supports customizable security configurations, and ensures interoperability to avoid vendor lock-in. Regular penetration testing, encryption, and disaster recovery mechanisms protect against cyber-attacks, while clear contractual agreements define responsibilities and liabilities. The platform meets regulatory requirements and international standards, ensuring secure and compliant operations.

Section	Compliance Points	1Kosmos Compliance Features
10.5	(h) termination of a cloud service provider including the ability to secure the financial institution's data following the termination; (i) demarcation of responsibilities, limitations and liability of the cloud service provider; and (j) ability to meet regulatory requirements and international standards on cloud computing on a continuing basis.	
10.23	A financial institution shall store public cryptographic keys in a certificate issued by a certificate authority as appropriate to the level of risk. Such certificates associated with customers shall be issued by recognized certificate authorities. The financial institution must ensure that the implementation of authentication and signature protocols using such certificates are subject to strong protection to ensure that the use of private cryptographic keys corresponding to the user certificates are legally binding and irrefutable. The initial issuance and subsequent renewal of such certificates must be consistent with industry best practices and applicable legal/ regulatory specifications	1Kosmos supports this requirement by issuing digital certificates through trusted certificate authorities and managing cryptographic keys securely using FIDO2 and PKI standards. Private keys are stored safely on user devices, while public keys are certified and verifiable. It ensures legally binding, non-repudiable authentication and handles certificate issuance and renewal in line with industry and regulatory best practices

Third-Party & External Assurance

Section	Compliance Points	1Kosmos Compliance Features
10.46 to 10.49, Section	Organizations must conduct thorough due diligence and establish clear Service Level Agreements (SLAs) with third-party vendors to ensure accountability. Additionally, continuous monitoring mechanisms should be implemented to detect and respond to risks in real-time, maintaining compliance with regulatory expectations.	Certified Platform: 1Kosmos meets industry-leading standards like SOC2, ISO 27001,NIST and GDPR, ensuring strong security, privacy, and regulatory compliance. Monitoring APIs: It offers APIs that integrate with SIEM tools, enabling real-time security monitoring and third-party assurance. Reporting: 1Kosmos provides detailed audit trails for identity verifications and system activity, supporting transparency and compliance audits.

Digital Services & Customer Protection

Section	Compliance Points	1Kosmos Compliance Features
12.1, Appendix 3 & 4	Organizations must ensure the secure delivery of digital services by implementing robust cybersecurity measures, while also enforcing device-level security and fraud detection mechanisms to safeguard against unauthorized access and malicious activities.	Secure Mobile SDKs 1Kosmos provides secure SDKs that allow developers to embed strong, passwordless identity verification directly into mobile apps. Verification of Phone Number Through SIM The system requires the user to send an SMS from the SIM card tied to the registered phone number. This ensures that the mobile number being claimed is active on the user's device and not just controlled by someone with access to other personal details. SIM Binding Mechanism By requiring SMS consent from the SIM on the user's phone, the system creates a direct association between the phone number and the specific SIM, preventing attackers from using a different SIM card with the same phone number. Geo-location & Device Fingerprinting These features block login attempts from unfamiliar devices or locations, enhancing protection against identity-based attacks.

Section	Compliance Points	1Kosmos Compliance Features
Appendix 3 (Point 4)	Adopt MFA for financial and high-risk non-financial transactions. This includes when registering an account as a "favourite" beneficiary and, for all subsequent funds transfer to the favourite beneficiary;	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. Below MFA Supported: 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.

Section	Compliance Points	1Kosmos Compliance Features
Appendix 3 (Point 4)		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.

Section	Compliance Points	1Kosmos Compliance Features
Appendix 3 (Point 5)	A financial institution must ensure the MFA solution used to authenticate financial transactions are adequately secure and resistant to phishing attacks, which includes the following: (a) activation of MFA must be subject to robust verification by the financial institution; (b) timely notification to customers of any activation of and changes to the MFA solution via the customers' verified communication channel; and (c) deployment of MFA technology and channels that are more secure than unencrypted short messaging service (SMS).	The 1Kosmos platform is designed to meet the stringent security requirements of financial institutions for Multi-Factor Authentication (MFA) in financial transactions. The platform addresses the specified requirements as follows: (a) Activation of MFA Must Be Subject to Robust Verification by the Financial Institution 1. Identity Proofing During Enrollment: • 1Kosmos ensures that MFA activation is tied to a verified identity. During enrollment, users undergo robust identity proofing, which includes biometric verification (e.g., facial recognition with liveness detection) and document verification. This ensures that only legitimate users can activate MFA. 2. High Assurance Standards: • The platform complies with high assurance standards such as NIST 800-63-3, FIDO2, and ISO/IEC 30107-3, ensuring that the identity verification process is tamper-resistant and meets regulatory requirements. b)Deployment of MFA Technology and Channels That Are More Secure Than Unencrypted Short Messaging Service (SMS)

Section	Compliance Points	1Kosmos Compliance Features
Appendix 3 (Point 5)		1. Phishing-Resistant MFA: • 1Kosmos provides phishing-resistant MFA methods, including: • Biometric authentication (e.g., facial recognition with liveness detection, TouchID, FaceID). • FIDO2-compliant passkeys and tokens. • Time-Based One-Time Passwords (TOTP) generated through secure apps like the 1Kosmos app or third-party authenticators (e.g., Google Authenticator, Microsoft Authenticator). 2. Elimination of SMS Dependency: • While the platform supports SMS-based OTPs for legacy use cases, it strongly encourages the use of more secure alternatives, such as push notifications, TOTP, or FIDO2 tokens, which are resistant to phishing and SIM-swapping attacks. 3. End-to-End Encryption: • All communication between the 1Kosmos platform and the user is encrypted using industry-standard protocols, ensuring that sensitive data is protected during transmission. 4. Passwordless Authentication: • The platform supports passwordless authentication, which eliminates the risks associated with traditional credentials and SMS-based OTPs.

Section	Compliance Points	1Kosmos Compliance Features
Appendix 3 (Point 6)	A financial institution must ensure that the security controls of MFA solutions include adherence to the following requirements: (a) the MFA solution is resistant to interception or manipulation by any third party throughout the authentication process; (b) payer/sender must be made aware and prompted to confirm details of the identified beneficiary and amount of the transaction; (c) authentication code must be initiated and generated locally by the payer/sender using MFA; (d) authentication code generated by payer/sender must be specific to the confirmed identified beneficiary and amount; (e) secure underlying technology must be established to ensure the authentication code accepted by the financial institution corresponds to the confirmed transaction details; and (f) notification must be provided to the payer/sender of the transaction.	The 1Kosmos platform supports the specified MFA security controls for financial institutions as follows: (a) Resistance to Interception or Manipulation • 1Kosmos employs phishing-resistant MFA methods, such as biometrics and FIDO2-compliant tokens, ensuring authentication is tied to the user's verified identity and cannot be intercepted or manipulated by third parties. (b) Confirmation of Beneficiary and Transaction Details • The platform can integrate with financial systems to prompt users to review and confirm transaction details (beneficiary and amount) before completing authentication, ensuring user awareness and consent. (c) Local Generation of Authentication Code • Authentication codes, such as Time-Based One-Time Passwords (TOTP), are generated locally on the user's device via secure apps like the 1Kosmos app, ensuring no external interception. (d) Transaction-Specific Authentication Code • 1Kosmos supports transaction binding, where authentication codes are dynamically generated and tied to specific transaction details (beneficiary and amount), ensuring they cannot be reused or altered.

Section	Compliance Points	1Kosmos Compliance Features
Appendix 3 (Point 6)		(e) Secure Technology for Code Validation • The platform uses end-to-end encryption and secure APIs to validate that the authentication code corresponds to the confirmed transaction details, ensuring integrity and security. (f) Notification to Payer/Sender • Real-time notifications are sent to the payer/sender via verified communication channels (e.g., email, push notifications) to confirm transaction completion and provide transparency.
Appendix 3 (Point 6)	Where a financial institution deploys OTP as an additional factor of authentication, the following features must be implemented: (a) OTP must be dynamic where it changes each time it is required and time-bound; (b) binding of the transaction details to the OTP generated by the device (e.g. beneficiary account number, amount of transaction); and (c) generation of the OTP from the customer's device and not from the bank's server to mitigate the risk of manipulating OTP in the financial institution's infrastructure and increase customer control over authentication process.	1Kosmos supports Time-Based One-Time Passwords (TOTP), which are dynamic and change with each authentication request. These OTPs are time-bound, expiring after a predefined duration, ensuring enhanced security.

Control Measures for Digital Services

Section	Compliance Points	1Kosmos Compliance Features
Appendix 3 (Point 9)	A financial institution must offer to customer a robust cryptographic key based authentication30 such as digital certificate or passwordless as alternative to existing password-based authentication method to mitigate the risk of credential of password being compromised or stolen. The enrolment of this method must subject to robust verification and resilient against cyber threats and fraud techniques.	1Kosmos supports this requirement by offering passwordless, cryptographic key-based authentication using FIDO2 and digital certificates, eliminating the risks of password theft. It ensures secure enrollment through strong identity verification (biometrics and ID proofing) and protects against cyber threats with phishing-resistant login

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.

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