Cyber Recovery Maturity Model Standard

Cyber Recovery Authority (CRA)

CRMM Version 1.0

Document Control

Item	Detail
Title	CRA Cyber Recovery Maturity Model Standard
Version	1.0
Status	Published
Publisher	Cyber Recovery Authority (CRA)
Owner	Standards & Assurance Division, CRA
Classification	Public Standard
Effective Date	January 2025
Review Cycle	Annual
Next Review Date	January 2026
Supersedes	N/A
Contact	standards@cyberrecoveryauthority.org

Copyright Notice

Contents

Cyber Recovery Maturity Model Standard 1
Document Control 2
Copyright Notice 3
Contents 4
1. Foreword 7
2. Introduction 8
3. Scope 9
3.1 In Scope 9
3.2 Out of Scope 9
4. Normative References 10
Regulatory & Industry Standards 10
Regulatory Guidance 10
Technology-Specific References 11
CRA Reference Materials 11
5. Terms and Definitions 12
5.1 Cyber Recovery 12
5.2 Recovery Environment (RE) 12
5.3 Clean Zone 12
5.4 Immutable Backup 12
5.5 Recovery Pipeline 12
5.6 Loss-of-Trust Event 12
5.7 Recovery Pattern 12
5.8 Evidence Artefact 12
5.9 Independence of Control 12
5.10 Recovery Test 12
5.11 Recovery Readiness 13
5.12 Critical Data Class (CDC) 13
5.13 Orchestration Layer 13
5.14 Recovery Assurance 13
5.15 Authoritative Data Source 13
5.16 Recovery Safety Check 13
5.17 Control Plane 13
5.18 Gold Image 13

5.19 Recovery Governance Board 13
5.20 Triggering Event 13
6. Symbols and Abbreviations 14
7. Cyber Recovery Maturity Model Overview 15
7.1 Purpose of the Model 15
7.2 Model Structure 15
7.3 Model Philosophy 15
7.4 Intended Use Cases 16
7.5 Relationship to Disaster Recovery (DR) 16
8. Maturity Levels 17
Level 1: Initial / Ad Hoc 17
Level 2: Defined and Basic 17
Level 3: Assured and Repeatable 17
Level 4: Resilient and Automated 18
9. Assessment Domains 19
9.1 Domain 1: Recovery Architecture 19
9.2 Domain 2: Backup, Storage & Data Integrity 19
9.3 Domain 3: Identity & Access Separation 20
9.4 Domain 4: Recovery Orchestration & Tooling 20
9.5 Domain 5: Testing & Validation 20
9.6 Domain 6: Governance & Operating Model 21
10. Domain Criteria 22
10.1 Domain 1: Recovery Architecture 22
10.2 Domain 2: Backup, Storage & Data Integrity 23
10.3 Domain 3: Identity & Access Separation 24
10.4 Domain 4: Recovery Orchestration & Tooling 25
10.5 Domain 5: Testing & Validation 25
10.6 Domain 6: Governance & Operating Model 26
11. Assessment Method 28
11.1 Stage 1: Assessment Plan 28
11.2 Stage 2: Evidence Register 28
11.3 Stage 3: Domain Assessment Records 29
11.4 Stage 4: Validation Statement 29
11.5 Stage 5: CRMM Assessment Report 29

12. Evidence Catalogue 30
12.1 Evidence Category Definitions 30
12.2 Evidence Requirements by Domain 30
ANNEX A: ASSESSMENT TEMPLATES A1. Assessment Overview 33
A2. Domain Assessment Form 35
A3. Evidence Register 36
A4. Final Maturity Summary 37
Annex B: Example Recovery Pattern 39
B.1 Pattern Overview 39
B.2 Phase 1: Identity Reconstruction 39
B.3 Phase 2: Platform & Control Plane Rebuild 40
B.4 Phase 3: Application & Data Recovery 40
B.5 Phase 4: Service Validation & Promotion to Production 41
B.6 Pattern Characteristics 41
B.7 Conceptual Recovery Flow 42
Annex C: Scoring 43
C.1 Interpretation of Levels 43
C.2 Domain Weighting Guidance 43
C.3 Rating Confidence Levels 44
C.4 Determining Overall Posture 44
C.5 Gap Analysis 44
C.6 Uplift Prioritisation Framework 44
C.7 Regulatory Alignment 45
C.8 Scorecard Template 45
Cyber Recovery Authority (CRA) 46
Copyright Statement 46
Licensing 46
Contact for Licensing, Accreditation, and Feedback 46
Document Status 46
Trademarks 46
Disclaimer 47
End of Standard 47

1. Foreword

The Cyber Recovery Authority (CRA) was established to support consistent assessment of organisational cyber recovery capability against destructive cyber events. As adversaries increasingly target identity infrastructure, control planes, backup systems and recovery tooling, traditional disaster recovery frameworks are no longer sufficient to ensure safe restoration of business services.

The Cyber Recovery Maturity Model (CRMM) provides an evidence-based method for assessing an organisation's readiness to recover from loss-of-trust cyber scenarios.

It has been developed with the following objectives:

- To define a common language for cyber recovery capability
- To provide a measurable model aligned with modern threat patterns
- To support regulator, auditor, and board-level assessment
- To guide organisations in prioritising investments toward assured recovery
- To drive convergence toward standardised patterns and governance

This first edition of the CRA Cyber Recovery Maturity Model reflects extensive analysis of industry incidents, architectural patterns, recovery testing practices, and international regulatory standards. It will evolve in future editions as threats, technologies, and global regulatory expectations continue to develop.

CRA welcomes feedback and contributions from practitioners, assessors, and regulators.

Acknowledgements

The CRA would like to thank contributors from the cyber resilience, architecture, disaster recovery, and crisis management communities who provided insights, case studies, and validation across financial services, critical national infrastructure, cloud providers, and regulatory bodies.

How to Use This Document

This document is intended to be used by:

- Cyber resilience and operational risk teams
- Architects and engineering leads
- Disaster recovery and business continuity professionals
- Security operations and incident response teams
- Regulators and auditors assessing recovery readiness

It defines:

- The CRA maturity levels
- The six assessment domains
- The detailed criteria for each level
- The assessment and evidence requirements
- Supporting annexes, templates, and rubrics

Assessment outputs may be used for internal improvement, external assurance, vendor evaluation, or regulatory reporting.

2. Introduction

Modern destructive cyber incidents create conditions fundamentally different from traditional disaster recovery scenarios. These events frequently involve corruption or compromise of:

- Directory services
- Hypervisor or virtualisation stacks
- Backup repositories
- Automation pipelines
- Orchestration tools
- Privileged credentials
- Management networks

The result is a *loss of trust* in some or all components of the production environment, rendering traditional recovery approaches insufficient or unsafe.

The Cyber Recovery Maturity Model (CRMM) reflects increasing regulatory expectations for demonstrable cyber-resilience, including clean recovery, identity rebuild capability, and isolation of recovery tooling. The CRMM provides a structured method for assessing readiness to restore services following high-impact cyber events where data integrity, identity infrastructure, or underlying control planes may be compromised.

The model:

- Breaks cyber recovery capability into **six domains**
- Defines **four levels of maturity**
- Provides **detailed criteria** for each domain × level
- Establishes **evidence requirements** to support audit or regulatory assurance
- Supports a **repeatable, scoring-neutral assessment method**

CRMM is designed to complement, not replace, business continuity, resilience, and disaster recovery frameworks. It focuses specifically on **technical recoverability under cyber-compromise conditions**, and the ability to reconstruct a trusted operational environment with controlled, assured processes.

Mandatory vs Advisory Content:

- Sections 3-9 of this document are normative and define the requirements for CRMM assessment.
- Sections 1-2 and 10-11 are informative and support interpretation.

3. Scope

3.1 In Scope

This standard applies to all organisations seeking to evaluate or demonstrate their ability to recover from destructive cyber events, including those affecting:

- Identity and authentication systems
- Virtualisation platforms and hypervisors
- Backup and replication systems
- Storage and data protection layers
- Application hosting environments (on-premises or cloud)
- Network infrastructure required for recovery
- Control-plane tooling and management services
- Operational data required for service restoration

The scope includes:

- Architectural design of cyber recovery environments
- Control mechanisms ensuring clean, assured recovery
- Backup patterns and immutability requirements
- Recovery workflows and orchestration
- Separation of duties and governance
- Evidence and artefacts demonstrating capability

The model is applicable to:

- Financial institutions
- Government and critical infrastructure
- Cloud service providers
- Managed service providers
- Enterprises with complex production workloads

3.2 Out of Scope

The following areas are **not** evaluated directly by this standard:

- Business continuity planning (unless directly relevant to technical recovery)
- Crisis communications and crisis management
- Physical disaster recovery unrelated to cyber compromise
- Traditional RTO/RPO-based DR metrics
- Information security controls unrelated to recovery capability
- Legal and regulatory breach notification processes
- Cyber insurance requirements

While these areas may influence recovery outcomes, CRMM focuses exclusively on **technical reconstruction of a trusted environment after a destructive or integrity-impacting cyber incident.**

4. Normative References

The following documents contain provisions which, through reference in this text, constitute requirements of the Cyber Recovery Maturity Model. For dated references, only the edition cited applies. For undated references, the latest edition applies.

Regulatory & Industry Standards

- **NIST SP 800-34 Rev.1 (2010)**
  Contingency Planning Guide for Federal Information Systems.
- **NIST SP 800-184 (2016)**
  Guide for Cybersecurity Event Recovery.
- **NIST SP 800-53 Rev.5 (2020)**
  Security and Privacy Controls for Information Systems and Organisations.
- **NIST Cybersecurity Framework (CSF) 2.0 (2024)**
  US National Institute of Standards and Technology.
- **NIST SP 800-207 (2020)**
  Zero Trust Architecture.
- **ISO/IEC 27001:2022**
  Information security, cybersecurity and privacy protection - Information security management systems - Requirements.
- **ISO/IEC 27002:2022**
  Information security, cybersecurity and privacy protection - Information security controls.
- **ISO/IEC 27031:2011**
  Guidelines for information and communication technology readiness for business continuity.
- **ISO/IEC 22301:2019**
  Security and resilience - Business continuity management systems - Requirements.
- **ISO/IEC 27040:2015**
  Storage security.
- **ISO/IEC TS 23264-1:2023**
  Cybersecurity - IT Security and Operational Assurance - Part 1: Cyber resilience.
- **ENISA (2023)**
  Good Practices for Secure Backup and Recovery.

Regulatory Guidance

- **HKMA Cybersecurity Fortification Initiative (CFI) 2.0 (2023)**
  Technology Risk Management Framework.
- **HKMA Supervisory Policy Manual (SPM): OR-2 Operational Resilience (2022).**
- **HKMA TMA-2 (“STDB”) Secure Tertiary Data Backup Requirements (2021)**
  most relevant normative reference for destructive recovery.
- **MAS Technology Risk Management (TRM) Guidelines (2021, updated 2022)**
- **Bank of England Operational Resilience Policy (2022)**
  PRA Rulebook and Supervisory Statement SS1/21.

- **NCSC / NIST Joint Guidance (2022)**
  Securing data against ransomware attacks.
- **NCSC CAF (Cyber Assessment Framework) v3.1 (2023)**
  UK National Cyber Security Centre.
- **Digital Operational Resilience Act (DORA) Regulation (EU) 2022/2554**
  Articles 8, 11, 12, 15 and 22 relating to ICT risk management, testing, and recovery.

Technology-Specific References

While not normative, the following technical references may inform implementation:

- Vendor hypervisor and virtualisation platform hardening guides
- Backup platform immutability and air-gap reference architectures
- Cross-cloud and hybrid recovery pattern documentation

CRA Reference Materials

- CRA Cyber Recovery Architecture Reference
- CRA Zero-Trust Recovery Environment Pattern
- CRA Assessment Methodology Guide (AMG)
- CRA Evidence Catalogue v1.0

5. Terms and Definitions

For the purposes of this document, the following terms and definitions apply.

5.1 Cyber Recovery (CR)

A structured capability that enables the restoration of systems, data, and services following a destructive cyber event in which the trustworthiness of production infrastructure, identity systems, or data is compromised or cannot be assured.

5.2 Recovery Environment (RE)

A logically or physically separate environment used to reconstruct, validate, and restore services during a cyber recovery event. Also referred to as a Clean Room, Sterile Zone, or Recovery Landing Zone.

5.3 Clean Zone

An isolated and highly controlled environment designed to remain uncompromised during a cyber incident and to provide the trusted base from which recovery orchestration, validation, and rebuild activities are executed.

5.4 Immutable Backup

A backup or snapshot stored using mechanisms that prevent modification, deletion, or encryption within a defined retention period, irrespective of administrative privileges.

5.5 Recovery Pipeline

A structured sequence of automated or semi-automated steps used to reconstruct systems from known-good artefacts, with integrity validation applied at each stage.

5.6 Loss-of-Trust Event

A cyber incident that compromises, or is reasonably suspected to compromise, critical components of production infrastructure, including identity, hypervisors, management tooling, or data integrity.

5.7 Recovery Pattern

A prescriptive architectural approach for restoring services in a controlled way, including identity rebuild, platform rebuild, workload restore, and data integrity verification.

5.8 Evidence Artefact

Documentation, logs, configuration exports, or automated output that demonstrates the existence, operation, or results of a cyber recovery capability.

5.9 Independence of Control

A separation-of-duties model ensuring that individuals who manage production infrastructure do not possess unrestricted ability to modify or destroy cyber recovery environments or artefacts.

5.10 Recovery Test

A controlled, repeatable exercise performed to validate the organisation’s ability to restore a trusted operational environment under realistic cyber-compromise conditions.

5.11 Recovery Readiness

The demonstrated ability to execute the organisation's recovery pattern(s) reliably, consistently, and within required time and assurance thresholds.

5.12 Critical Data Class (CDC)

A classification applied to data that is required for safe or compliant restoration of business services and must therefore be covered by enhanced protection and recovery controls.

5.13 Orchestration Layer

A platform or toolset responsible for coordinating recovery actions, sequencing dependencies, and enforcing verification steps during the rebuild process.

5.14 Recovery Assurance

A measure of confidence validated through evidence, testing, and governance that recovery processes will operate successfully during a destructive cyber incident.

5.15 Authoritative Data Source

A system or repository designated as the single valid source for specific configuration, identity, or operational data during a recovery.

5.16 Recovery Safety Check

A verification step intended to ensure data, systems, or credentials imported into a recovery environment do not reintroduce compromise.

5.17 Control Plane

The set of tools, privileged systems, interfaces, and platforms that operate or administer production or recovery workloads.

5.18 Gold Image

A validated, signed, tamper-evident system image used as a baseline to rebuild workloads within the recovery environment.

5.19 Recovery Governance Board

A formal governance body responsible for oversight, risk management, approval and accountability of cyber recovery planning, testing and ongoing capability assurance.

5.20 Triggering Event

A condition confirmed or suspected, that necessitates activation of the cyber recovery process.

6. Symbols and Abbreviations

The following abbreviations are used throughout this standard:

Abbreviation	Meaning
AD	Active Directory
BCP	Business Continuity Planning
CDC	Critical Data Class
CRA	Cyber Recovery Authority
CRMM	Cyber Recovery Maturity Model
DR	Disaster Recovery
IAM	Identity and Access Management
IR	Incident Response
ISMS	Information Security Management System
ISO	International Organization for Standardization
LZ	Landing Zone
NIST	National Institute of Standards and Technology
RBE	Recovery Build Environment
RE	Recovery Environment
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SOC	Security Operations Centre
TDA	Threat and Dependency Analysis
VM	Virtual Machine
ZTR	Zero Trust Recovery

7. Cyber Recovery Maturity Model Overview

7.1 Purpose of the Model

The Cyber Recovery Maturity Model (CRMM) establishes a structured, repeatable method for evaluating an organisation's capability to recover from destructive cyber incidents. It provides:

- A **common language** for cyber recovery readiness
- A **domain-based structure** aligned to modern cyber threats
- A **level-based progression** that supports planning and improvement
- A **scoring-neutral assessment approach** suitable for regulators, auditors, and internal stakeholders

The model evaluates cyber recovery capability across **six domains**, each of which represents a critical dimension of readiness:

1. **Recovery Architecture**
2. **Backup, Storage & Data Integrity**
3. **Identity & Access Separation**
4. **Recovery Orchestration & Tooling**
5. **Testing & Validation**
6. **Governance & Operating Model**

Each domain contains **four maturity levels** defining clear, objective criteria.

7.2 Model Structure

The CRMM is structured using the following hierarchical components:

Domains → Criteria → Evidence → Assessment Result

- **Domains** describe thematic capability areas.
- **Criteria** define objective, observable characteristics at each maturity level.
- **Evidence** validates the presence and operation of each criterion.
- **Assessment Result** provides a level rating for each domain, with no aggregation into a single composite score unless justified by local governance.

This ensures the model remains **transparent, auditable, and defensible**

7.3 Model Philosophy

CRMM is built upon the following principles:

a. Zero-Trust Recovery

Assume no component of production infrastructure is inherently trustworthy following a destructive cyber event.

b. Independence of Control

Recovery environments and artefacts must be protected from compromise by ensuring separation of duties, credentials, and administrative boundaries.

c. Evidence-Based Assurance

Maturity ratings must be supported by verifiable artefacts, not solely by policy statements or intent.

d. Pattern-Based Recovery

Recovery should be executed using consistent, predictable patterns that encapsulate identity rebuild, platform rebuild, and application recovery.

e. Fail-Safe Restoration

Prefer designs that prevent unsafe recovery, even if human error or misconfiguration occurs under crisis conditions.

7.4 Intended Use Cases

The model is designed for use by:

- Organisations self-assessing resilience
- Internal and external auditors
- Regulators evaluating systemic risk
- Managed service providers demonstrating capability
- Procurement teams assessing vendor resilience
- Boards and executive committees monitoring improvements

CRMM is technology-agnostic and can be applied to:

- On-premises environments
- Private cloud platforms
- Public cloud and hybrid workloads
- Managed service operations

7.5 Relationship to Disaster Recovery (DR)

CRMM does not replace traditional DR frameworks. Key differences include:

Traditional DR	**Cyber Recovery (CR)**
Assumes infrastructure is trustworthy	Assumes infrastructure may be compromised
Focus on availability	Focus on integrity and trust
Emphasises RTO/RPO	Emphasises correctness, safety, and assurance
Relies on production identity and tooling	Rebuilds these components independently
Often centralised	Requires high assurance, independent recovery paths

8. Maturity Levels

The CRMM defines four levels of maturity. Each level represents a measurable, evidence-backed progression of capability. These levels apply **independently for each domain**.

Level 1: Initial / Ad Hoc

The organisation has limited capability to recover following a destructive cyber incident.

Characteristics:

- Recovery processes are informal, undocumented, or inconsistently applied
- Backups may exist, but trust in their integrity cannot be assured
- Identity, hypervisor, and control-plane dependencies are not recoverable independently
- Tests are infrequent, highly manual, or non-representative of cyber scenarios
- Governance and ownership are unclear or fragmented
- Recovery patterns do not address loss-of-trust situations

Outcomes:

- Recovery is **highly unreliable**
- Safety and correctness cannot be assured
- Recovery is dependent on key individuals
- Significant risk of reinfection or recovery failure

Level 2: Defined and Basic

Recovery capabilities exist but lack completeness, assurance, or independence.

Characteristics:

- Documented recovery processes covering key systems
- Backups are taken consistently and have defined retention
- Some immutability controls exist but may not be comprehensive
- A basic recovery environment exists but is not fully isolated
- Identity rebuild process is partially documented but not regularly validated
- Recovery tests occur, but are typically narrow or low fidelity

Outcomes:

- Recovery is **possible** but unreliable under cyber-compromise scenarios
- Integrity checks are limited
- Manual effort remains high
- Dependencies on production systems are reduced but still significant

Level 3: Assured and Repeatable

Recovery processes are repeatable and supported by independent control measures.

Characteristics:

- A well-defined, isolated Recovery Environment exists

- Immutable backups with enforced retention
- Independently protected identity rebuild pathway
- Recovery orchestration is partially automated and pattern-based
- Recovery tests simulate realistic cyber events
- Governance structures enforce change control and separation of duties
- Evidence capture is consistent and auditable

Outcomes:

- Recovery is **reliable and defendable**, even under adverse conditions
- Trust is re-established through structured safety checks
- Plans are validated by testing, not assumed

Level 4: Resilient and Automated

Recovery capability is automated, assured, and architecturally independent of production infrastructure.

Characteristics:

- Fully pattern recovery from zero-trust assumptions
- Identity, hypervisor, backup systems, and orchestration control planes recoverable independently
- Extensive automation reduces human error and accelerates restoration
- Comprehensive immutability, air-gapping, and integrity verification controls
- Continuous validation of recovery artefacts
- Governance and oversight are embedded into enterprise-level risk management
- Evidence is captured automatically and retained for audit

Outcomes:

- Recovery is **predictable, repeatable, and trusted**
- Organisation can demonstrate high assurance to regulators and stakeholders
- Recovery processes withstand sophisticated, targeted destructive attacks
- Strong alignment with sector resilience expectations

9. Assessment Domains

The Cyber Recovery Maturity Model evaluates capability across **six domains**.
Each domain represents a critical dimension of cyber recovery readiness and contains criteria for Levels 1–4.

The domains are:

1. **Recovery Architecture**
2. **Backup, Storage & Data Integrity**
3. **Identity & Access Separation**
4. **Recovery Orchestration & Tooling**
5. **Testing & Validation**
6. **Governance & Operating Model**

9.1 Domain 1: Recovery Architecture

Definition

The structures, environments, trust boundaries, platforms, and isolation controls required to rebuild production services in a clean and controlled manner following a destructive cyber incident.

Purpose

To ensure the organisation can reconstruct a trusted operational environment regardless of the state of production systems, hypervisors, networks, or control planes.

Key Capability Themes

- Architectural separation between production and recovery environments
- Zero-trust assumptions applied to compromised infrastructure
- Clean-room or sterile-zone recovery capability
- Network and identity isolation controls
- Ability to rebuild platform layers (virtualisation, compute, storage) independently
- Safe reconstruction processes that prevent reinfection

9.2 Domain 2: Backup, Storage & Data Integrity

Definition

The mechanisms by which data, system images, configurations, and operational artefacts are captured, protected, validated, and restored safely in a cyber recovery event.

Purpose

To ensure the organisation has trustworthy data and system artefacts available and verifiable for safe restoration.

Key Capability Themes

- Immutable backups and enforced retention
- Air-gapping or equivalent isolation
- Integrity checks, validation, and anti-contamination measures

- Protection against credential compromise and administrative abuse
- Coverage of critical data classes (CDCs)
- Storage architectures that support high-assurance recovery

9.3 Domain 3: Identity & Access Separation

Definition

The ability to rebuild and operate identity systems required for recovery independently from compromised production identity and access infrastructure.

Purpose

To ensure recovery can proceed safely even if identity providers, authentication mechanisms, or privileged credentials in production are compromised.

Key Capability Themes

- Independent identity rebuild pathway
- Separation of privilege, administration, and access between production and recovery
- Short-lived, constrained, or single-purpose credentials
- Protection of break-glass accounts
- Assurance that recovery identities cannot compromise production, or vice versa
- Control-plane segmentation (identity, directory, MFA, secrets)

9.4 Domain 4: Recovery Orchestration & Tooling

Definition

The tools, automation, workflows, and pipeline components that execute or coordinate the recovery of systems, applications, and data.

Purpose

To ensure the organisation can perform recovery operations consistently, safely, and at scale with reduced reliance on manual actions.

Key Capability Themes

- Automated orchestration pipelines
- Signed or tamper-evident artefacts
- Safeguards and validation gates
- Repeatable recovery patterns
- Trusted toolchains isolated from production compromise
- Structured workflows for identity rebuild, platform rebuild, and workload recovery

9.5 Domain 5: Testing & Validation

Definition

The organisation’s ability to validate recovery processes, artefacts, infrastructure, and safety mechanisms against realistic cyber scenarios.

Purpose

To ensure cyber recovery capability is demonstrably effective through structured, repeatable testing.

Key Capability Themes

- Full-scope recovery exercises
- Scenario-based destructive testing
- Controlled re-introduction of compromised artefacts (if required)
- Evidence generation and validation
- Continuous measurement of readiness
- Automation of testing and verification processes

9.6 Domain 6: Governance & Operating Model

Definition

The ownership, oversight, processes, and risk management structures governing cyber recovery capability.

Purpose

To ensure roles, responsibilities, and controls are defined, enforced, and aligned with enterprise risk appetite and regulatory expectations.

Key Capability Themes

- Leadership accountability and sponsorship
- Recovery Governance Board or equivalent
- Policies, standards, and architectural guardrails
- Separation of duties and privileged access governance
- Change control and configuration management
- Evidence retention and auditability
- Continual improvement processes

10. Domain Criteria

Each domain contains four levels of maturity (L1–L4).
Criteria are written to be **objective, observable, and evidence-verifiable**.

10.1 Domain 1: Recovery Architecture

Level 1: Initial / Ad Hoc

The organisation exhibits the following characteristics:

1. Recovery architecture is undefined or inconsistent across systems.
2. No dedicated recovery environment exists; recovery relies on production infrastructure that may be compromised.
3. Network boundaries do not enforce separation between production and recovery activities.
4. Recovery processes assume trust in production hypervisors, storage, and identity systems.
5. No validated clean-room or sterile environment is available for safe reconstruction.
6. System rebuilds rely on manual processes, technician knowledge, or ad-hoc scripting.
7. No assurance mechanisms exist to prevent reinfection during recovery.

Level 2: Defined and Basic

1. A basic recovery environment exists but shares dependencies with production infrastructure.
2. Documented architectural patterns exist, but implementation varies across systems or business units.
3. Partial network isolation controls are implemented, though routing and firewalling dependencies remain.
4. Recovery environment capacity is not sized, validated, or independently assured.
5. Rebuild of platform components (e.g., hypervisors, storage nodes) is possible but requires manual coordination.
6. Some workloads may be restored into an alternative compute environment, but not consistently.
7. Risks of reinfection are reduced but not systematically mitigated through architectural controls.

Level 3: Assured and Repeatable

1. A formally designed **Recovery Environment (RE)** exists with architectural separation from production.
2. Network, identity, and control-plane isolation is enforced through dedicated trust boundaries.
3. Platform rebuild (compute, storage, hypervisors) is possible without reliance on compromised production tooling.
4. Clean-room recovery patterns are documented, tested, and consistently applied.
5. Recovery architecture enforces zero-trust assumptions toward production systems.
6. Changes to recovery architecture follow strict governance and separation-of-duties controls.
7. Reinfection risk is mitigated through validated safety checkpoints, including image verification and integrity inspection.
8. Capacity planning ensures the RE can support critical services during recovery.

Level 4: Resilient and Automated

1. The Recovery Environment is fully independent, self-sufficient, and continuously validated.
2. Architectural patterns enforce rigorous trust boundaries, preventing compromise propagation by design.
3. Recovery from bare metal or cloud landing zones is automated, deterministic, and consistent.
4. Identity, platform, backup, and storage layers can all be rebuilt without production inputs.
5. The RE supports pattern-based, automated deployment of compute, networking, and application layers.
6. All recovery architectures are tested under realistic destructive scenarios.
7. Reinfection prevention mechanisms (e.g., signed artefacts, attestation, automated safety checks) are integrated end-to-end.
8. Architectural design adheres to CRA reference models and sector-level resilience expectations.

10.2 Domain 2: Backup, Storage & Data Integrity

Level 1: Initial / Ad Hoc

1. Backups exist for some systems but are inconsistent in coverage or retention.
2. No immutability controls exist, or immutability relies on administrative trust.
3. Backup repositories may be directly accessible from production networks.
4. Integrity checks (hashing, scanning, validation) are absent or ad hoc.
5. Backup storage relies on shared credentials or privileged accounts without separation.
6. Backups of identity, configuration, and platform components may be missing or incomplete.
7. Recovery from backup risks reintroducing compromised artefacts.

Level 2: Defined and Basic

1. Backup policies define retention, frequency, and coverage for critical systems.
2. Some immutability controls exist (e.g., retention locks, WORM storage) but may not be comprehensive.
3. Critical data classes (CDC) are identified but not fully mapped to backup design.
4. Integrity checks exist but are limited to periodic or manual verification.
5. Separation between backup and production administration is partially enforced.
6. Copies of configuration data, VM templates, or images exist but may lack assurance mechanisms.
7. Isolation between backup repositories and production is improved but not fully independent.

Level 3: Assured and Repeatable

1. Immutable backups with enforced retention exist for all critical data classes.
2. Backup systems and repositories are architecturally isolated from production.
3. Continuous or scheduled integrity validation verifies:
    a. data correctness
    b. consistency
    c. absence of tampering or malware
4. Backup credentials are segregated from production administrative roles.

5. Backup coverage includes identity systems, hypervisors, orchestration tooling, and configuration repositories.
6. Airgap or equivalent isolation capability is validated through testing.
7. Backup catalogue and metadata integrity is ensured through checksums, signatures, or dual-control mechanisms.

Level 4: Resilient and Automated

1. All backup artefacts (data, images, configurations, templates) undergo automated integrity verification.
2. Immutability is policy-enforced, tamper-evident, and cannot be overridden by privileged production accounts.
3. Backups are synchronised into the Recovery Environment through controlled, unidirectional mechanisms.
4. Machine-verifiable provenance (e.g., signed snapshots) ensures artefact trustworthiness.
5. Automated contamination detection prevents reinjection of compromised data.
6. Storage architectures guarantee independence, resilience, and recoverability regardless of production compromise.
7. Backup integrity status is continuously monitored and auditable.

10.3 Domain 3: Identity & Access Separation

Level 1: Initial / Ad Hoc

1. Recovery processes depend on production identity systems (AD, IAM, MFA, SSO).
2. Privileged accounts may have broad administrative access across production and backup systems.
3. No isolated identity platform exists for recovery operations.
4. Break-glass accounts are undocumented or not regularly validated.
5. Identity compromise would render recovery unsafe or impossible.

Level 2: Defined and Basic

1. Documented procedures exist for identity rebuild but are partially manual.
2. A limited, separate identity environment exists but lacks independence and hardening.
3. Break-glass accounts are managed but not regularly tested under recovery conditions.
4. Privileged access in backup and recovery environments is partially segregated.
5. Production identity compromise still poses significant recovery risk.

Level 3: Assured and Repeatable

1. A dedicated identity system supports recovery operations independently of production.
2. Credential separation enforces clear boundaries between production, backup, and recovery administration.
3. Identity rebuild processes are tested and validated as part of recovery exercises.
4. Temporary, short-lived, or single-purpose credentials are used for recovery stages.
5. MFA, secrets vaults, and privileged access tooling for recovery are isolated and hardened.
6. Compromise of production identity cannot directly compromise recovery environments.

Level 4: Resilient and Automated

1. Identity rebuild is automated, pattern-based and fully independent.
2. Cryptographic signing, attestation, and integrity verification protect identity bootstrap artefacts.
3. Trust boundaries prevent lateral compromise between identity tiers.
4. Recovery identity provisioning is automated with ephemeral identities.
5. Privileged access for recovery follows strict just-in-time issuance.
6. Identity controls meet the highest level of regulatory cyber recovery expectations.

10.4 Domain 4: Recovery Orchestration & Tooling

Level 1: Initial / Ad Hoc

1. Recovery tasks are manual or reliant on engineer knowledge.
2. Scripting is informal, unsourced, or not version controlled.
3. No structured orchestration or sequencing exists.
4. Tooling resides in production environments and may be compromised.
5. Inconsistent rebuild results across teams or attempts.

Level 2: Defined and Basic

1. Recovery workflows are documented and partially sequenced.
2. Some tooling exists in a non-production environment but may not be isolated.
3. Version-controlled scripts or playbooks support portions of the recovery.
4. Manual steps remain significant; errors or omissions are common.
5. Toolchain trust depends on production identity or infrastructure.

Level 3: Assured and Repeatable

1. An independent recovery toolchain exists within the Recovery Environment.
2. Orchestration pipelines automate major recovery stages (identity → platform → application).
3. Artefacts (images, scripts, manifests) are signed or tamper evident.
4. Validation gates enforce integrity checks before progression.
5. Automation ensures consistent rebuild outcomes across tests.
6. Toolchain changes follow strict version control and governance.

Level 4: Resilient and Automated

1. Orchestration is fully automated, deterministic, and end-to-end.
2. Recovery toolchain is isolated, self-healing, and continuously validated.
3. Autonomous verification ensures safe progression between stages.
4. Trust is anchored in signed artefacts and attestation mechanisms.
5. Pattern libraries encode recovery of all critical workloads.
6. Tooling supports regulator-grade evidence capture.

10.5 Domain 5: Testing & Validation

Level 1: Initial / Ad Hoc

1. Recovery tests are infrequent, narrow, or non-existent.

2. No destructive or scenario-based testing takes place.
3. Test results are not documented or retained.
4. Recovery outcomes depend heavily on individual knowledge.
5. No validation of identity or platform rebuild.

Level 2: Defined and Basic

1. Periodic recovery tests occur for selected workloads.
2. Some scenario testing exists but does not simulate destructive events.
3. Test documentation exists but is inconsistent.
4. Evidence of test outcomes is partially captured.
5. Testing does not validate full recovery patterns.

Level 3: Assured and Repeatable

1. Annual or semi-annual full-scope cyber recovery exercises.
2. Tests simulate realistic destructive cyber events.
3. Identity, platform, and application layers are rebuilt under test conditions.
4. Validation mechanisms and safety checks are assessed.
5. Evidence retention is consistent across all tests.
6. Remediation actions feed into improvement cycles.

Level 4: Resilient and Automated

1. Continuous or automated validation of recovery artefacts and pipelines.
2. Regular destructive scenario testing, including hypervisor and identity compromise.
3. Full recovery patterns tested end-to-end, including dependent systems.
4. Evidence is automatically captured and retained.
5. Metrics quantify readiness, reliability, and time-to-recover.
6. Testing satisfies regulator-grade resilience standards.

10.6 Domain 6: Governance & Operating Model

Level 1: Initial / Ad Hoc

1. No clear ownership of cyber recovery capability.
2. Policies and standards do not address destructive cyber recovery.
3. Authority for recovery decisions is unclear.
4. No formal governance structure exists.
5. Recovery activities occur outside enterprise risk oversight.

Level 2: Defined and Basic

1. Ownership exists for recovery capability, though responsibilities may be fragmented.
2. Policies document recovery expectations but lack assurance mechanisms.
3. Governance meetings occur but are operational rather than strategic.
4. Limited separation of duties for privileged access.
5. Recovery decisions partially aligned with enterprise risk processes.

Level 3: Assured and Repeatable

1. A formal **Recovery Governance Board** oversees capability, testing, and risk.

2. Policies, standards, and architectural guardrails are enforced through change control.
3. Separation of duties is actively monitored and validated.
4. Recovery capability is integrated into enterprise risk reporting.
5. Evidence retention and auditability are mandated.
6. Resilience objectives influence strategic investment decisions.

Level 4: Resilient and Automated

1. Governance is proactive, dynamic, and driven by continuous risk intelligence.
2. Recovery capability is embedded into enterprise-wide resilience frameworks.
3. Automation supports compliance, evidence capture, and oversight.
4. Metrics inform board-level decisions and investment prioritisation.
5. Governance aligns with sector resilience and regulatory expectations.

11. Assessment Method

The CRMM requires assessments to be **objective**, **evidence-based**, and **domain-specific**. The model does **not** prescribe aggregated scoring unless explicitly required by regulators or boards.

Each domain is assessed independently. The assessment method consists of **five stages**:

1. **Preparation**
2. **Evidence Collection**
3. **Assessment & Rating**
4. **Validation**
5. **Reporting**

11.1 Stage 1: Assessment Plan

The assessor shall:

1. Confirm assessment scope (business units, systems, environments).
2. Identify required personnel (architecture, IT, identity, storage, backup, IR, DR, governance).
3. Define the assessment window and logistics.
4. Obtain access to relevant documentation (architecture diagrams, policies, test artefacts).
5. Ensure independence of assessment personnel (internal audit, second line, or external party recommended).

11.2 Stage 2: Evidence Register

Evidence must be sourced from:

- System configurations
- Architecture / network diagrams
- Backup platform outputs
- Identity system logs and exports
- Recovery orchestration pipelines
- Recovery test plans and reports
- Screenshots, logs, or artefacts demonstrating RE independence
- Interviews with SMEs (used only to supplement objective evidence)

Types of acceptable evidence:

- Automated output
- Configuration exports
- Signed artefacts
- System logs
- Test results
- Screenshots capturing system states
- Policies, procedures, and governance records

Types of unacceptable evidence:

- Assertions of intent

- Policy statements without operational artefacts
- Unverified manual descriptions
- Capabilities not demonstrated in testing

11.3 Stage 3: Domain Assessment Records

Each domain is assessed independently.

Note: A domain is assigned the highest level for which **all criteria at that level are met.**

Example:

- If a domain meets Level 3 criteria but fails any Level 4 criterion → **Rated Level 3**
- If a domain meets some Level 2 criteria but not all → **Rated Level 1**

This ensures:

- Consistency
- Objectivity
- Defence against audit/regulator challenge

11.4 Stage 4: Validation Statement

The assessor must:

1. Cross-validate evidence across domains (e.g., identity patterns vs backup immutability).
2. Obtain independent confirmation from system owners.
3. Validate that test results align with documentary evidence.
4. Confirm that no contradictory artefacts exist (e.g., firewall rules violating isolation claims).
5. Ensure accuracy and completeness of the final report.

Where discrepancies are found:

- The assessor shall downgrade the affected level or request further evidence.

11.5 Stage 5: CRMM Assessment Report

The final assessment report must include:

1. Overview of assessment scope
2. Summary narrative of overall cyber recovery capability
3. Level for each domain
4. Supporting evidence references
5. Key gaps and risks
6. Recommended improvements
7. Alignment with regulatory expectations
8. Trend comparison (where prior assessments exist)

Optional (recommended):

- Executive heatmap showing levels across domains
- Gap analysis
- Dependency/risk mapping

12. Evidence Catalogue

This catalogue defines required evidence types for each domain.
The table below is written at a meta-level; Annex A later includes a full assessment template.

12.1 Evidence Category Definitions

Category	Description
AR	Architectural evidence (diagrams, network maps, trust boundaries)
CF	Configuration artefacts (exports, manifests, snapshots)
LG	Logs demonstrating operation or enforcement of controls
SC	Screenshots validating system states or isolation
PL	Policies, standards, and governance documents
TC	Test results (reports, orchestrator outputs, success/failure logs)
VC	Verification and checksum artefacts
IA	Identity and access artefacts (role exports, credential separation evidence)
BK	Backup system artefacts (immutability status, catalogues, retention proofs)

12.2 Evidence Requirements by Domain

Domain 1: Recovery Architecture

Required evidence types: **AR, CF, LG, SC, PL**

Examples:

- Clean room / RE architecture diagrams
- Network isolation configurations
- Storage and compute rebuild manifests
- Screenshots proving independent admin boundaries
- Governance records for RE changes

Domain 2: Backup, Storage & Data Integrity

Required evidence types: **BK, VC, CF, LG, PL**

Examples:

- Backup immutability reports
- Air-gap or isolation-mode audit logs
- Integrity validation results (checksums, malware scans)
- Backup catalogue exports for CDC workloads
- Retention lock configuration evidence

Domain 3: Identity & Access Separation

Required evidence types: **IA, CF, PL, LG, SC**

Examples:

- Identity rebuild runbooks
- Exports of identity roles and privilege boundaries
- MFA and privileged-access segregation evidence
- Logs proving isolation of identity tiers
- Screenshots of ephemeral credential issuance

Domain 4: Recovery Orchestration & Tooling

Required evidence types: **CF, LG, SC, TC, VC**

Examples:

- Orchestrator pipelines and manifests
- Logs detailing recovery stage execution
- Signed image or script verification reports
- Automated safety-check outputs
- Toolchain access boundary evidence

Domain 5: Testing & Validation

Required evidence types: **TC, LG, SC, PL**

Examples:

- Full-scope test reports
- Screenshots of recovery phases
- Logs from destructive testing scenarios
- Records of remediation and gap closure
- Evidence of continuous validation pipeline runs

Domain 6: Governance & Operating Model

Required evidence types: **PL, SC, LG**

Examples:

- Recovery Governance Board minutes
- Policies, standards, and architectural guardrails
- Separation-of-duties controls and approval workflows
- Evidence of alignment with risk and compliance processes

12.3 Evidence Quality Requirements

All evidence must meet the following standards:

1. **Authenticity**: must reflect actual operating state.
2. **Integrity**: must be untampered and timestamped.
3. **Completeness**: covers all systems within scope.
4. **Relevance**: directly supports the maturity claim.

5. **Repeatability**: can be regenerated consistently.

Evidence that fails these criteria shall not be accepted.

ANNEX A: ASSESSMENT TEMPLATES

A1. Assessment Overview

Organisation Name

< >

Assessment Period

< >

Assessment Team (Assessor Names & Roles)

< >

Assessment Version / Internal Reference

< >

Applicable Regulatory or Audit Context

<> (e.g., HKMA, MAS, PRA, DORA, ISO/IEC audits)

Scope of Assessment

<systems, environments, applications included>
<geography / business lines>
<limitations or exclusions>

Assessment Objectives

< > (e.g., determine maturity level, validate recovery readiness, identify gaps)

Key Contacts (Client)

<roles, names, contact details>

Assessor Notes

< >

A2. Domain Assessment Form

Repeat this form **for each of the six maturity domains**.

Domain Name

[Recovery Architecture / Backup, Storage & Data Integrity / Identity & Access Separation / Recovery Orchestration & Tooling / Testing & Validation / Governance & Operating Model]

Assessed Maturity Level (1-4)

< >

Control Areas Evaluated

<list of relevant controls or subcomponents>

Assessment Summary

<description of control effectiveness, observed strengths, systemic weaknesses>

Supporting Evidence (references only)

<List evidence item IDs from A3>

Assessor Judgement

- Does the evidence support the claimed maturity level?

  [yes/no/conditional]

- Gaps preventing advancement to next level:
  < >
- Recommended uplift actions:
  < >

Assessor Notes

< >

A3. Evidence Register

Use *one instance of the following block for each evidence item*.
This format **avoids table width issues** and is aligned with ISO/NIST audit forms.

Evidence Entry

Evidence Identifier (Ref)
< >

Domain
[Recovery Architecture / Backup, Storage & Data Integrity / Identity & Access Separation / Recovery Orchestration & Tooling / Testing & Validation / Governance & Operating Model]

Control Area Supported
< >

Evidence Type
<Document / Screenshot / Log / System Output / Test Result / Interview Note / Configuration Extract / Other>

Description

<summary of what the evidence demonstrates and why it is relevant>

Source System / Location
< >

Date Collected
< >

Submitted By
< >

Verification Method
<Inspection / Reproduction / Log Analysis / Test Execution / Automated Validation>

Verified By
< >

Verification Date
< >

Verification Result
[Pass / Conditional / Fail]

Assessor Notes
< >

A4. Final Maturity Summary

This section presents the organisation’s final maturity outcome.

Overall Cyber Recovery Maturity Level

■ **Assessed Maturity Level (1-4)**

< >

■ **Determining Factors**

- < >
- < >
- < >

Domain-Level Maturity Ratings

■ **Recovery Architecture**

Level: <1-4>
Notes: < >

■ **Backup, Storage & Data Integrity**

Level: <1-4>
Notes: < >

■ **Identity & Access Separation**

Level: <1-4>
Notes: < >

■ **Recovery Orchestration & Tooling**

Level: <1-4>
Notes: < >

■ **Testing & Validation**

Level: <1-4>
Notes: < >

■ **Governance & Operating Model**

Level: <1-4>
Notes: < >

Key Strengths Identified

< >

Priority Gaps / Risks

< >

Recommended Uplift Roadmap

- < >

- < >
- < >

Sign-Off

Lead Assessor:
<name, role, signature>

Assessment Sponsor:
<name, role, signature>

Date Completed:
<DD/MM/YYYY>

Annex B: Example Recovery Pattern

***Informative**, not mandatory, reflects sector best practice.

This annex provides an illustrative, high-level recovery pattern that demonstrates how an organisation may structure its cyber recovery capability in alignment with the CRA reference architecture.

B.1 Pattern Overview

The recovery pattern is structured into four sequential phases:

1. **Phase 1: Identity Reconstruction**
2. **Phase 2: Platform & Control Plane Rebuild**
3. **Phase 3: Application & Data Recovery**
4. **Phase 4: Service Validation & Promotion to Production**

Each phase incorporates:

- Trusted artefacts
- Independent tooling
- Integrity verification
- Strong trust boundaries
- Evidence generation

B.2 Phase 1: Identity Reconstruction

The recovery process begins with re-establishing **trusted identity** in an isolated environment.

Objectives

- Establish a secure, minimal identity foundation
- Prevent compromise propagation from production
- Ensure privileged access is controlled, auditable, and ephemeral

Key Activities

1. Deploy a **clean, signed identity bootstrap image** into the Recovery Environment (RE).
2. Establish a recovery-only identity tree or domain.
3. Issue ephemeral administrative credentials with limited lifetimes.
4. Restore identity groups, roles, and service accounts from **validated configuration artefacts**, not from compromised production systems.
5. Enforce MFA and privileged access vault integration for all recovery admin sessions.

Outputs

- Operational recovery identity platform
- Separation of access between production and recovery
- Integrity-generated evidence: logs, attestations, bootstrap signatures

B.3 Phase 2: Platform & Control Plane Rebuild

This phase regenerates the infrastructure required to host restored services in a trustworthy state.

Objectives

- Establish clean compute, storage, hypervisors, and networking
- Deploy a clean control-plane for recovery orchestration
- Ensure independence from compromised production tooling

Key Activities

1. Rebuild hypervisors or equivalent compute layers using **signed, validated images**.
2. Deploy a recovery-side management plane (orchestration, monitoring, automation).
3. Restore configuration baselines from version-controlled, validated repositories.
4. Establish isolated network segments with strict firewalling and zero-trust defaults.
5. Validate platform integrity through automated attestation or checksum methods.

Outputs

- Fully operational clean platform stack
- Recovery control-plane deployed in the RE
- Artefacts validating pipeline and environment integrity

B.4 Phase 3: Application & Data Recovery

With identity and platform layers rebuilt, applications and data are restored using controlled patterns.

Objectives

- Restore applications and services into a trusted landing zone
- Prevent reinfection from compromised data or binaries
- Ensure recovered workloads operate using validated configurations

Key Activities

1. Import immutable backups into the RE through a **unidirectional**, controlled transfer mechanism.
2. Validate backups through malware scans, checksums, signatures, and behavioural analysis.
3. Deploy workloads using pattern-based manifests and automation pipelines.
4. Restore application configurations from validated configuration repositories.
5. Perform iterative integrity checks (runtime telemetry, behaviour validation, logs).

Outputs

- Reconstructed application tiers
- Engines, databases, and microservices reinstated in clean state
- Integrity reports ensuring safe restoration

B.5 Phase 4: Service Validation & Promotion to Production

The final stage ensures the recovered services are safe, complete, functional, and ready for business use.

Objectives

- Validate correctness, behaviour, and integrity of all restored services
- Demonstrate trust in the recovered state
- Prepare for reintroduction into production or for production rebuild

Key Activities

1. Conduct functional and non-functional service validation.
2. Execute application-specific and cross-platform tests.
3. Confirm configuration baselines and policy compliance.
4. Regenerate new production environment(s) or promote RE workloads to production if deemed safe.
5. Capture complete evidence sets for governance and regulatory reporting.

Outputs

- Validation report covering integrity, functionality, and readiness
- Evidence bundles for audit and regulators
- Authorisation for production cutover

B.6 Pattern Characteristics

This recovery pattern exhibits the following characteristics aligned with CRA expectations:

Predictability

Recovery follows deterministic, repeatable workflows.

Safety

Integrity checks, signed artefacts, and isolation controls prevent reinfection.

Independence

Recovery does not rely on compromised production systems or identities.

Auditability

Evidence is automatically captured throughout the process.

Zero-Trust Defaults

No assumption of inherent trust in production artefacts.

Scalability

Pattern supports large-scale multi-system rebuilds.

Technology-Agnostic

Applicable to on-premises, cloud, and hybrid environments.

B.7 Conceptual Recovery Flow

Recovery is executed in four sequential phases.
Each phase is designed to rebuild system integrity while preventing the reintroduction of compromised components.

Phase 1: Identity Reconstruction

Activities include:

1. Deploy the isolated recovery identity domain.
2. Establish baseline authentication services (temporary or permanent).
3. Issue ephemeral privileged credentials.
4. Restore critical identity objects (roles, groups, service accounts) from validated sources.

Phase 2: Platform & Control Plane Rebuild

This phase prepares the foundational recovery environment:

1. Rebuild compute, storage, and virtualisation layers in isolation.
2. Deploy orchestration, automation, monitoring, and configuration baselines.
3. Apply strict segmentation to prevent lateral propagation.
4. Verify platform integrity using attestation, checksums, or hash validation.

Phase 3: Application & Data Recovery

Workloads and datasets are reintroduced from immutable backup sources:

1. Import validated backup data using a one-directional recovery path.
2. Perform malware scanning, content validation, and structural checks.
3. Deploy application components following approved recovery patterns.
4. Restore configuration and operational dependencies using trusted repositories.

Phase 4: Service Validation & Promotion

The recovered environment is validated and prepared for production handover:

1. Execute functional, integration, and availability tests.
2. Validate baseline configurations, authentication flow, and role assignments.
3. Document integrity, completeness, and readiness of restored services.
4. Promote recovered services to production or conduct cutover operations.

Summary

This flow provides a structured sequence for rebuilding critical systems after a cyber event. While implementations may vary, the principles of isolation, integrity, controlled restoration, and validated promotion remain universal.

Annex C: Scoring

This annex provides guidance for interpreting maturity levels, evaluating organisational posture, and identifying uplift priorities.
Scoring is **informative**, not mandatory, to preserve flexibility across sectors.

C.1 Interpretation of Levels

The table below summarises how each maturity level should be interpreted from a risk and resilience perspective.

This weighting is **informative** and **must not** be used to override domain independence.

Level	Interpretation	Risk Position	Regulatory Readiness
L1	Capability is unstructured or unreliable; recovery may fail under cyber-attack conditions.	High systemic risk	Not acceptable for critical workloads
L2	Recovery possible but fragile; strong dependency on manual effort or production systems.	Significant risk	Below baseline expectations
L3	Recovery is reliable and independently assured; controls enforce separation and integrity.	Moderate, controlled risk	Meets most regulatory expectations
L4	Recovery is predictable, automated, and independent of production; strongest assurance level.	Low risk, high trust	Exemplary resilience posture

C.2 Domain Weighting Guidance

CRMM does **not** mandate weighted scoring. However, regulators and enterprises MAY weight domains according to their risk context.

Suggested weighting (**informative only**):

Domain	Suggested Weight (%)	Rationale
Recovery Architecture	20%	Foundation for all other domains
Backup & Data Integrity	20%	Integrity of recovery artefacts is critical
Identity & Access Separation	20%	Prevents reinfection and control-plane compromise
Recovery Orchestration & Tooling	15%	Determines consistency and repeatability

Testing & Validation	15%	Ensures capability is proven, not assumed
Governance & Operating Model	10%	Governs sustainability and oversight

*This weighting may vary by sector.

C.3 Rating Confidence Levels

Assessors should assign a confidence level to each domain based on evidence strength. Confidence should influence uplift prioritisation even when level ratings are identical.

Confidence	Description
High	Evidence is complete, validated, and multi-sourced
Medium	Evidence is sufficient but may include gaps or dependencies
Low	Evidence is weak, incomplete, or contradicted

C.4 Determining Overall Posture

While CRMM avoids composite scoring, organisations MAY summarise posture using the following categories:

Category	Criteria
Foundational	≥4 domains at L1 or L2
Developing	Majority at L2, at least one at L3
Capable	Majority at L3, no L1
Resilient	≥4 domains at L3, at least one at L4
Advanced	All domains at L4

C.5 Gap Analysis

For each domain, assessors should evaluate:

1. **Unmet criteria** at the next level
2. **Dependencies** preventing uplift (identity, architecture, immutability, etc.)
3. **Investment requirement** (people, tooling, architecture)
4. **Expected uplift timeline**
5. **Change ownership**

This forms the basis of improvement planning.

C.6 Uplift Prioritisation Framework

The following 2×2 matrix helps organisations prioritise which domains to uplift first.

Impact on Recovery × Difficulty of Uplift

Impact	Low Difficulty	High Difficulty
High	Priority 1: Immediate uplift (RA, Identity, Backup)	Priority 2: Strategic investment (RE automation, orchestration)
Low	Priority 3: Opportunistic uplift (Testing, Governance)	Priority 4: Long-term optimisation

Domains with cross-cutting dependencies (Identity, Backup, Recovery Architecture) should be prioritised.

C.7 Regulatory Alignment

Regulators may interpret maturity levels as follows:

- **L1**: Inadequate; material resilience deficiency
- **L2**: Requires remediation plan with fixed deadlines
- **L3**: Meets sector baseline expectations
- **L4**: Preferred state for systemic institutions and critical infrastructure

C.8 Scorecard Template

A scorecard may be constructed as follows:

Domain	Level	Confidence	Rationale	Priority
Recovery Architecture	L2	Medium	Isolation incomplete	P1
Backup & Data Integrity	L3	High	Immutability demonstrated	P2
Identity & Access Separation	L1	Low	No independent identity environment	P1
Recovery Orchestration	L2	Medium	Partial tooling isolation	P2
Testing & Validation	L2	Low	No destructive scenario testing	P3
Governance	L3	Medium	Governance board in place	P4

Cyber Recovery Authority (CRA)

Cyber Recovery Maturity Model Standard — Version 1.0 (2025)

Copyright Statement

Licensing

Contact for Licensing, Accreditation, and Feedback

Cyber Recovery Authority
Email: **contact@cyberrecoveryauthority.org**
Website: **https://www.cyberrecoveryauthority.org**

Document Status

This is the **official published version (v1.0)** of the CRA Cyber Recovery Maturity Model Standard.

Future revisions, amendments, or supplemental guidance will be issued under the same document series and versioning structure.

CRA welcomes feedback from regulated entities, auditors, regulators, and cybersecurity practitioners. Feedback may inform future releases.

Trademarks

Disclaimer

This standard describes best practices for cyber recovery architecture, operations, and assurance. CRA assumes no liability for:

- Organisational use or interpretation
- Implementation errors
- Third-party assessments
- Consequential damages arising from reliance on this publication

Organisations are responsible for ensuring compliance with local regulations, sector-specific requirements, and enterprise risk management frameworks.

End of Standard

This concludes the **CRA Cyber Recovery Maturity Model Standard: Version 1.0**.