COHESITY

WHITE PAPER

Mapping the FISC Security Guidelines to Cohesity

How Cohesity addresses the 68 measures of the FISC Security Guidelines on Computer Systems for Financial Institutions, 13th Edition (March 2025), that apply to data protection, cyber resilience and recovery.

TABLE OF CONTENTS

Executive summary 3

Scope of this paper 4

Cohesity platform overview 5

Cyber resilience framework – FISC alignment 6

Platform components relevant to FISC 7

How to read the chapters that follow 7

Identify – know your assets and your data risk 8

Mapping – Identify (12 measures) 8

Protect – immutability, encryption and access control 10

DataLock modes 10

Encryption 10

Zero-trust architecture 10

Mapping – Protect (29 measures) 11

Detect – surfacing threats inside the protected estate 14

Detection capabilities 14

SIEM and SOC integration 15

Mapping – Detect (11 measures) 15

Respond – containing incidents and enabling clean response 17

Cohesity CERT 17

Mapping – Respond (5 measures) 17

Recover – restoring critical services with tested recovery 19

Four copies, one policy engine 19

Recovery execution and rehearsal 20

Mapping – Recover (11 measures) 20

Coverage summary 22

Cloud and hybrid deployments 22

Conclusion 23

Executive summary

The FISC Security Guidelines on Computer Systems for Financial Institutions are the de facto security baseline for Japan's financial sector. The 13th Edition, published in March 2025 by The Center for Financial Industry Information Systems, frames cybersecurity as a matter of national economic security and requires institutions to build safe, stable and resilient information systems that keep delivering critical services through cyber incidents, system failures and third-party disruption.

WHAT FISC REQUIRES	HOW COHESITY ANSWERS IT
Reliable, tested recovery of critical systems and data after failure, disaster and cyberattack	Instant mass restore, point-in-time recovery and Recovery Agent runbooks, proven by non-disruptive testing against defined RPO and RTO
Tamper-resistant, isolated backups that survive ransomware and destructive attack	Immutable SpanFS with DataLock WORM retention, and the network-isolated FortKnox cyber vault no single administrator can delete
Confidentiality, integrity and availability of data, with strong access control and encryption	AES-256 GCM under a FIPS 140-3 validated module, granular RBAC, MFA and Multi-Person Authorization on destructive actions
Documented contingency and incident-response plans that explicitly assume cyberattack	Clean-copy identification, quarantine of infected copies, rehearsable runbooks and Cohesity CERT on call 24x7x365
Governance, auditability and continuous validation of controls	Centralised Helios reporting, immutable audit logs, SIEM and SOAR integraiont, and recorded recovery-test evidence

68 measures maped • 57 basic, 11 additional • 67 of 68 apply on-premises and in cloud

Figure 1: What the 13th Edition requires of institutions, and the Cohesity capability that answers each requirement.

Cohesity maps to 68 FISC measures across the Control, Practice and Audit guideline families. 57 of those are Basic Guidelines—FISC's minimum expected level, applicable to every financial information system—and 67 of the 68 apply to on-premises and cloud deployments alike.

Cohesity is not simply a backup vendor. It is positioned as part of a broader operational resilience and cyber recovery strategy that helps financial institutions address FISC's core requirement: critical services and data must remain recoverable, resilient and defensible under attack.

Scope of this paper

This paper covers the 68 FISC measures that a data security and management platform can address—not the full standard. Facilities (F) measures and most network, endpoint, application-security and organisational-governance measures fall outside it. Coverage described here is platform capability that supports an institution in meeting a measure; responsibility for compliance rests with the institution, and actual coverage depends on the capabilities deployed, licensed and configured. The Identify / Protect / Detect / Respond / Recover grouping used throughout is presentational; FISC's own C / P / F / A families and its Basic and Additional designations are preserved unchanged.

Cohesity platform overview

Cohesity provides a unified, policy-driven data security and management platform that consolidates data protection, cyber resilience and recovery across on-premises, hybrid and multi-cloud environments. Protection policies, immutability, encryption, access control and reporting are defined once and applied consistently to virtual machines, physical servers, containers, databases, NAS and file systems, SaaS applications and cloud workloads.

That consistency is what makes the platform defensible under FISC review. Where copy management is split across several tools, each with its own retention semantics, access model and reporting, an institution cannot easily show an auditor that a control applies uniformly across the estate. Where one policy engine governs every copy, it can.



Figure 2: The Cohesity five steps to cyber resilience — the maturity model this mapping is organised by.

Cyber resilience framework – FISC alignment

Cohesity's approach to cyber resilience maps to the five phases of Identify, Protect, Detect, Respond and Recover. Each phase is supported by specific platform capabilities and consulting services, enabling institutions to build an auditable cyber resilience posture aligned to FISC. Representative FISC measures are shown beneath each phase.

Identify	Protect	Detect	Respond	Recover
12 measures	**29 measures**	**11 measures**	**5 measures**	**11 measures**
• Information-asset discovery • Data classification (PII, regulated) • Global index & catalogue • Third-party assurance evidence	• Immutable SpanFS with DataLock (WORM) • AES-256 GCM, FIPS 140-3 validated • RBAC, MFA, Multi-Person Authorization • FortKnox isolated cyber vault	• ML anomaly & entropy detection • Threat Protection IOC scanning • Mandiant threat library (24h refresh) • SIEM / SOAR event forwarding	• Clean-copy identification • Quarantine of infected copies • Isolated forensic restore • Cohesity CERT 24×7×365	• Instant mass restore • Recovery Agent runbook orchestration • Cross-site & cloud replication • Non-disruptive recovery testing
C5-1 · C5-2 · C7 · C24 · A1	P3 · P5 · P25 · P39 · P41	P14-1 · P21 · P32 · P38 · P46	P19 · P22 · P72 · P73-1 · A1-1	C5-4 · P71 · P73 · P103-1 · P106

Figure 3: Cohesity cyber resilience framework – FISC measure alignment. Measure counts are the totals mapped in each function; the codes shown are representative, not exhaustive.

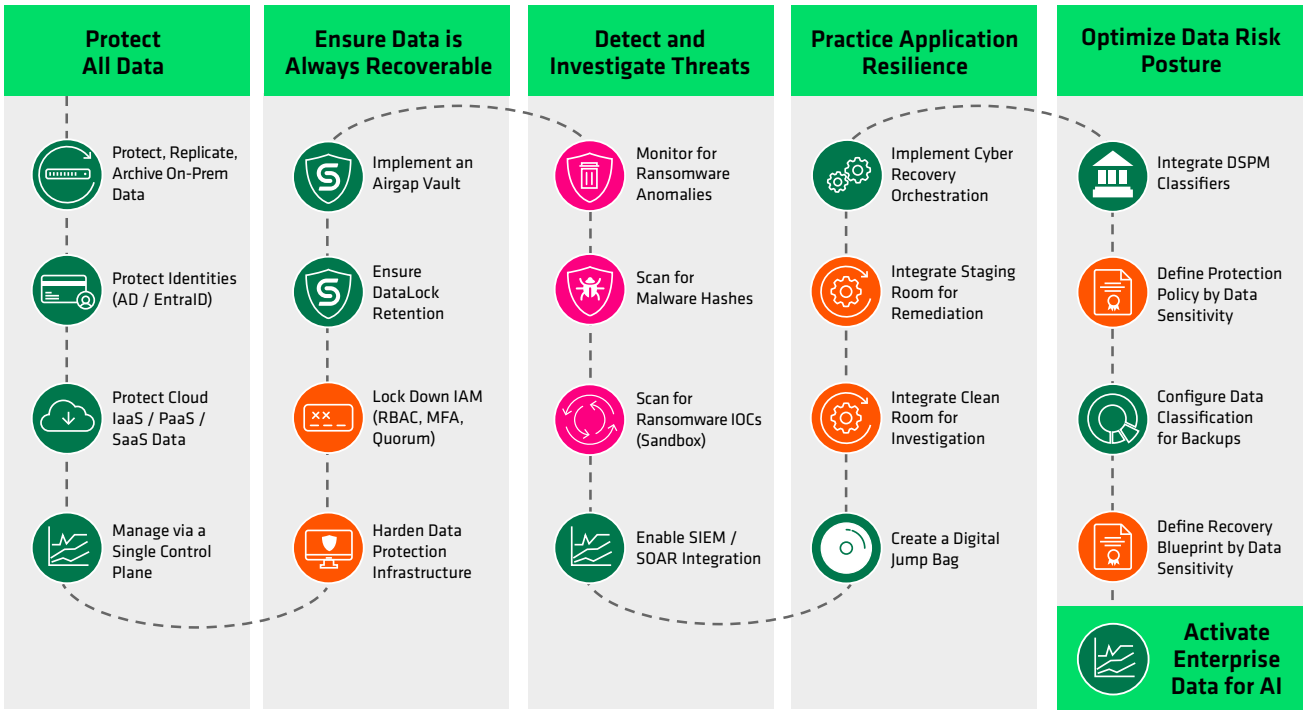


Figure 4: Where Cohesity capability, Cohesity scanners and the institution's own processes and technology meet across the five steps.

Platform components relevant to FISC

DataProtect	Policy-driven backup and recovery across VMs, physical servers, containers, databases, NAS and SaaS, with workloads auto-protected on discovery.
SpanFS with DataLock	Purpose-built distributed file system. Redirect-on-write so data is never overwritten in place; DataLock applies WORM retention that cannot be shortened, including by an administrator.
FortKnox cyber vault	Isolated, air-gapped vault reached only over a controlled, outbound-initiated path – the copy that survives when production and its everyday backups are compromised together.
Threat Protection	Scans backup snapshots for indicators of compromise using the Mandiant threat library from Google Threat Intelligence, custom YARA rules and custom or third-party hash feeds.
Anomaly detection	ML models flag abnormal change and deletion rates and entropy shifts that signal mass encryption, and identify the last known-good recovery point.
Recovery Agent	Captures recovery procedures as executable, versioned runbooks and orchestrates DR failover and application recovery to defined RTO and RPO.
Helios	Single management and reporting plane across on-premises, edge and cloud – SLA attainment, protection coverage, capacity, cluster health, security posture and immutable audit logs.
Zero-trust access	Granular RBAC, MFA, SAML/SSO, LDAP and Active Directory federation, and Multi-Person Authorization on destructive or retention-reducing operations.
Cohesity CERT	Cyber Emergency Response Team available 24×7×365 to support institutions when an anomaly or incident is detected. Mapped against measures P19, P22, P72 and P73-1.
Cyber Resiliency Consulting	Vendor-neutral advisory covering recovery strategy, cyber-recovery exercises, tabletop drills and incident-response readiness. Mapped against measures C5-4, C16 and P73-1.

How to read the chapters that follow

The five chapters that follow take one function each. Each sets out what FISC asks for and how the platform answers it, and then maps every FISC measure in that function to the capability that addresses it. Guideline type (Basic or Additional) and guideline area are FISC's own and are read directly from the mapping matrix; intent text is paraphrased for brevity—refer to the 13th Edition for authoritative wording. Together the five chapters cover all 68 measures.

Identify – know your assets and your data risk

FISC's Identify measures ask a question that sounds administrative and turns out to be hard: what data does the institution hold, how important is it, where does it live and who is accountable for it? Measure C5-1 requires institutions to classify information systems, hardware and software, stored data and networks by importance across their lifecycle. Measure C7 requires a data management system that enforces those properties, controls access rights and logs data usage.

This is where a protection platform has an unusual advantage. Because Cohesity already holds a copy of the protected estate, it can index and catalogue it globally and apply automated classification to discover sensitive and regulated data such as personal information. The institution learns where its high-importance data actually is, rather than where the asset register says it should be—which is the input the FISC risk assessment depends on.

The function also captures third-party and supply-chain risk. Measures C20, C24 and C28 concern outsourcing selection, cloud service use and supply-chain cybersecurity management. Where Cohesity is the contractor or the platform behind an outsourced service, the institution's due diligence can draw on published third-party assurance – SOC 2 and ISO 27001, FIPS 140-3 cryptographic module validation under the NIST CMVP, independent penetration testing and documented secure development practice. FISC contemplates the use of third-party assurance reports where direct verification by the institution is impractical.

Mapping — Identify (12 measures)

12 measures · 12 Basic, 0 Additional · all rows below are drawn from the Cohesity × FISC mapping matrix

FISC measure	Type	Guideline intent (paraphrased)	Cohesity capability mapping
C4-2 Internal control – Organisational structure	**Basic**	Monitor and check the cybersecurity management system; review its effectiveness and report to management.	Helios dashboards, protection-coverage and SLA reporting, recovery-test results and immutable audit logs give management and the CISO objective evidence that data-protection and cyber-recovery controls are operating as intended.
C5-1 Internal control – Organisational structure	**Basic**	Manage information assets to identify cybersecurity risks; classify systems, data and networks by importance across their lifecycle.	The platform indexes and catalogues protected data globally, and data classification automatically discovers sensitive and regulated data such as PII, so protection is prioritised by confidentiality, integrity and availability.
C5-2 Internal control – Organisational structure	**Basic**	Identify and assess cybersecurity risks and develop risk response plans.	Global indexing and classification reveal where sensitive and high-value data resides to inform the risk assessment, while immutable backups, isolation and tested recovery form a primary risk-response control for destructive attack.
C5-3 Internal control – Organisational structure	**Basic**	Establish procedures for managing vulnerabilities in hardware and software.	Cohesity runs a managed vulnerability and patch lifecycle for the platform, with independent penetration testing and security advisories with fixed releases, so the institution's own vulnerability process extends to the protection estate.

FISC measure	Type	Guideline intent (paraphrased)	Cohesity capability mapping
C7 Internal control – Organisational structure	**Basic**	Establish a data management system that ensures confidentiality, integrity and availability, controls access rights and logs data usage.	One policy-driven system across the enterprise: protection policies, granular RBAC, immutable storage and comprehensive audit logging, with global visibility and reporting through Helios.
C20 External control – Outsourcing management	**Basic**	When outsourcing, identify purpose and scope beforehand and define the procedures for selecting contractors.	Contractor selection and periodic re-evaluation can draw on published third-party assurance: SOC 2 and ISO 27001, FIPS 140-3 cryptographic module validation, independent penetration testing and secure development evidence.
C24 External control – Use of cloud services	**Basic**	Set up cloud security measures with cloud-specific risks considered, under a clear division of responsibility, verified through provider assurance reports.	Protection, immutability and recovery controls the institution owns and operates independently of the cloud provider, across on-premises, hybrid and multi-cloud, reducing reliance on contractual assurance alone.
C28 External control – Cybersecurity risk management	**Basic**	Properly manage cybersecurity risks, taking the supply chain into account.	As a supplier, Cohesity supports supply-chain risk management through published security posture, third-party assurance and secure development practice, and through provider-independent controls that reduce single-vendor concentration risk.
P14-2 Information security – Prevention of unauthorized access	**Basic**	Conduct vulnerability assessment and penetration testing.	Threat Protection scans recovery points for indicators of compromise using the Mandiant threat library, YARA rules and custom hash feeds. For the platform itself, independent penetration testing is available as assurance evidence.
P23 Common system operation – Documentation	**Basic**	Document and maintain manuals for normal operation.	Operating procedures are codified in the platform: protection policies, schedules, retention and RBAC definitions are declarative, exportable and version-tracked, and Helios reporting evidences that operations ran as documented.
P47 Management of various facilities – Resource management	**Basic**	Check the capabilities and usage of various resources.	Helios reports capacity, consumption, data-reduction and performance trends across the estate, with forecasting so capacity exhaustion is anticipated before it affects protection.
A1 ISystem auditing – System auditing	**Basic**	Establish system auditing structures.	Immutable audit logs, protection-coverage and compliance reporting, recovery-test records and explicit RBAC definitions give auditors a standing evidence base, with read-only auditor roles for review without operational privilege.

Protect – immutability, encryption and access control

A central requirement of the 13th Edition – measure P41, on backup copies of program files—is tamper-resistant backup held in multiple environments separated from the organisational network. The guideline unit is explicit that these arrangements must account for ransomware that searches out and deletes backups, making it the clearest point of alignment between FISC and immutable, air-gapped architecture.

Cohesity answers it at the filesystem level rather than by policy. SpanFS is redirect-on-write, so protected data is never overwritten in place, and DataLock applies WORM semantics for the duration of the retention period. A locked copy cannot be modified or deleted before retention expires —not by ransomware, and not by a platform administrator acting alone.

DataLock modes

Enterprise mode	Protects backup data during a pre-defined retention period using dual authorization. Two individuals with different RBAC levels must agree before any change is made.
Compliance mode	Renders storage fully immutable. No user, including root or administrative users, can delete data during the retention period.

Encryption

Data at rest is encrypted with AES-256 in Galois/Counter Mode using a FIPS 140-3 validated cryptographic module (NIST CMVP), addressing measures P3 and P83. Data in transit – including replication between clusters, to cloud and to the FortKnox vault—is protected with TLS, addressing P4. Data-encryption keys are themselves encrypted by key-encryption keys, are never stored or exposed in plaintext, and rotate on a configurable schedule with a 30-day default. Keys can be held in the built-in key manager or in an external KMIP-based manager or AWS KMS, so they can be isolated from the media they protect as measures P13 and P30 require.

Zero-trust architecture

FISC devotes a cluster of measures—P8, P9, P25, P26, P27, P35 and P36—to identification, authorisation and the separation of request from approval. Cohesity federates administrative identity through SAML/SSO, LDAP or Active Directory so accounts are governed centrally, enforces MFA on privileged access, and scopes every role to specific objects and actions. Multi-Person Authorization requires a second authorised approver before high-impact operations proceed: deleting protected data, lowering retention, altering immutability or changing policy. Every grant, change and revocation is written to a tamper-resistant audit log that can be streamed to SIEM, so contractor and third-party compliance under measure C22 is verified from evidence rather than self-reporting.

Mapping — Protect (29 measures)

12 measures · 12 Basic, 0 Additional · all rows below are drawn from the Cohesity × FISC mapping matrix

FISC measure	Type	Guideline intent (paraphrased)	Cohesity capability mapping
C22 External control – Outsourcing management	**Basic**	contractor staff comply with the rules, and check their state of compliance.	Minimum-necessary access for contractor and third-party staff: RBAC scoped to specific objects, identity federated through SSO, LDAP or AD, MFA, and Multi-Person Authorization. Every action is logged, so compliance is verified from evidence rather than self-reporting.
P3 Information security – Data protection	**Additional**	Prevent leakage of stored data; protect important and personal data with encryption so content cannot be read even if files are copied or media stolen.	Data at rest is encrypted with AES-256 in Galois/Counter Mode using a FIPS 140-3 validated cryptographic module (NIST CMVP), so backup contents remain unreadable if media or files are copied or stolen.
P4 Information security – Data protection	**Additional**	Prevent leakage of data in transit; protect important data with encryption against interception during transfer.	Traffic is encrypted with TLS. Replication between clusters, to cloud and to the FortKnox vault is encrypted, protecting backup and replication data as it moves between on-premises, remote and cloud environments.
P5 Information security – Data protection	**Basic**	Provide file access control; protect critical files from intentional or accidental destruction and unauthorized access.	Granular RBAC over data and management operations with least-privilege scoping, and immutable redirect-on-write SpanFS that prevents backup data being overwritten or destroyed, whether accidentally or maliciously.
P8 Information security – Prevention of unauthorized use	**Basic**	Set up functions of personal identification.	Individual users are identified for all platform and data access, with MFA enforced and integration with enterprise identity providers via SAML/SSO, LDAP and Active Directory so authentication follows the institution's standards.
P9 Information security – Prevention of unauthorized use	**Basic**	Prevent unauthorized use of IDs.	Every account is restricted to least-privilege roles, with password policy, session timeout and lockout after failed attempts. Multi-Person Authorization means a single compromised credential cannot delete data or weaken retention alone.
P10 Information security – Prevention of unauthorized use	**Basic**	Collect and retain access logs as audit trails for a required period, check them regularly, and protect them from falsification.	Administrative and data-access activity is recorded in tamper-resistant audit logs retained on the immutable platform and streamed to external SIEM or syslog such as Splunk and IBM QRadar.
P13 Information security – Prevention of unauthorized uset	**Additional**	Protect cryptographic keys on the devices and media that store them.	Keys are held in a built-in key manager or an external KMIP-based manager or AWS KMS, so they can be isolated from the media they protect. Data-encryption keys are themselves encrypted, never stored in plaintext, and rotate on schedule.
P15 Information security – Prevention of unauthorized access	**Basic**	Minimize the number of connected devices accessible from external networks.	The platform runs as a hardened appliance with a minimal service footprint, and the FortKnox vault holds copies in a network-isolated environment reached only over a controlled, outbound-initiated path.
P20 Information security – Measures against malicious programs	**Basic**	Preventive measures against malicious programs.	Threat Protection scans protected data, immutable WORM copies cannot be encrypted or deleted by ransomware, and infected recovery points can be quarantined so a clean copy is selected for restore.

FISC measure	Type	Guideline intent (paraphrased)	Cohesity capability mapping
P25 Common system operation – Management of access rights	**Basic**	Make access authority clear; identify authorized persons and limit them to the minimum necessary to prevent unauthorized use and tampering.	Granular RBAC with built-in and custom roles and least-privilege object scoping, plus Multi-Person Authorization so sensitive actions require multiple approvers. Combined with MFA and access logging, this both enforces and evidences the limit.
P26 Common system operation – Management of access rights	**Basic**	Take proper precautions so that passwords are not known to anyone other than the respective user.	Administrative identity is federated through SSO, SAML, LDAP or Active Directory so password policy is enforced centrally. MFA is required for privileged access, and authorisation can be revoked immediately if a credential is suspected compromised.
P27 Common system operation – Management of access rights	**Basic**	Authorize access and review access authorization.	Roles are explicitly defined, assigned and scoped to specific objects, and can be reviewed and reported through Helios. Audit logs record every grant, change and revocation, giving reviewers evidence for periodic re-authorisation.
P28 Common system operation – Data management	**Basic**	Define handling, storage periods, transfer and disposal for data files according to their importance.	Retention set by system importance, DataLock immutability and WORM so files cannot be deleted early, legal hold where required, secure disposal with an auditable record, encrypted replication for transfer, and RBAC control over export.
P30 Common system operation	**Basic**	Establish key management procedures covering generation, distribution, use, storage, rotation and compromise, including key backup and restoration.	Built-in AES-256 key management with rotation, and integration with external KMS or HSM via KMIP for centralised, standards-based key lifecycle control. Keys can be securely backed up and restored.
P35 Operation control – Operation management	**Basic**	Verify operator qualifications; confirm the person performing an operation is authorised to do so.	Qualification is verified technically rather than visually: identity federated through SSO, LDAP or AD, MFA enforced for privileged and remote access, and RBAC restricting each operator to the roles and objects their duties require.
P36 Operation control – Operation management	**Basic**	Define procedures for assignment and approval of operations; establish who may request an operation and who must approve it before it runs.	Multi-Person Authorization requires a second authorised approver before high-impact operations proceed, and RBAC separates who may request from who may approve. Routine work runs from approved policies, with changes recorded and attributable.
P39 Operation control – Data file management	**Basic**	Establish backup rules covering (a) requirements by importance, (b) isolation and protection of backup data, (c) integrity verification and (d) recovery tests.	Policy-based frequency and retention by system importance; immutable SpanFS with DataLock for isolation; continuously verified integrity with ML anomaly detection; and non-disruptive recovery testing – addressing each of the four elements.
P41 Operation control – Program file management	**Basic**	Save backup copies of program files using tamper-resistant backup in multiple environments separated from the organisational network, accounting for ransomware that searches for and deletes backups.	Under DataLock/WORM, locked copies cannot be modified or deleted before retention expires – including by a platform administrator. Data replicates to a separate cluster, to cloud and to the isolated FortKnox vault, plus tape or media archive.
P43 Operation control – Network configuration management	**Basic**	Save backup copies of network configuration information; protect device and virtual network configuration against illegal change, failure and disaster.	Configuration files and the data stores holding network and virtual-network configuration are protected with the same immutable, versioned backups and generation management used for data files, enabling reliable restoration.

FISC measure	Type	Guideline intent (paraphrased)	Cohesity capability mapping
P45 Operation control – Document management	**Basic**	Save backup copies of documents required for restoring operations, ideally with remote storage.	Recovery documentation stored as files or objects is held under immutable retention and replicated to remote sites, cloud and the vault. Recovery Agent captures the runbooks and recovery sequence so procedures stay current and executable.
P63 System usage – Transaction management	**Basic**	Keep a log of transaction operations performed from terminals and inspect the log.	Cohesity preserves rather than generates terminal journals. Journal files, operation records and centre-side logs are held under DataLock WORM retention so the inspected record set cannot be altered or deleted early. Legal hold supports long retention.
P69 System usage – Customer data protection	**Basic**	Define management and handling methods that maintain strict confidentiality of customer information throughout its lifecycle.	Encryption, RBAC and immutability protect customer data, and classification discovers sensitive information so handling follows importance. Masking, where required, is delivered by DataMasque – a separately licensed partner application.
P76 System development & modification – Development management	**Basic**	Establish proper test environments.	Test and development environments are provisioned directly from backup snapshots using instant zero-space clones, so test data is production-realistic without capacity overhead, and clones are torn down when testing completes.
P79 System development & modification – Document management	**Basic**	Define procedures for storing and managing documents during development and modification.	Repositories holding development documents are protected with policy retention, DataLock WORM immutability, AES-256 encryption at rest, and RBAC with Multi-Person Authorization over deletion and recovery. Every access is logged.
P82 System development & modification – Disposal of systems	**Basic**	Develop a system disposal plan and procedure.	Retention and lifecycle policies define when protected data is disposed of, while legal hold and DataLock prevent premature deletion, so disposal follows an enforced schedule. Node and cloud-instance decommissioning is recorded in the audit trail.
P83 System development & modification – Disposal of systems	**Basic**	Prevent information leaks during system disposal.	All data at rest is encrypted with AES-256 GCM using a FIPS 140-3 validated module, and keys are never stored in plaintext, so residual data on retired media is unreadable. Secure drive erase and node clean-up are documented, support-guided procedures.
P99 System reliability – Operational reliability	**Additional**	Automate and simplify operations.	Declarative, policy-driven protection replaces manual backup administration: workloads inherit protection automatically on discovery, and REST APIs allow protection to be provisioned as code – reducing the operator error this measure targets.
P140 Individual operations and services – Biometric authentication	**Additional**	Implement security controls for biometric information: encryption, key management, restricted access, separated backup media, retention and secure deletion.	Where biometric templates are held as data, every copy is encrypted with AES-256 GCM under a FIPS 140-3 validated module with keys the institution controls. RBAC, MFA and MPA restrict access, copies can be held on isolated media, and retention enforces secure disposal.

Detect – surfacing threats inside the protected estate

FISC measure P14-1 asks institutions to employ monitoring and analysis to discover a clue of cyberattack—to detect anomalies and indicators of compromise and report them. Measure P21 asks for multiple solutions to detect intruding or embedded malware and to verify system validity. Most detection investment sits at the endpoint, the network edge and the SIEM; the backup estate is a blind spot in many programmes, and it is precisely where a patient attacker operates.

Detection capabilities

Anomaly detection	ML models continuously analyse backup metadata and job patterns, flagging abnormal change and deletion rates and entropy shifts that signal mass encryption. Addresses P14-1 and P98.
Threat Protection scanning	Backup snapshots scanned against the built-in Mandiant threat library from Google Threat Intelligence, refreshed every 24 hours, plus custom YARA rules and hash hunts across custom and third-party feeds. Addresses P20, P21 and P32.
Clean-copy identification	Points in time can be compared to establish when a discrepancy first appeared, determining the last known-good state before infection. Addresses P22 and P98.
Integrity verification	Checksums and end-to-end verification detect corruption or tampering between source, storage and replication targets. Addresses P7 and P100.

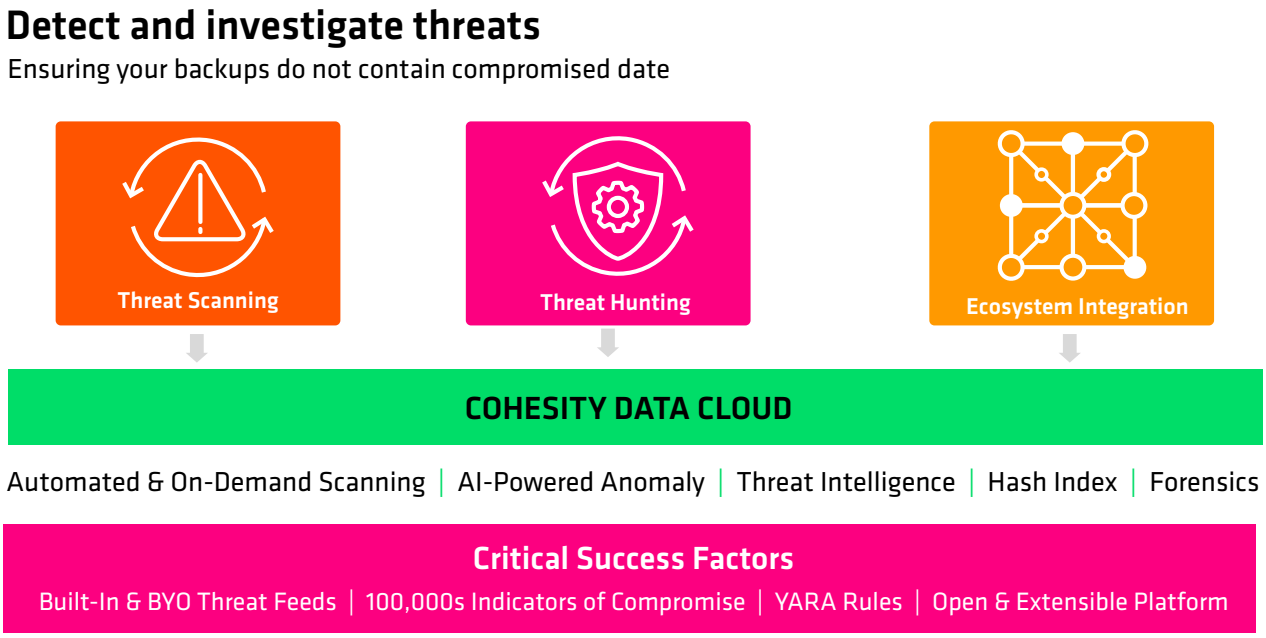


Figure 5: Threat scanning, threat hunting and ecosystem integration applied to backup data, so recovery points are known clean before they are restored.

SIEM and SOC integration

Cohesity events, alerts and audit logs are forwarded to external SIEM and SOAR platforms including Splunk and IBM QRadar, so detections from the data layer are correlated alongside endpoint and network telemetry. Audit logs are retained on the immutable platform, giving the falsification-resistant trails measure P10 requires for periodic review and investigation.

Helios provides the operational monitoring FISC asks for under measures P38, P46, P100 and P102: a single plane across on-premises, edge and cloud covering job success and failure, SLA attainment, capacity, cluster health and security posture, with proactive alerting on failed, missed or partially completed jobs. Every protection, replication, archival and recovery run is recorded with start and end time, objects processed, counts and completion status—the reconciliation of scheduled work against work actually completed that P38 calls for.

Mapping — Detect (11 measures)

11 measures · 8 Basic, 3 Additional · all rows below are drawn from the Cohesity × FISC mapping matrix

FISC measure	Type	Guideline intent (paraphrased)	Cohesity capability mapping
P7 Information security – Data protection	**Additional**	Detect tampered transmitting data.	Integrity of protected data is verified end to end, detecting corruption or tampering between source, storage and replication targets, with TLS protecting data in transit against undetected modification.
P14-1 Information security – Prevention of unauthorized access	**Basic**	Employ monitoring and analysis to discover a clue of cyberattacks; detect anomalies and indicators of compromise, and report them.	Machine-learning anomaly detection runs continuously over backup data, surfacing abnormal change and deletion rates and entropy changes that signal encryption. Alerts and IoCs are raised to administrators and forwarded to SIEM and SOAR.
P16 Information security – Detect unauthorized access	**Basic**	Provide monitoring of unauthorized access; record access errors and detect unauthorized access at an early stage.	Access errors and administrative activity are monitored and logged, with account lockout, MFA enforcement and alerting on suspicious access patterns. Events stream to SIEM for correlation.
P21 Information security – Measures against malicious programs	**Basic**	Use multiple solutions to detect intruding or embedded malware and verify system validity.	Threat Protection provides native on-platform anti-malware scanning plus YARA-rule threat hunting and curated threat intelligence, identifying infected or compromised copies before recovery and validating the integrity of protected systems.
P32 Common system operation – Measures against viruses	**Basic**	Take measures against computer viruses.	Threat Protection scans backup snapshots using the Mandiant threat library from Google Threat Intelligence, refreshed every 24 hours, with custom YARA rules and hash hunts. Matches surface in Security Center with a threat-protection score.
P38 Operation control – Operation management	**Basic**	Record what was actually executed so it can be compared against what was scheduled.	Every protection, replication, archival and recovery run is recorded with time, objects processed, counts and status. Helios consolidates run history and SLA attainment and alerts on failed, missed or partially completed jobs.
P46 Operation control – Operation monitoring	**Basic**	Establish a monitoring system for system operation.	Helios provides a single monitoring plane across on-premises, edge and cloud – job success and failure, SLA adherence, capacity, cluster health and security posture – with proactive alerting and forwarding to external SIEM and SOAR tools.

FISC measure	Type	Guideline intent (paraphrased)	Cohesity capability mapping
P98 System reliability – Software quality	**Additional**	Provide file-matching functions; detect inconsistencies between files early, including those caused by program error or falsification.	ML anomaly detection across successive backups flags unexpected change rates, entropy shifts and mass modification. Points in time can be compared to establish when a discrepancy first appeared. Business-level reconciliation between ledgers and journals sits outside the platform.
P100 System reliability – Operational reliability	**Basic**	Reinforce the functions of checking operations.	Every protection job is verified and reported – success and failure status, SLA compliance, backup integrity checks and non-disruptive recovery tests – providing an independent check rather than inferring success from the absence of errors.
P102 System reliability – Failure detection & recovery	**Basic**	Monitor the operational conditions of a system.	Helios continuously monitors cluster and node health, capacity, performance, job state and security posture across on-premises and cloud, with proactive alerting and event forwarding to external SIEM and SOAR tools.
P103 System reliability – Failure detection & recovery	**Additional**	Detect failures and isolate points of failure.	The platform detects component, node and job failures, isolates the affected element and continues operating on the remaining nodes, self-healing once the fault clears, with alerts and logs identifying the point of failure.

Respond – containing incidents and enabling clean response

The Respond measures are few but consequential. Measure P19 requires defined response and recovery procedures that prevent the spread of an intrusion and set out recovery from damage. Measure P22 addresses cases involving damage from malicious programs. Measure P72 requires institutions to identify and analyse the causes of system failures. Measure P73-1 requires incident response and contingency plans that explicitly assume ransomware and destructive attack. Measure A1-1 requires internal audits of cybersecurity, including of response and recovery status and the remediation of identified issues.

The hardest question in a real ransomware response is not how to restore. It is what to restore from. An institution that cannot establish the last known-good state faces a choice between an old copy with unacceptable data loss and a recent copy that may reintroduce the attacker. Cohesity narrows that gap: anomaly detection and Threat Protection help establish the point of infection, clean-copy identification finds the last uncompromised recovery point, infected copies are quarantined so they cannot be selected by mistake, and recovery proceeds from the isolated vault.

For root-cause analysis under P72, a point-in-time copy can be restored into an isolated environment so a compromised system is examined forensically without touching production. For A1-1, the audit evidence is generated by the system rather than assembled by the team being audited.

Cohesity CERT

Cohesity's Cyber Emergency Response Team is available 24×7×365 to support institutions when an anomaly is detected, supporting the response and recovery procedures required under measures P19 and P22 and the incident-response planning required under P73-1.

Mapping — Respond (5 measures)

5 measures · 5 Basic, 0 Additional · all rows below are drawn from the Cohesity × FISC mapping matrix

FISC measure	Type	Guideline intent (paraphrased)	Cohesity capability mapping
P19 Information security – Response to unauthorized access	**Additional**	Define response and recovery procedures that prevent the spread of an intrusion, and recovery-from-damage procedures.	The latest clean, uncompromised copy is identified and used for rapid recovery of affected systems and data. Immutable copies isolated in the cyber vault remain available even if production is compromised. Cohesity CERT supports escalation 24×7×365.
P22 Information security – Measures against malicious programs	**Basic**	Measures for cases involving damage from malicious programs.	Threat Protection and anomaly detection help establish the point of infection, clean-copy identification finds the last uncompromised recovery point, infected copies are quarantined, and clean recovery restores from the isolated vault without reintroducing the malware, with Cohesity CERT providing emergency response support.

FISC measure	Type	Guideline intent (paraphrased)	Cohesity capability mapping
P72 Emergency response – Failure & disaster	**Basic**	Identify and analyse the causes of system failures.	Detailed job, system and audit logs, health telemetry and alert history supply the evidence root-cause analysis depends on, and a point-in-time copy can be restored into an isolated environment for forensic examination without touching production. Cohesity CERT assists with investigation and escalation.
P73-1 Emergency response – Contingency plans	**Basic**	Develop incident response and contingency plans that assume cyberattacks including ransomware and destructive attacks, defining response priorities, target recovery times and levels, and periodic review.	Immutable air-gapped copies, ML ransomware detection, clean-copy identification and Recovery Agent orchestration let institutions execute and test the recovery portion of cyber incident-response plans against defined RTO and RPO targets. Cyber Resiliency Consulting supports plan development and periodic review, and Cohesity CERT is available when the plan is invoked.
A1-1 System auditing – System auditing	**Basic**	Conduct internal audits of cybersecurity; audit maintenance, operation, response and recovery status, and grasp remediation of identified issues.	Centralised Helios reporting, dashboards, immutable audit logs and compliance/ protection reporting give internal audit objective evidence of coverage, recovery testing, access control and response and recovery status.

Recover – restoring critical services with tested recovery

If one theme carries the weight of the 13th Edition, it is recovery – and specifically recovery that has been tested rather than assumed. FISC asks for definitive recovery measures coordinated with the contingency plan, contingency plans that assume ransomware and destructive attack, backup centres for risk dispersion that are mandatory in principle for critical settlement systems, and verification that redundant and backup structures actually function. It also requires that staff rehearse the procedures they will have to execute. The measures are set out in full below.

Four copies, one policy engine

FISC's backup and recovery measures collectively describe a copy posture stronger than a conventional 3-2-1 rule: four distinct copies with four distinct jobs, all governed by one policy engine, one immutability model and one model of RBAC, MFA and Multi-Person Authorization.

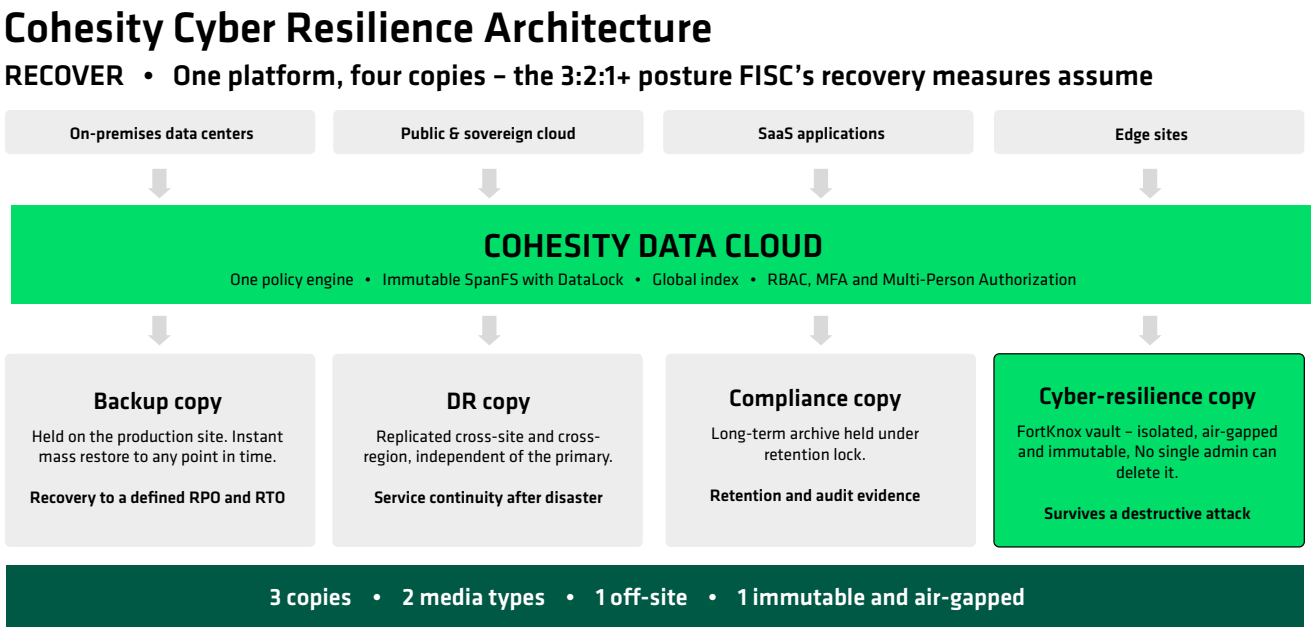


Figure 6: One platform, four copies. The vault copy is what makes recovery defensible when production and its everyday backups are compromised together.

Recovery execution and rehearsal

Instant mass restore	Returns large numbers of VMs, files and databases to service; point-in-time, file-level and application-consistent recovery. Addresses P106.
Granular, priority-sequenced recovery	Only the affected component is restored, sequenced by business priority, so critical services return first while lower-priority operations stay suspended – the degraded-mode continuation P104 contemplates.
Recovery Agent runbooks	Recovery procedures captured as executable, versioned runbooks covering sequence, dependencies, target environment and validation steps, so the failure and disaster manual required by P24 is tested and current rather than a static document.
Non-disruptive recovery testing	Drills and clean-room restores run against isolated targets using zero-space clones, without disturbing live workloads. Results, timings and outcomes are recorded and reportable as evidence against recovery objectives. Addresses C5-4, C16, P39 and P103-1.
Geographic and logical dispersion	Replication to alternate sites, to public and sovereign cloud, and to the isolated FortKnox vault provides the dispersed, network-isolated copies P74 contemplates for critical settlement services.

The same capabilities apply outside incident scenarios. Measures P77 and P96 require a fallback path for production transitions and a held pre-change state: an immutable copy is taken immediately before cutover, and the rollback itself can be rehearsed and timed before it is needed under pressure. Cohesity Cyber Resiliency Consulting supports the organisational side—recovery strategy, cyber-recovery exercises and tabletop drills for C5-4 and C16.

Mapping — Recover (11 measures)

11 measures · 8 Basic, 3 Additional · all rows below are drawn from the Cohesity × FISC mapping matrix

FISC measure	Type	Guideline intent (paraphrased)	Cohesity capability mapping
CS-4 Internal control – Organisational structure	**Basic**	Conduct exercises and training on cybersecurity; carry out drills that assume cyberattacks and verify response and recovery readiness.	Non-disruptive recovery drills and clean-room restores in an isolated environment rehearse recovery from ransomware and destructive attack, validate RTO and RPO, and prove the recovery portion of incident-response plans. Cyber Resiliency Consulting complements the drills with tabletop exercises and scenario design.
C16 Internal control – Personnel (staffing and training)	**Basic**	Provide education and training for possible failures and disasters; rehearse the response and recovery procedures staff will have to execute.	Recovery Agent runbooks can be rehearsed against isolated recovery targets, and zero-space clones stand up production-like environments without disturbing live workloads. Test results are recorded and reportable, and Cyber Resiliency Consulting supports staff readiness.
P24 Common system operation – Documentation	**Basic**	Prepare manuals used in case of failure or disaster.	Recovery Agent captures recovery procedures as executable runbooks – sequence, dependencies, target environment and validation steps – so the manual is tested and current. Runbooks are versioned and recovery documentation is protected immutably.
P71 Emergency response – Failure & disaster	**Basic**	Define definitive recovery measures, including switching to redundant or backup systems, coordinated with the contingency plan.	Instant mass restore, point-in-time recovery and cross-site or cloud replication, with Recovery Agent orchestrating and automating DR failover and application recovery to restore critical systems within target times.

FISC measure	Type	Guideline intent (paraphrased)	Cohesity capability mapping
P73 Emergency response – Contingency plans	**Basic**	Formulate contingency plans prepared in advance to minimise damage and enable prompt recovery from disasters, accidents, failures and cyberattacks.	Recovery Agent provides tested, automatable recovery workflows and runbooks, with replication to alternate sites and cloud and defined RPO/RTO policies. Non-disruptive testing validates that plan assumptions still hold.
P74 Emergency response – Backup centers	**Additional**	Establish backup centres; maintain an alternate site for risk dispersion and business continuity, mandatory in principle for critical settlement systems.	Replication to alternate sites, to public and sovereign cloud, and to the isolated FortKnox vault provides geographically dispersed, network-isolated copies from which critical systems can be recovered if the primary data centre is lost.
P77 System development & modification – Development management	**Basic**	Define procedures for transition to production, including the fallback path if the transition fails.	An immutable copy of the outgoing environment is taken immediately before cutover, so the previous state can be restored quickly if the transition fails. Zero-space clones let transition tests be rehearsed against realistic data.
P96 System reliability – Software quality	**Basic**	Maintain software quality after changes or added functions; hold the pre-change state as a backup and establish recovery procedures before the change.	An immutable point-in-time copy of the affected systems is captured ahead of the change window, so the pre-change state can be restored if quality degrades. Executable runbooks let the rollback be tested and timed beforehand.
P103-1 System reliability – Failure detection & recovery	**Additional**	Verify and test that backup and redundant structures actually work, reducing the chance both production and backup are lost to one attack.	Regular non-disruptive recovery testing, automatable with Recovery Agent, proves backups are recoverable before an incident. Immutable isolated copies in the cyber vault reduce the risk that production and backup are compromised simultaneously.
P104 System reliability – Failure detection & recovery	**Additional**	Provide functions for reduction, shutdown and rearrangement of business operations on failure; continue in degraded mode rather than stopping entirely.	Only the affected component is restored – granular recovery at file, object, VM, database and application level – with runbooks sequencing recovery by business priority so critical services return first. Recovery can be directed to an alternative site or cloud.
P106 System reliability – Failure detection & recovery	**Basic**	Provide recovery functions that shorten recovery time and minimise operational impact, with file and point-in-time recovery capabilities.	Instant mass restore of VMs, files and databases, point-in-time and file-level recovery, and application-consistent restores, with Recovery Agent automating and orchestrating the recovery sequence from verified backup copies.

Coverage summary

Cohesity maps to 68 FISC measures spanning 12 FISC guideline category bands within the Control, Practice and Audit families. The table below summarises coverage by function.

Function	Measures	Basic / Additional	Primary Cohesity capability	Key differentiator
Identify	**12**	12 / 0	Data classification · global index · Helios reporting · third-party assurance	Discovery of where high-importance data actually is
Protect	**29**	24 / 5	SpanFS with DataLock · AES-256 GCM (FIPS 140-3) · RBAC, MFA, MPA · FortKnox	Immutability no administrator can override
Detect	**11**	8 / 3	ML anomaly detection · Threat Protection · Mandiant library · SIEM/SOAR	Detection inside the backup estate, not just at the edge
Respond	**5**	5 / 0	Clean-copy identification · quarantine · isolated forensic restore · CERT	Knowing which copy is clean before restoring
Recover	**11**	8 / 3	Instant mass restore · Recovery Agent runbooks · replication · recovery testing	Recovery proven by test, with recorded evidence
Total	**68**	57 / 11	One policy engine across on-premises, hybrid and multi-cloud	67 of 68 apply to both on-premises and cloud

Cloud and hybrid deployments

Section 3.3 of the 13th Edition sets out additional considerations where financial services run on cloud infrastructure. Sixty-seven of the 68 measures mapped here apply to on-premises and cloud deployments alike; only C24, on the use of cloud services itself, is cloud-specific. The Section 3.3 rating carried by each individual measure is recorded in the companion matrix.

The practical consequence is a division-of-responsibility problem. Cloud providers offer durable storage, snapshots and regional redundancy, and publish assurance reports describing them. But the controls FISC most insists on at the data layer—immutability that resists a compromised administrator, isolation from the production network, tested recovery to a defined objective, and evidence of all three—are ones the institution is expected to retain. Cohesity sits deliberately on the institution's side of that line: one control model across the estate, provider-independent recovery, and third-party assurance the institution can use in its own due diligence under C20 and C24.

Conclusion

The 13th Edition asks Japanese financial institutions to plan for the failure of prevention: to hold backups an attacker with administrative credentials cannot destroy, to know which copy is clean, to recover critical services within objectives they have committed to, and to show the working.

Cohesity is well positioned to address FISC 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 FISC objectives by:

- **Ensuring reliable recovery of critical systems and data**, with instant mass restore, point-in-time and file-level recovery, cross-site and cloud replication, and periodic recovery validation aligned to RPO, RTO and system criticality.
- **Strengthening cyber resilience against destructive attacks,** through immutable SpanFS with DataLock, the FortKnox isolated cyber vault, air-gapping, ML-based ransomware detection and clean recovery.
- **Protecting data confidentiality and integrity,** with AES-256 encryption at rest and in transit, granular RBAC, MFA, Multi-Person Authorization and immutable audit logging.
- **Maintaining institutional accountability for cloud-stored data,** providing consistent protection and recovery controls independent of the cloud service provider.
- **Improving governance, auditability and operational visibility**, through centralised Helios policy management, reporting and monitoring, with SIEM and SOAR integration that supports system audits and regulatory review.

Positioned as the last line of defence, Cohesity helps financial institutions meet FISC's core requirement: critical services and data must remain recoverable, resilient and defensible even under cyberattack.

Source: FISC Security Guidelines on Computer Systems for Financial Institutions, 13th Edition, March 2025, The Center for Financial Industry Information Systems. Measure text in this paper is paraphrased for brevity – refer to the 13th Edition for authoritative wording. The English translation is unofficial; only the Japanese text is authoritative, and the institution's compliance team should validate wording. Companion materials: Cohesity_FISC_13thEd_Mapping_Deck_v1.1.pptx and Cohesity_FISC_13thEd_Mapping_Matrix_v1.1.xlsx.

This material is intended to provide information about Cohesity and our business and products. It does not constitute legal, regulatory or audit advice and does not certify compliance; responsibility for compliance with the FISC Security Guidelines rests with the financial institution. Capability described depends on the deployment, licensing and configuration in use. Data masking referenced under measures P69 and P76 is delivered by the DataMasque partner application running on Cohesity, a separately licensed integration. Product names and third-party marks are the property of their respective owners.

© 2026 Cohesity, Inc. All rights reserved.
Cohesity, the Cohesity Logo, and other Cohesity Marks are trademarks of Cohesity, Inc. or its affiliates in the US and/or internationally. Other names may be trademarks of their respective owners. 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

2000104-001-EN 8-2026