

WHITE PAPER

Risk Management in Technology (RMiT)

Regulatory Mapping

How Cohesity solutions and consulting can help financial institutions address Bank Negara Malaysia's Risk Management in Technology (RMiT) requirements.



TABLE OF CONTENTS

Executive summary	3	Threat Detection & SOC Integration	6
Cohesity Platform Overview	4	Detection Capabilities	6
Cyber Resilience Framework	4	SIEM & SOC Integration	6
Immutability & Data Protection	5	Cohesity CERT	6
DataLock Modes	5	Mapping to RMIT Clauses	7
Encryption	5	Conclusion	10
Zero-Trust Architecture	5		

Executive summary

Bank Negara Malaysia’s Risk Management in Technology (RMiT) requires financial institutions to ensure operational resilience, protect customer data, and maintain continuous delivery of critical financial services, even during cyber incidents, system failures, or third-party disruptions. Institutions must demonstrate:

- Reliable recovery of critical systems and data
- Protection against data destruction and ransomware
- Continued accountability for risk in cloud and outsourced environments
- Clear governance, auditability, and incident readiness

Cohesity is not just a backup and recovery company—its solutions align with RMiT’s intent by:

- Enabling recovery-first resilience through trusted-state recovery
- Providing immutable data protection to support cyber recovery
- Supporting hybrid and multi-cloud recovery control, independent of service providers
- Improving consistency, visibility, and defensibility of recovery controls

Cohesity is positioned as part of a broader operational resilience and cyber recovery strategy that helps financial institutions address RMiT’s core requirement—critical services and data must remain recoverable, resilient, and defensible under stress.

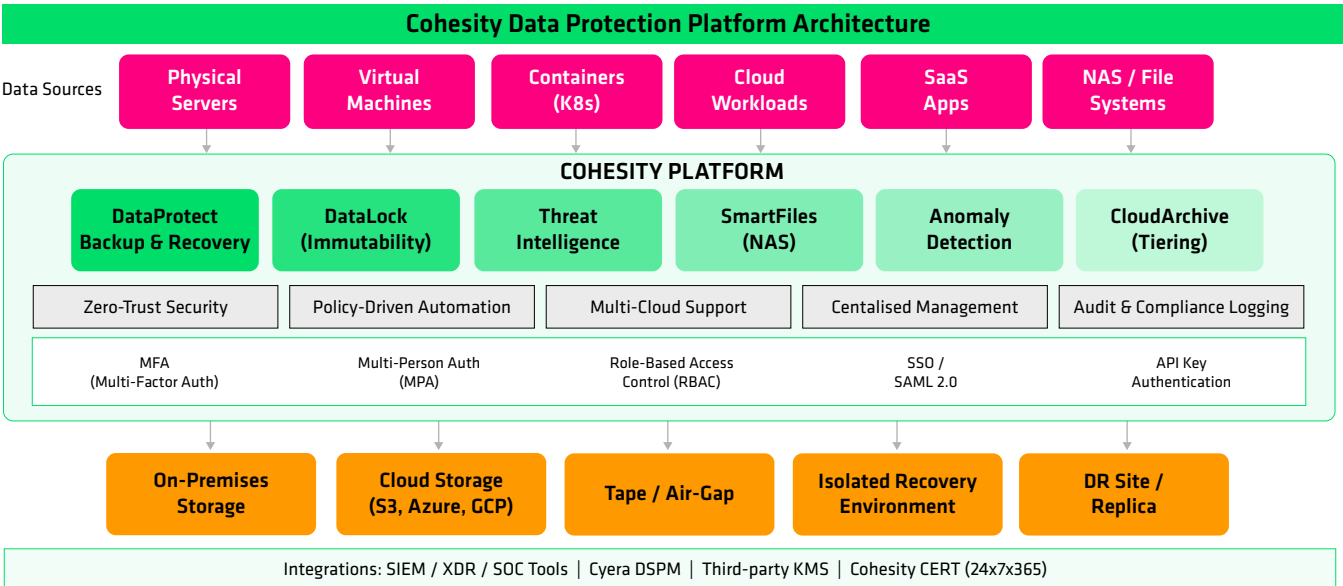


Figure 1: Cohesity Data Protection Platform Architecture

Cohesity Platform Overview

Cohesity provides a unified, policy-driven data security and management platform that consolidates data protection, cyber resilience, and recovery capabilities across on-premises, hybrid, and multi-cloud environments. This section describes the key platform components relevant to RMIT compliance.

Cyber Resilience Framework

Cohesity’s approach to cyber resilience maps directly to the five-phase framework of Identify, Protect, Detect, Respond, and Recover. Each phase is supported by specific platform capabilities and consulting services, enabling financial institutions to build a comprehensive and auditable cyber resilience posture aligned with RMIT requirements.

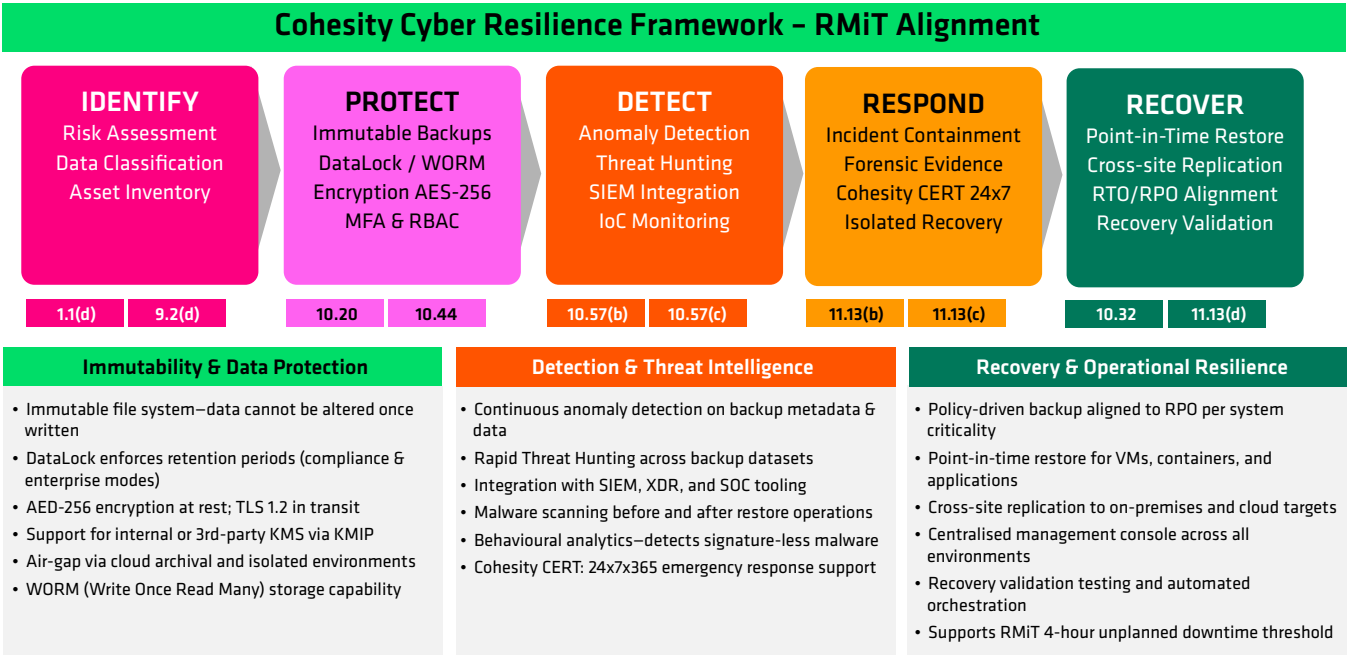


Figure 2: Cohesity Cyber Resilience Framework–RMIT Clause Alignment

Immutability & Data Protection

A central requirement of RMIT—particularly clause 10.45 — is the establishment of tamper-proof backup arrangements and isolated recovery environments. Cohesity addresses this through its DataLock capability and immutable file system, which ensures backup data cannot be modified, encrypted, or deleted during a defined retention period, even by administrators.

DataLock Modes

Cohesity DataLock provides two modes of immutability to suit different institutional requirements and regulatory obligations:

- **Enterprise Mode:** Protects backup data during a pre-defined retention period using dual authorization. Two individuals with different RBAC levels must agree before any changes can be made.
- **Compliance Mode:** Renders storage fully immutable. No user, including the root or administrative user, can delete data during a pre-defined retention period. Meets SEC Rule 17a-4(f) and FINRA Rule 4511(c).

Encryption

All backup data is protected at rest using AES-256 encryption. Data in transit is secured using TLS 1.2. Cohesity supports both internal KMS and third-party KMS integration via KMIP. FIPS 140-2 validated cryptographic modules are used throughout.

Zero-Trust Architecture

Cohesity's platform is built on a zero-trust security model. Multi-Person Authorization (MPA) requires multiple authorized users to approve sensitive operations, and all activity is fully audited for compliance.

Threat Detection & SOC Integration

RMiT places significant emphasis on the continuous monitoring of technology systems and the timely detection of cyber incidents. Cohesity addresses these requirements through anomaly detection, threat hunting, and SIEM integration capabilities.

Detection Capabilities

- **Anomaly Detection:** Continuously monitors backup metadata and job patterns to identify deviations from established baselines, flagging potential ransomware activity or unauthorized access.
- **Threat Hunting:** Enables security teams to query backup datasets directly for indicators of compromise (IoCs), supporting proactive threat detection as required by Appendix 5 Part C.
- **Malware Scanning:** Backup data is scanned against known malware signatures and threat intelligence feeds before and after recovery operations.

- **Rapid Threat Hunting:** Automated scanning across backup history rapidly identifies compromised files, supporting incident containment aligned with RMiT clauses 11.13(b) and 11.13(c).

SIEM & SOC Integration

Cohesity events, alerts, and audit logs can be forwarded to external SIEM platforms including Splunk, IBM QRadar, and Microsoft Sentinel. Activity logs are retained for a minimum of three years as required under RMiT clause 10.57(c).

Cohesity CERT

Cohesity's own Cyber Emergency Response Team (CERT) is available 24x7x365 to support institutions when an anomaly is detected, aligned with RMiT Appendix 10 Part B, clause 14(d).

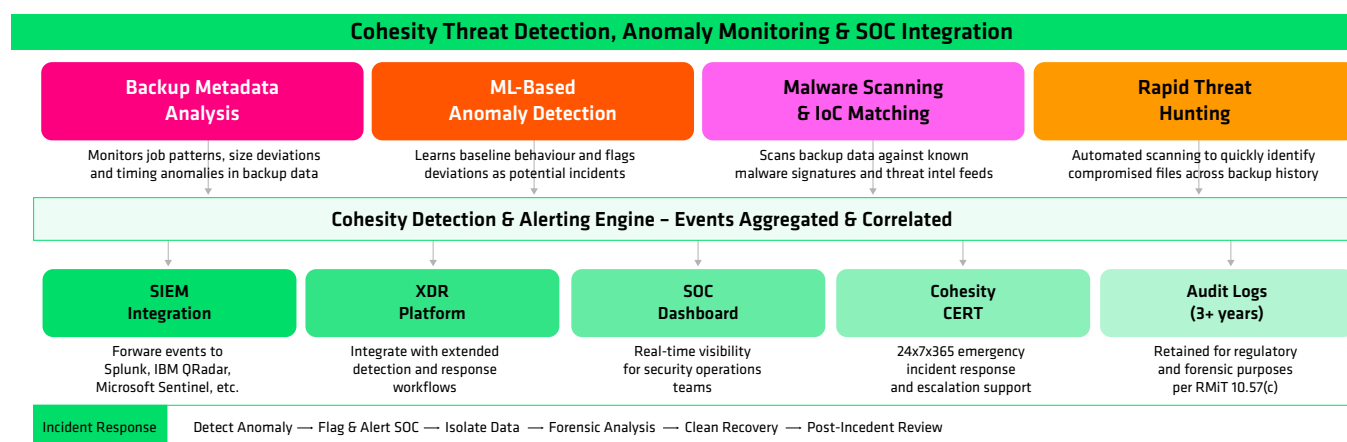


Figure 3: (overleaf) illustrates the full detection and SOC integration architecture.

Mapping to RMIT Clauses

The table below provides a detailed mapping of Cohesity's capabilities to the specific clauses within Bank Negara Malaysia's RMIT policy framework.

Part	Clause	Clause Description	Cohesity's Mapping
A. Overview	1.1 (d)	Build operational resilience against sophisticated and malicious cyber threats amidst heightened cyber risks globally.	Cohesity supports operational resilience by protecting critical data against advanced cyber threats using immutable backups, multi-layered security controls, and ransomware-aware recovery mechanisms, enabling financial institutions to maintain service availability and recover operations quickly in the event of cyber-attacks.
B. Policy Requirements	9.2 (d)	Risk classification of all information assets/systems based on its criticality.	Cohesity facilitates risk-based classification of information assets by aligning data protection policies, retention, immutability, and recovery objectives with the criticality and risk profile of systems and data. Cohesity integrates with Cyera to enhance identification of sensitive information through DSPM integration.
B. Policy Requirements	10.20	A financial institution must establish a robust and resilient cryptography policy promoting the adoption of strong cryptographic controls for protection of important data and information.	Cohesity enables adherence to a robust cryptography policy with strong encryption mechanisms, secure key management integration, and protected communication channels. Encryption modules are in-built and support internal or 3rd-party KMS.
B. Policy Requirements	10.32	For critical systems, a financial institution must ensure high availability with cumulative unplanned downtime of not more than 4 hours on a rolling 12 months basis and maximum tolerable downtime of 120 minutes per incident.	Cohesity enables rapid, reliable recovery of critical systems and data following technology failures or cyber incidents, minimising service disruption and supporting timely resumption of essential services within regulatory thresholds.
B. Policy Requirements	10.44	A financial institution must establish a robust backup strategy and procedures covering lifecycle management, adequate backup copies, secure storage, encryption, periodic testing, and independent risk assessment.	Cohesity's Recovery Agent enables workloads to be recovered efficiently to meet appropriate RTOs. DataLock secures backup copies and retention periods. Replication and archival to on-premises or cloud locations is policy-driven. All backup data transfers are protected using TLS 1.2 encryption.
B. Policy Requirements	10.45	A financial institution shall establish tamper-proof backup and an isolated recovery environment to enable timely resumption of critical services in the event of destructive cyber-attacks such as ransomware.	Cohesity provides tamper-proof, immutable backups through an immutable file system and zero-trust cluster architecture. The solution enhances cyber resilience through MFA, Multi-Person Authorization (MPA), DataLock-based immutability, and malware scanning.
B. Policy Requirements	10.50 (g)	A financial institution must conduct a comprehensive risk assessment prior to cloud adoption addressing risks associated with exposure to cyber-attacks via cloud service providers.	Cohesity enables protection of workloads across cloud environments through a single management console. Cohesity Cyber Resiliency Consulting supports vendor-neutral risk assessment aligned with industry best practices.

Part	Clause	Clause Description	Cohesity's Mapping
B. Policy Requirements	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 solution supports Multi-Factor Authentication (MFA) to strengthen user authentication and protect access to critical systems data.
B. Policy Requirements	10.57 (b)	Anomalies are flagged for prompt investigations to contain any cyber incidents.	Cohesity supports prompt investigation and containment of cyber incidents by detecting and flagging anomalous activity within backup data, enabling timely identification of potential threats and appropriate incident response actions.
B. Policy Requirements	10.57 (c)	User activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years.	Cohesity supports audit and investigation requirements by logging user and administrative activities within the management platform. Activity logs can be retained for a minimum of three years to support audits, investigations, and regulatory compliance.
B. Policy Requirements	11.3 (e)	Timely detection of cybersecurity incidents through continuous surveillance and monitoring.	Cohesity enhances cybersecurity incident detection by continuously monitoring backup data for suspicious or anomalous activity, supporting timely identification of potential cybersecurity incidents.
B. Policy Requirements	11.13 (b)	Detection and analysis: Ensure effective processes for identifying points of compromise, assessing extent of damage and preserving sufficient evidence for forensics purposes.	Cohesity enables effective detection and analysis through continuous monitoring and anomaly detection. The platform supports identification of compromise, assessment of affected data, and preservation of immutable evidence. Cohesity Cyber Resiliency Consulting aligns with NIST SP 800-61, SANS 6-Step IR, and MITRE D3FEND frameworks.
B. Policy Requirements	11.13 (c)	Containment and eradication: Identify and implement remedial actions to prevent or minimise damage, contain and remove known threats, and resume business activities.	Cohesity enables effective containment and eradication by supporting rapid identification of affected data, isolation of compromised environments, and recovery from trusted, immutable backup copies.
B. Policy Requirements	11.13 (d)	Recovery: Implement multiple strategies including contingency plans as part of incident recovery to swiftly resume business operations and significantly enhance redundancy and resilience.	Cohesity enables multiple recovery and contingency strategies by supporting recovery from trusted, immutable backup copies across on-premises and cloud environments, with structured recovery methodology informed by globally recognized frameworks.
B. Policy Requirements	11.13 (e)	Post-incident activity: Conduct post-incident review incorporating lessons learned and develop long-term risk mitigations.	Cohesity enables effective post-incident review by preserving immutable evidence, providing visibility into incident impact, and supporting analysis of incident patterns. Cohesity Cyber Resiliency Consulting supports post-incident review incorporating lessons learned.
Appendix 5 Part B	1	A financial institution shall ensure all data-at-rest of PII and transaction data are securely protected and rendered unreadable to unauthorized access through robust encryption mechanisms.	Cohesity encrypts backup and archived data containing PII and transaction information using industry-standard encryption mechanisms. Secure key management integration ensures encryption controls remain effective and aligned with the institution's cryptography policies.
Appendix 5 Part C	1	A financial institution must ensure its SOC has adequate capabilities for proactive monitoring of its technology security posture, enabling detection of anomalous activities and appropriate responses.	Cohesity enhances SOC effectiveness by continuously monitoring backup data and forwarding detected events to SOC, SIEM, or XDR tools. Cohesity's CERT is a 24x7x365 resource available for emergency response support.

Part	Clause	Clause Description	Cohesity's Mapping
Appendix 5 Part C	2 (a)	Log collection and implementation of an event correlation engine with parameter driven use cases such as SIEM.	Cohesity centrally captures system, audit, and security events. These logs can be securely forwarded to external SIEM solutions to support event correlation and SOC-driven investigations using parameter-based correlation rules.
Appendix 5 Part C	2 (d)	Threat hunting.	Cohesity enables threat hunting by providing continuous monitoring and analytics across protected backup data to identify indicators of compromise. Cohesity Cyber Resiliency Consulting supports threat hunting practices including IoC hunting, proactive threat hunting, and forensic investigation.
Appendix 5 Part C	2 (f)	Provision of situational awareness to detect adversaries and threats including threat intelligence, monitoring IoCs, and advanced behavioral analysis to detect signature-less and file-less malware.	Cohesity enhances situational awareness by analyzing backup data using threat intelligence, IoCs, malware scanning and behavioral analytics to identify suspicious activity and advanced threats, including signature-less and file-less malware.
Appendix 10 Part A	1 (d)	A financial institution is responsible for protection of data stored in cloud irrespective of cloud service models and providers.	Cohesity enables financial institutions to uphold responsibility for cloud-stored data by delivering uniform backup, recovery, and security capabilities across different cloud service models and providers, maintaining direct oversight regardless of contractual delineation.
Appendix 10 Part B	5 (b)	A financial institution should ensure backup and restoration procedures are periodically tested to validate recovery capabilities, with frequency commensurate with system criticality and RPO.	Cohesity supports scheduled, policy-driven backups aligned with system criticality and defined RPOs. Recovery capabilities can be validated through restore exercises, while centralized monitoring provides visibility into backup success or failure.
Appendix 10 Part B	5 (c)	A financial institution should ensure sufficient backup and recovery of virtual machines and containers including point-in-time restore and replication to alternate recovery sites.	Cohesity protects virtual machines and containers through policy-based backups supporting point-in-time restoration. Replication and archival capabilities allow VM and container images to be made available at alternate or recovery sites.
Appendix 10 Part B	14 (d)	A financial institution should ensure CERT members are conversant with the CIRP covering cloud services to effectively activate it when incidents occur.	Cohesity enables CERT teams to support CIRP execution for cloud environments by providing visibility into security events and recovery readiness. Cohesity's own CERT and Cyber Resiliency Consulting support CERT readiness through advisory services and tabletop exercises.

Conclusion

Cohesity is well positioned to address RMIT because it provides a unified, policy-driven data protection and cyber recovery platform that enables financial institutions to demonstrate recoverability, control, and accountability across on-premises, hybrid, and multi-cloud environments.

Specifically, Cohesity supports RMIT objectives by:

- Ensuring reliable recovery of critical systems and data, with point-in-time restores, cross-site replication, and periodic recovery validation aligned to RPOs and system criticality.
- Strengthening cyber resilience against destructive attacks, through immutable backups, isolated recovery environments, threat detection, and clean recovery capabilities.
- Maintaining institutional accountability for cloud-stored data, providing consistent protection and recovery controls independent of cloud service providers.
- Improving governance, auditability, and operational visibility through centralized policy management, reporting, and monitoring.

Learn more at [Cohesity.com](https://cohesity.com)

© 2026 Cohesity, Inc. All rights reserved.

Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.

COHESITY

cohesity.com

1-855-926-4374

2625 Augustine Drive, Santa Clara, CA 95054

2000087-001-EN 5-2026