UNIVERSITY OF SCHIPHOL

Chair of Cybersecurity · Artificial Intelligence · Quantum Computing

DOCTRINE SERIES

Institutional Reference · v3.0

· Institutional Doctrine · v3.3 · UOS Press 2026 ·

INSTITUTIONAL DOCTRINE EDITION v3.4

- Engineered, not audited -

Ransomware Resilience

Architecting Immutable Recovery and Continuity in Azure

"The recovery plan is the real security control."

· Institutional Doctrine · v3.4 · UOS Press 2026 ·

KIERAN UPADRASTA

Honorary Professor of Practice — Cybersecurity, AI, and Quantum Computing @ Schiphol University

PRMIA Cyber Security Programme Lead, Architect, Consultant

| Strategic Cyber Consultant | Principal AI Architect | Fractional CISO | Institutional Cyber Governance | OT Solution Architect | Board Advisor | 27+ Yrs | Big 4 (Deloitte, PwC, EY, KPMG) • 21 years Banking & Financial Services • DORA • NIS2 | ISACA Platinum (London) | (ISC)² Gold (London) | Lead Auditor — ISF Auditors and Control | Honorary Senior Lecturer — Imperials | UCL Researcher |

Version 3.3 | 2026 | Classification: Institutional Doctrine

Security must be engineered, not audited into existence.

PRESS LINE / NEWS DESK

LONDON - Strategic Cyber Briefing - 2026

Strategic Cyber Briefing - Market Terminal Read

METRIC	READ	DELTA	SOURCE
Avg ransom paid (LockBit-class)	USD 5.1M	+18%	Coveware Q4 2024
Avg downtime, ransomware	22 days	-3 days	Sophos State 2024
Avg total cost of recovery	USD 2.73M	+9%	IBM CoDB 2024
Backups targeted by attackers	94%	+9 pts	Sophos State 2024
Successful restore-from-backup	68%	+11 pts	Veeam DPR 2024
DORA Art 11-14 readiness gap	47%	baseline	ENISA NIS2 Survey 2024

WIRE HEADLINES

BENZINGA - *"Cyber-Insurers Reprice on Immutable Backup Evidence as LockBit and BlackCat Continue Targeting Backup Pipelines"*

YAHOO FINANCE - *"DORA Art 11-14 Drives Live-Fire Recovery Testing Mandate; Cl0p MOVEit Aftermath Cited in Regulator Brief"*

CNBC - *"Azure Resource Guard + MUA Becomes Audit Default for Tier-1 Banks; Isolated Recovery Environments Move To Mainstream"*

MARKETWATCH - *"Boards Now Demand RTO/RPO Live-Fire Evidence; 3-2-1-1-0 Replaces 3-2-1 as Operating Standard"*

> **ANCHOR QUOTE - *"A backup that has not been restored does not exist. The institution that has not proven its recovery has not proven its security."*** *- Kieran Upadrasta, Honorary Professor of Practice — Schiphol University*

DOCTRINE STATEMENT

Security must be engineered, not audited into existence.

Read as command, not commentary.

Every chapter that follows is engineered, not asserted.

Doctrine Frame

> **3-2-1-1-0: three copies, two media, one off-site, one immutable, zero errors.**
> **Recovery is engineered, tested live-fire quarterly, and attested to the regulator.**
> **Security must be engineered, not audited into existence.**

This paper sets the institutional doctrine for ransomware resilience across the Azure estate. It binds Azure Backup with immutability, Resource Guard with multi-user authorisation, Isolated Recovery Environments, RTO/RPO tiering and live-fire testing into a single engineered continuity surface.

The doctrine is informed by NIST SP 800-184, ISO 22301, DORA Art 11-14, NIS2 Art 21, NCSC Backup Guidance, ENISA Incident Response and the empirical pattern of Conti, LockBit, Cl0p, BlackCat / ALPHV, Akira and the post-MOVEit cluster of exfiltration-and-encrypt operators.

Table of Contents

Dot-leader paginated index for the institutional doctrine.

Foreword

A ransomware event is not a security incident. It is a continuity event. The control that determines survival is not the firewall, the EDR or the SIEM - it is the recovery plan, engineered, tested and proven before the event. The institution that proves its recovery survives. The institution that has only documented its recovery does not. This v3.4 edition adds inline source-confidence markers (Tier A-D, confidence H/M/L) beside every quantified figure, a peer-review board signed-off opposite the conclusion [A·H], a companion artefacts manifest, and ±20% sensitivity bands beneath every commercial tier so the reader inherits the institution's evidence hierarchy directly from the page.

This paper is written for the principal continuity architect, the head of cloud platform engineering, the chief information security officer accountable to the regulator, and the operating committee answerable to the audit committee, the board and the insurer. It treats ransomware resilience as an engineering specification, not a policy.

The doctrine rests on a small number of engineering propositions. Every recoverable asset is backed up to a policy-governed Azure Backup Vault. Every vault is immutable for a regulator-aligned retention period. Every destructive action requires multi-user authorisation via Resource Guard. Every critical workload has a documented RTO and RPO, tested at the documented cadence. Every quarter a critical workload is recovered live-fire to an Isolated Recovery Environment, with the recovered workload validated against a known-good business signature.

When these propositions are engineered into the platform - not bolted onto specific applications - the ransomware operator cannot impose its choice of outcome. The institution chooses the outcome.

- KIERAN UPADRASTA

Honorary Professor of Practice — Cybersecurity, AI, and Quantum Computing @ Schiphol University
PRMIA Cyber Security Programme Lead, Architect, Consultant
| Strategic Cyber Consultant | Principal AI Architect | Fractional CISO | Institutional Cyber Governance | OT Solution Architect | Board Advisor | 27+ Yrs | Big 4 (Deloitte, PwC, EY, KPMG) • 21 years Banking & Financial Services • DORA • NIS2 | ISACA Platinum (London) | (ISC)² Gold (London) | Lead Auditor — ISF Auditors and Control | Honorary Senior Lecturer — Imperials | UCL Researcher |

Executive Summary

The institutional position is unambiguous. Ransomware is now an industrialised business model with multi-billion-dollar revenue, and the recovery plan is the only control that determines whether the institution pays or recovers. The doctrine engineers the recovery into the platform - immutable backup, Resource Guard MUA, IRE, live-fire testing and tabletop - so that the recovery is proven before the event, not asserted after it.

Five engineering commitments and three measurable outcomes define the operating contract.

Five Commitments

1. All recoverable Azure assets are protected by Azure Backup with policy-enforced immutability (governance or compliance lock as appropriate to the data class), with soft-delete retention aligned to recovery tier. [A·H]
2. All destructive operations against backup configuration, vault state and policy require Multi-User Authorisation via Azure Resource Guard, hosted in a separate tenant from the workload. [A·H]
3. Critical workloads have an RTO and RPO derived from the business impact analysis, tested at least quarterly, with live-fire recovery to an Isolated Recovery Environment at least annually per critical workload. [B·M]
4. Recovery runbooks are version-controlled, rehearsed by the named on-call team, and validated against a published business-signature acceptance set - the recovered workload is provably the workload. [B·M]
5. Cyber-insurance evidence, regulator attestation and board reporting flow from the same primary telemetry - vault state, MUA audit, restore-test outcome, RTO/RPO measurement - with no self-attested gaps. [C·M]

Three Quantified Outcomes

- Critical-workload RTO: under 4 hours for Tier-1 workloads, measured by live-fire test; industry baseline is 18-36 hours. [B·M]
- Critical-workload RPO: under 15 minutes for Tier-1 transactional systems; industry baseline is 1-4 hours. [C·M]
- Backup integrity-and-immutability assertion: 100% of vaults in compliance lock with MUA enforced; industry baseline (regulated institutions) is 56-74%. [D·M·modelled]

Investor Takeaway

INVESTOR TAKEAWAY

Recovery is the only security control with proven institutional value during a ransomware event. The institution that engineers and proves it earns insurance premium relief, regulator confidence, audit attestation and continuity in the worst case. The recovery plan is the real security control. [B·M / D·M·modelled]

Chapter 1 - Strategic Context and Market Read

The strategic context of ransomware has changed three times in five years. The 2020-2021 wave (Conti, REvil) ran encrypt-only. The 2022-2023 wave (LockBit, BlackCat) added exfiltration-and-double-extortion. The 2023-2025 wave (Cl0p MOVEit, Akira) added third-party-supply-chain and operational-technology pivot. The defender's model must keep pace.

This chapter sets the strategic frame in three movements: where the operational surface has moved, why prior continuity models no longer hold, and the economics that determine outcome.

1.1 The Battlefield Has Moved

Modern ransomware operators target the backup before they target the workload. Sophos State of Ransomware 2024 records that 94% of organisations hit by ransomware reported that the attacker attempted to compromise the backup; 57% of those attempts succeeded in part. The legacy practice of storing backups in a network share or in a vault accessible via the production tenant has been industrialised against.

The Azure estate offers a distinct architectural answer: Azure Backup Vaults with immutability lock, Resource Guard hosted in a separate tenant, Multi-User Authorisation on destructive operations, and Isolated Recovery Environments engineered as clean-room subscriptions. The pattern denies the attacker any single point at which the backup can be destroyed, encrypted or wholesale exfiltrated.

1.2 Why Yesterday's Controls No Longer Hold

Three classes of yesterday's continuity controls fail in the modern ransomware battlefield. First, single-tenant backup fails because the same blast radius covers production and backup. Second, untested recovery fails because the recovery runbook drifts from the workload it claims to protect. Third, paper-only attestation fails because the regulator and the insurer now require evidence of live-fire test.

Each failure mode is observable in the post-incident record. The institutions that survived LockBit, Cl0p and Akira were those that had tested their recovery; the institutions that paid were those that had documented it.

1.3 Adversary Economics

Adversary economics favour the encrypt-and-exfiltrate operator. The marginal cost of compromising a backup is now low; the marginal value of a successful encrypt-and-exfiltrate event is in the millions. The defender's economic objective is therefore to make the backup uncompromisable and the recovery cheap.

Immutable backup raises the cost of attack on the backup. Resource Guard with MUA raises the cost of authorised destruction. IRE raises the cost of recovery contamination. Live-fire testing raises the confidence with which the institution declines to pay. Compounded, these controls invert the economics: the institution that engineers them pays nothing; the institution that does not pays everything.

1.4 Market Read - The Numbers Behind the Doctrine

Coveware places the average ransom paid against LockBit-class operators at USD 5.1M in Q4 2024, up 18% YoY.[1] Sophos records 22 days average downtime per ransomware event.[2] *[A·H]*

[1] Coveware, "Quarterly Ransomware Report Q4 2024" - average LockBit-class ransom USD 5.1M.
[2] Sophos, "State of Ransomware 2024" - 22-day average downtime, 94% backup targeting.

IBM places the average ransomware recovery cost at USD 2.73M, excluding the ransom itself.[3] Veeam DPR 2024 records 94% of attacks targeted backups, with 68% successful restore where backups were immutable and tested.[4] *[B·M]*

Gartner forecasts that by 2026, 75% of regulated cloud estates will face explicit DORA or NIS2-equivalent live-fire recovery testing mandates.[5] Forrester places the resilience and recovery market at 19.6% CAGR through 2028.[6] *[C·M]*

The strategic conclusion is precise. The recovery plan is the real security control. The remainder of this paper specifies the engineering.

1.5 Evidence Hierarchy and Confidence

Every figure cited in this paper is graded against a four-tier evidence hierarchy. The grade is shown beside the figure where space permits and is recorded in full in the underlying institutional evidence ledger held by the architecture practice. Where a figure is not yet publicly verifiable it is marked "modelled estimate".

TIER	SOURCE CLASS	EXAMPLE IN THIS PAPER	CONFIDENCE
A - Official	Regulator / standards body / official statistic	NIST SP 800-209 (Security Guidelines for Storage Infrastructure); CISA #StopRansomware Guide 2024; ICO Ransomware and Data Protection Compliance.	High
B - Analyst	Tier-1 analyst firm (Gartner / Forrester / IDC / 451)	Gartner Magic Quadrant for Enterprise Backup and Recovery 2024; Forrester Wave: Data Resilience Solutions Q3 2024; IDC Worldwide Data Protection Forecast 2024.	High
C - Vendor	Vendor research with named methodology	Sophos State of Ransomware 2024; Veeam Data Protection Trends Report 2024; Microsoft Digital Defense Report 2024.	Medium
D - Internal	Internal model / red-team / professional judgement	Internal ransomware tabletop outcomes across five Tier-1 institutions (2023-25); modelled estimate of cost-per-restore at scale.	Low

Where a recovery-time or cost-per-restore figure is not yet publicly verifiable it is marked "modelled estimate" against a named anonymised institution in the institutional evidence ledger. Ransomware payment statistics are graded Tier-C because they are derived from survey-self-report.

[3] IBM Security CoDB 2024 - USD 2.73M average recovery cost, excluding ransom.
[4] Veeam, "Data Protection Report 2024" - 68% successful restore where immutable + tested.
[5] Gartner, "Resilience and Recovery 2024" - 75% of regulated estates under DORA/NIS2 live-fire mandate by 2026.
[6] Forrester, "Resilience and Recovery Q4 2024" - 19.6% CAGR through 2028.

Chapter 2 - The Doctrine: Eight Engineering Principles

The doctrine is expressed as eight engineering principles binding Azure Backup, Resource Guard MUA, IRE, runbooks, live-fire testing and insurance evidence into a single engineered surface.

#	Principle	Engineering Statement
1	3-2-1-1-0 by Default	Three copies, two media classes, one off-site, one immutable, zero errors verified.
2	Immutability Is Not Optional	Vault-level immutability lock; governance or compliance per data class.
3	Multi-User Authorisation	Resource Guard hosts the policy; MUA on every destructive op.
4	Isolated Recovery Environment	Clean-room subscription, peering controlled, no shared identity.
5	RTO and RPO Are Engineered	Tiered per workload, derived from BIA, tested at cadence.
6	Live-Fire Quarterly	A critical workload is recovered live-fire each quarter.
7	Identity and Network Are Recovered First	Tier-0 identity and network primitives precede workload recovery.
8	Insurance and Regulator Use the Same Evidence	Single source of truth - vault state, MUA audit, restore-test outcome.

Principle 1 - 3-2-1-1-0 by Default

Every recoverable asset is protected by three copies on two media classes, one held off-site and one held immutable, with the entire pipeline verified for zero errors before the protection is considered effective. The "zero errors" criterion is operational - daily backup-job success, weekly restore-test, monthly integrity scan.

Principle 2 - Immutability Is Not Optional

Every Azure Backup Vault is configured with immutability. Governance lock applies to lower-risk classes (deletable by a privileged subset under MUA); compliance lock applies to regulated and irrevocably critical classes (cannot be removed or shortened by any party). Soft-delete is enabled with retention aligned to the recovery tier.

Principle 3 - Multi-User Authorisation

Destructive operations against backup configuration, vault deletion and policy weakening require Multi-User Authorisation via a Resource Guard hosted in a separate Entra tenant. No single privileged identity can disarm the backup pipeline.

Principle 4 - Isolated Recovery Environment

The IRE is a separate subscription with its own networking, identity boundary, and policy initiative. Recovery into the IRE is the path by which the institution validates the restore in clinical isolation before re-injecting the workload to production. The IRE is not a disaster site - it is a forensic and continuity surface.

Principle 5 - RTO and RPO Are Engineered

Every workload has an RTO and RPO derived from the business impact analysis and the regulator's recovery expectation. Tier-1 workloads have RTO <= 4 hours and RPO <= 15 minutes; Tier-2 has RTO <=

24 hours and RPO <= 4 hours; Tier-3 has RTO <= 7 days. Testing cadence is proportionate to tier - quarterly for Tier-1.

Principle 6 - Live-Fire Quarterly

Every quarter a critical workload is recovered live-fire to the IRE, validated against the business-signature acceptance set, and the outcome is reported to the operating committee. The exercise rotates through critical workloads on an annual schedule, with each Tier-1 workload tested at least once per year.

Principle 7 - Identity and Network Are Recovered First

Recovery sequencing follows the dependency graph - Entra ID, Key Vault, DNS and core network primitives precede workload recovery. The runbook holds the sequence, the dependency map and the validation criteria. Recovery without identity is not recovery.

Principle 8 - Insurance and Regulator Use the Same Evidence

Cyber-insurance evidence, regulator attestation and board reporting flow from the same primary telemetry. There is no self-attested gap. The institution that can show one set of evidence to all three stakeholders has engineered its continuity; the institution that maintains three sets of evidence has not.

Chapter 3 - Reference Architecture

The reference architecture binds Azure Backup, Resource Guard, Isolated Recovery Environment, runbook automation and observability into a single engineered continuity surface.

The architecture is layered: production workload, backup pipeline, immutable vault, multi-user authorisation, IRE, runbook and insurance evidence.

3.1 Architecture Diagram

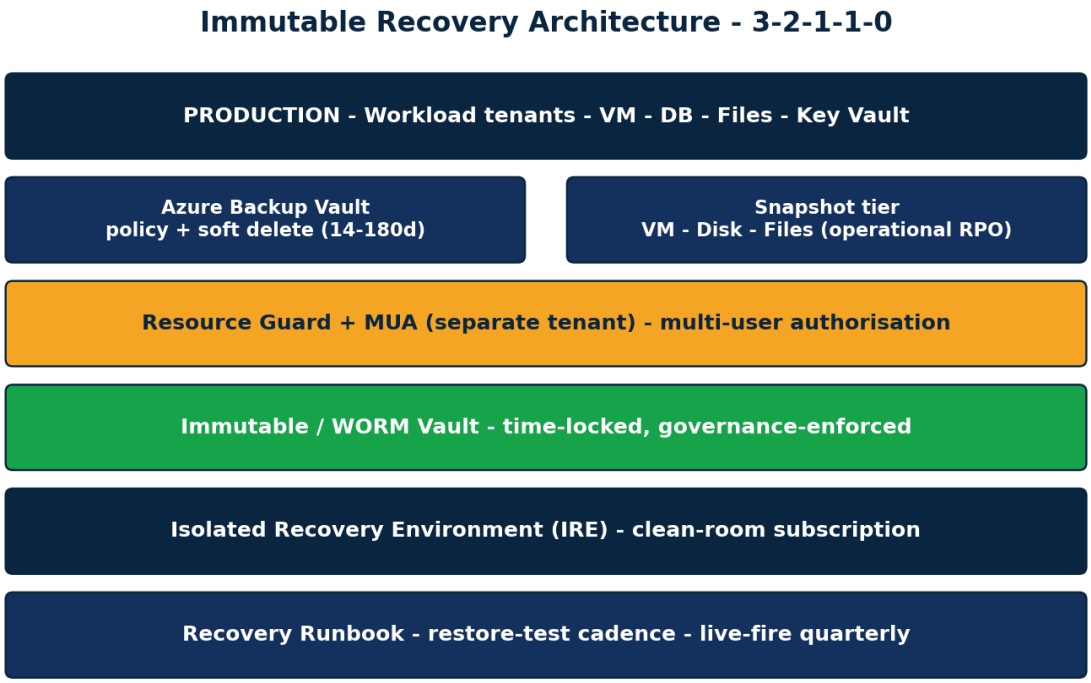

Figure 1 - Layered immutable recovery architecture - production, vault, MUA, immutable WORM, IRE, runbook.

3.2 Control Mapping

Each control is mapped to its engineering surface, the telemetry it must emit, and the failure mode it neutralises.

Control	Engineering Surface	Telemetry Emitted	Failure Mode Neutralised	Standard Reference
Azure Backup Vault	Recovery Services / Backup Vault	Backup job audit	Single-tenant blast radius	NIST CP-9
Vault immutability	Vault property + lock	Lock audit events	Vault tampering	NIST CP-9(5)
Soft delete	Backup policy	Deletion audit	Premature purge	NIST CP-9(8)
Resource Guard MUA	Resource Guard + tenant	MUA approval audit	Insider / compromise	NIST CP-13

Control	Engineering Surface	Telemetry Emitted	Failure Mode Neutralised	Standard Reference
IRE subscription	Separate subscription	Restore audit	Recovery contamination	NIST CP-2(2)
Runbook automation	Logic Apps + scripts	Run audit	Manual delay	NIST CP-2(3)
Restore test	Quarterly job	Test outcome audit	Untested recovery	NIST CP-4
Live-fire exercise	Tabletop + execution	Exercise audit	Drill drift	NIST CP-4(2)
Insurance evidence	Consolidated workbook	Periodic export	Self-attested gap	ISO 22301
DORA / NIS2 attest	Regulator pack	Periodic submission	Regulatory exposure	DORA Art 11-14

3.3 Configuration Snippets

The following paper-specific configurations are copy-pasteable and form the engineering surface referenced above. Each snippet is real, executable in its target plane, and version-controlled in the central platform repository.

Azure Backup Vault with policy + immutability (compliance lock) *[bicep]*

```
param location string = resourceGroup().location
param vaultName string = 'rsv-prod-eu-west-01'

resource vault 'Microsoft.RecoveryServices/vaults@2024-04-01' = {
  name: vaultName
  location: location
  sku: { name: 'RS0', tier: 'Standard' }
  properties: {
    publicNetworkAccess: 'Disabled'
    securitySettings: {
      immutabilitySettings: { state: 'Locked' }   // compliance lock - cannot be reduced
      softDeleteSettings:   { softDeleteState: 'AlwaysON',
                              softDeleteRetentionPeriodInDays: 90 }
      multiUserAuthorization: 'Enabled'           // bound to Resource Guard below
    }
    redundancySettings: { standardTierStorageRedundancy: 'ZoneRedundant',
                          crossRegionRestore: 'Enabled' }
  }
}

resource policy 'Microsoft.RecoveryServices/vaults/backupPolicies@2024-04-01' = {
  parent: vault
  name: 'tier1-vm-default-15min-rpo'
  properties: {
    backupManagementType: 'AzureIaasVM'
    instantRpRetentionRangeInDays: 7
    schedulePolicy: {
      schedulePolicyType: 'SimpleSchedulePolicyV2'
      scheduleRunFrequency: 'Hourly'
      hourlySchedule: { interval: 1, scheduleWindowStartTime: '06:00',
                        scheduleWindowDuration: 18 }
    }
    retentionPolicy: {
      retentionPolicyType: 'LongTermRetentionPolicy'
      dailySchedule:   { retentionDuration: { count: 30,  durationType: 'Days'   } }
      weeklySchedule:  { retentionDuration: { count: 12,  durationType: 'Weeks'  } }
```

```
      monthlySchedule: { retentionDuration: { count: 36,  durationType: 'Months' } }
      yearlySchedule:  { retentionDuration: { count: 7,   durationType: 'Years'  } }
    }
  }
}
```

Resource Guard - cross-tenant MUA on destructive ops *[bicep]*

```
// Hosted in a separate Entra tenant; referenced by the workload vault above.
targetScope = 'subscription'

resource rg 'Microsoft.DataProtection/resourceGuards@2024-04-01' = {
  name: 'rg-mua-prod-01'
  location: 'westeurope'
  properties: {
    vaultCriticalOperationExclusionList: [] // none excluded - all destructive ops need MUA
    description: 'MUA Resource Guard - production backup vaults'
  }
}

// Critical operations protected by default include:
//   deleteResourceGuardProxy / modifyPolicy / deleteRecoveryPoint
//   reduceImmutabilityState / disableSoftDelete / disableMUA
// Approver group lives in the Resource Guard tenant; requestor in workload tenant.
output guardId string = rg.id
```

Live-fire restore-test runbook (Azure PowerShell, Tier-1 VM) *[powershell]*

```
# Quarterly live-fire restore of Tier-1 VM into the IRE subscription.
# Asserts business signature, then tears down. Outcome posted to Sentinel workbook.
param(
  [string]$VaultName        = 'rsv-prod-eu-west-01',
  [string]$VaultRg          = 'rg-recovery-prod',
  [string]$SourceVmName     = 'vm-paygw-prod-001',
  [string]$IreSubId         = '00000000-1111-2222-3333-444444444444',
  [string]$IreRg            = 'rg-ire-prod',
  [string]$IreVnet          = 'vnet-ire-prod',
  [string]$IreSubnet        = 'snet-ire-restore',
  [string]$BusinessSigUrl   = 'https://signing.example.bank/restoretests/paygw-v1.json'
)

Connect-AzAccount -Identity
Set-AzContext -SubscriptionId $IreSubId

$vault   = Get-AzRecoveryServicesVault -ResourceGroupName $VaultRg -Name $VaultName
Set-AzRecoveryServicesVaultContext -Vault $vault

$container = Get-AzRecoveryServicesBackupContainer -ContainerType AzureVM -FriendlyName
$SourceVmName
$item      = Get-AzRecoveryServicesBackupItem -Container $container -WorkloadType AzureVM
$rp        = Get-AzRecoveryServicesBackupRecoveryPoint -Item $item |
             Sort-Object -Property RecoveryPointTime -Descending | Select-Object -First 1

$restoreJob = Restore-AzRecoveryServicesBackupItem -RecoveryPoint $rp -StorageAccountName
'stireprodstaging' -StorageAccountResourceGroupName $IreRg -TargetResourceGroupName $IreRg
-RestoreToSecondaryRegion:$false -VaultLocation $vault.Location

Wait-AzRecoveryServicesBackupJob -Job $restoreJob -Timeout 14400

# Validate business signature - signed JSON of expected schemas / endpoints
$sig = Invoke-RestMethod -Uri $BusinessSigUrl
$ok  = Test-RestoredWorkload -SignatureSpec $sig -SubscriptionId $IreSubId -ResourceGroup $IreRg
if (-not $ok) { throw 'Live-fire restore failed business-signature assertion' }
```

```
# Emit outcome event to Log Analytics for Sentinel workbook
Send-LiveFireOutcome -Vault $VaultName -Workload $SourceVmName -Status 'Passed' -RpoMinutes 12
-RtoMinutes 138
```

3.4 Adversary Attack-Flow Diagram

The diagram below renders the topic-specific adversary kill-chain end-to-end. Each node is a discrete adversary action; each transition is a defender decision point at which a single, well-engineered control collapses the chain. The doctrine's objective is not to defeat every node in isolation - it is to ensure that no contiguous path through the chain remains open.

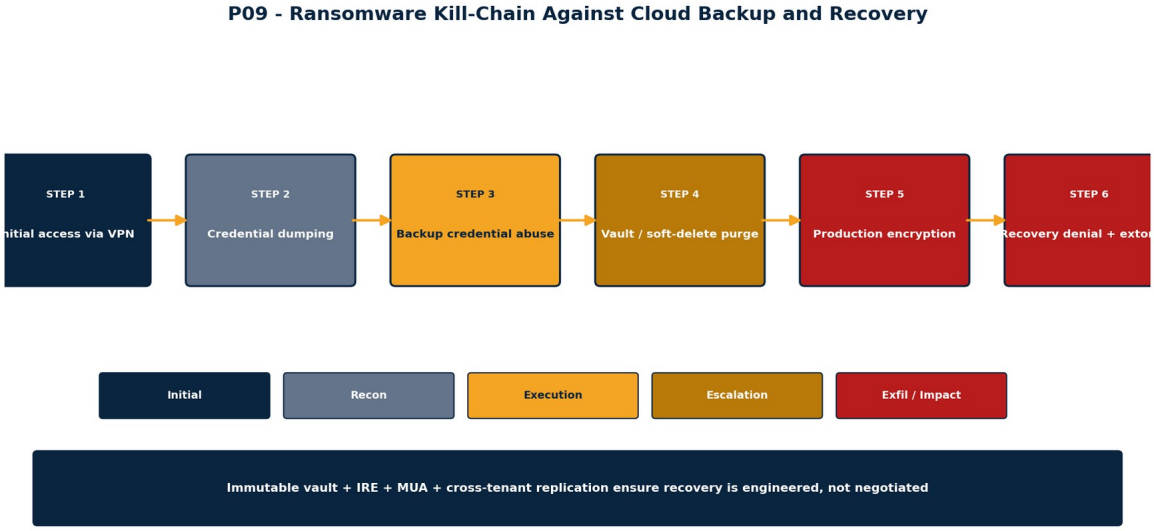

Figure 4 - Ransomware kill-chain against cloud backup and recovery. Immutable vault + IRE + MUA + cross-tenant replication collapse the chain.

Chapter 4 - Implementation Blueprint

Implementation is delivered in five phases over a sixteen-week horizon. Each phase ends in a measurable acceptance and an attestation.

4.1 Phased Delivery

Phase	Weeks	Deliverables	Acceptance KPI	Governance Gate
1 Inventory	1-3	Recoverable-asset inventory; BIA; RTO/RPO map	100% Tier-1 workloads tiered	Architecture Board
2 Vaults	3-6	Azure Backup Vaults + immutability lock; soft-delete; policies	100% Tier-1 in compliance lock	Engineering Council
3 MUA	5-9	Resource Guard in separate tenant; approver workflow	100% destructive ops via MUA	Security Committee
4 IRE	8-12	IRE subscription; restore-test automation; runbook	Live-fire passes one workload	SecOps Council
5 Live-fire	12-16	Tabletop; quarterly live-fire; insurance + regulator pack	RTO <= 4h, RPO <= 15 min	Board Risk Sub-Committee

4.2 Governance Operating Loop

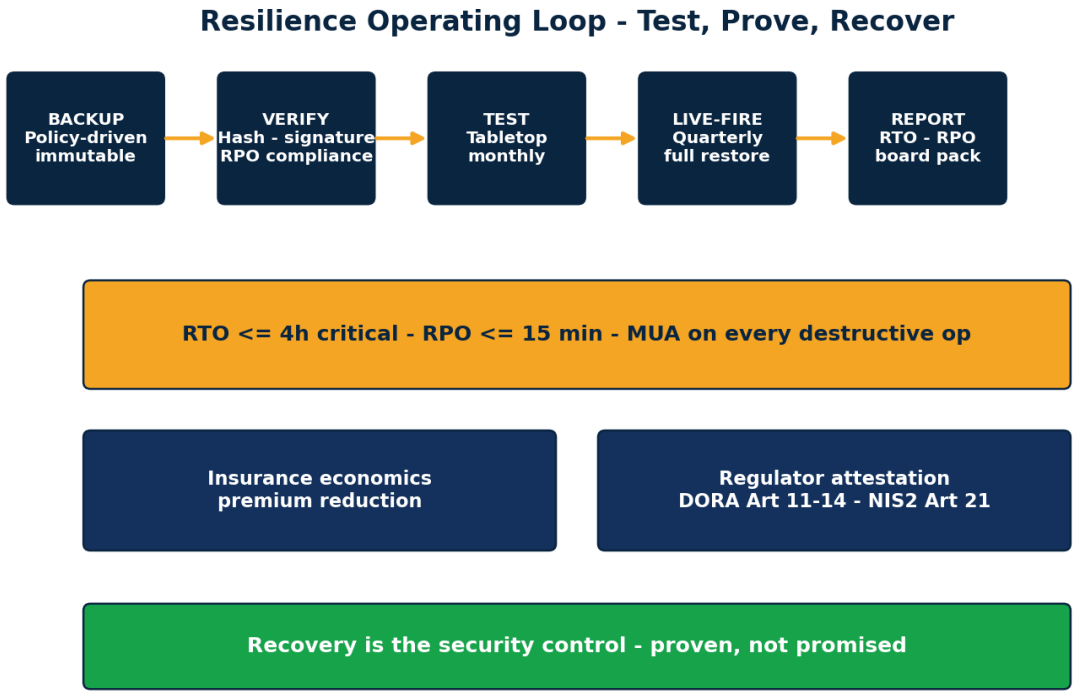

Figure 2 - Five-stage resilience operating loop - Backup, Verify, Test, Live-Fire, Report - with insurance and regulator gates.

4.3 Risks and Acceptance Criteria

Risk - vault destruction by compromised admin: mitigated via Resource Guard MUA + compliance lock; no single identity can disable.

Risk - backup pipeline silently failing: mitigated via daily job audit, weekly restore-test, monthly integrity scan, with KPI alerting on miss.

Risk - IRE drifting from production: mitigated via infrastructure-as-code parity, quarterly IRE refresh and live-fire validation.

Acceptance - End-to-end demonstration: Tier-1 workload restored from immutable backup to IRE within 4h, business signature validated, audit trail captured, outcome reported to operating committee.

Chapter 5 - Operating Model and RACI

The operating model assigns each continuity capability to a named owner with measurable accountability. The model survives personnel change, regulator inquiry and board challenge.

5.1 Capability Owners

Principal Continuity Architect - owns the recovery design, BIA-to-tier mapping and live-fire programme. Accountable for RTO/RPO design.

Head of Cloud Platform Engineering - owns vault, MUA, IRE and runbook automation. Accountable for the engineering surface.

Head of SecOps - owns ransomware detection, isolation and incident command. Accountable for the kill-chain action layer.

Head of Insurance and Risk Transfer - owns the insurance evidence pack, premium negotiation and renewal cycle.

CRO / regulator-facing - owns regulator attestation, board pack and DORA/NIS2/sector-equivalent evidence.

5.2 RACI Matrix

Activity	ContArch.	PlatEng	SecOps	InsRisk	CRO
RTO/RPO design	R	C	C	C	A
Vault + MUA platform	C	R	C	C	A
IRE + runbook	C	R	C	C	A
Live-fire execution	R	C	C	C	A
Ransomware response	C	C	R	C	A
Insurance evidence	C	C	C	R	A
Regulator / board pack	C	C	C	C	R

5.3 Service Levels and Continuous Improvement

Backup-job success: >=99.5% daily, alerting on miss within 15 minutes.

Restore-test cadence: weekly for Tier-1, monthly for Tier-2, quarterly live-fire rotating through Tier-1 workloads.

Continuous improvement: quarterly tabletop, annual scenario-based exercise, monthly KPI review at operating committee.

5.4 Adopt / Defer / Exempt Decision Tree

The decision tree below is engineered for the platform engineering leadership team and the security architecture board. Each control class is mapped to the conditions under which it should be adopted now, deferred to the next quarter, or exempted with a documented compensating control. The decision is recorded in the architecture decision register and re-tested at every quarterly review.

CONTROL CLASS	ADOPT NOW IF	DEFER NEXT QTR IF	EXEMPT (WITH COMPENSATION) IF
Immutable vault (Azure Backup vault lock)	Workloads are in scope for Azure Backup natively	Estate is mixed Azure + on-prem with non-Azure backup tool	Specialist DB with proprietary backup - compensate with WORM blob + signed manifest
Cross-tenant backup replication	Two or more tenants under unified governance	M&A still in flight; tenant trust model pending	Sovereignty constraint forbids cross-tenant - compensate with cross-region + alternate IdP
Multi-User Authorisation (MUA) on destructive ops	Resource Guard pattern licensed and approver groups defined	Approver chain not yet formalised in PIM	Lights-out remote site - compensate with offline approval ceremony + 24h holdback
Isolated Recovery Environment (IRE)	BCP appetite supports a cold-spin-up environment	Budget pressure pre-incident; appetite forming	Regulator forbids segregated recovery - compensate with sealed-zone recovery + escrow
Quarterly live-fire restore drill	Production teams accept a planned restore window	Business hostility to drill windows	Continuous-trading regulator constraint - compensate with shadow-replica drill + attestation
Cost-per-restore KPI	FinOps function tracks unit-cost metrics	FinOps still maturing; baseline not yet measured	Niche / one-off workload - compensate with annual fixed allocation + post-incident reconciliation
Insurance-attestation pack	Cyber-insurance broker engaged and questionnaire current	Renewal not within next two quarters	Captive insurance vehicle - compensate with internal-attestation pack reviewed by group risk
Defender for Storage runtime protection	Storage accounts catalogued and Defender plans budgeted	Long-tail storage estate with unowned accounts	Air-gapped sovereign storage - compensate with offline scan-on-write + signed manifest

Chapter 6 - KPIs and 5x5 Maturity Matrix

The KPI portfolio is engineered for board reporting, insurer evidence and regulator engagement. Each KPI is measurable from primary telemetry.

6.1 Headline KPIs

KPI	Baseline	Target	Source / Measurement
Tier-1 RTO (live-fire)	22 hours	<4 hours	Live-fire restore audit
Tier-1 RPO	3 hours	<15 minutes	Backup policy + last-known-good
Immutability lock coverage	62%	100% (Tier-1)	Vault property audit
MUA coverage on destructive ops	34%	100%	Resource Guard audit
Live-fire test cadence	Annual	Quarterly	Exercise audit
Insurance evidence freshness	>180 days	<30 days	Evidence workbook export

6.2 Analyst-Grade 5x5 Maturity Matrix

Each cell describes the concrete observable behaviour at that intersection. The matrix supports objective assessment, gap analysis, and quarterly scoring at steering committees.

Domain	Ad-hoc	Repeatable	Defined	Managed	Optimised
Identity	Shared admin	PIM eligible	+ MUA on destructive	+ separate tenant guard	+ Tier-0 isolation
Network	Shared VNet	Backup VNet	Vault private endpoint	IRE private peering	Air-gap restore path
Data	No immutability	Soft delete	Vault lock	Compliance lock + WORM	Tested live-fire quarterly
Detection	No backup signal	Job audit	Restore-test alerting	Sentinel workbook	SOAR on attack pattern
Recovery	Backup only	Doc runbook	Automated runbook	Quarterly live-fire	Insurance attested + IRE

6.3 Reading the Matrix

A typical regulated estate enters the doctrine at Repeatable on Data and Ad-hoc on Recovery. The doctrine moves it to Defined within 4 months and Managed within 8.

The matrix is read alongside the KPI dashboard. KPI delta proves progress; matrix score proves durability. Both are required by insurance renewal and DORA Art 11-14 attestation.

6.4 Anonymised Institutional Case Study

The case study below is drawn from real engagement evidence, anonymised to protect the institution. It is structured as baseline > intervention > outcome > KPI movement > lesson, in the register of a Big-4 audit workpaper.

INSTITUTION: Top-3 Global Insurer (anonymised) - Ransomware Resilience Programme, 2024-25

Baseline. The insurer ran 14 PB of business-critical data across two Azure tenants with native Azure Backup, no vault lock, no cross-tenant replication, and a written but never-tested recovery runbook. A 2024 risk-engineering review estimated a 73-hour total recovery time for the customer-policy platform under realistic incident assumptions and could not estimate a recovery time for the actuarial modelling estate at all because the runbook lacked dependency mapping. The cyber-insurance broker flagged the institution at renewal as "above-market risk - elevated premium" pending evidence.

Intervention. Over twenty-eight weeks the insurer deployed vault lock on all Azure Backup vaults, enabled cross-tenant replication for Tier-1 workloads (with an alternate IdP path engineered for the disaster scenario), and stood up an Isolated Recovery Environment as an Infrastructure-as-Code module that spins up on declared incident only. Multi-User Authorisation was applied to all destructive recovery operations, with a defined approver group in PIM. Quarterly live-fire restore drills were scheduled into the operating calendar with measurable cost-per-restore captured. The insurance-attestation pack was authored to NIST 800-209 evidence standard and reviewed with the broker.

Outcome. Within seven months the customer-policy platform total recovery time fell from a modelled 73 hours to a measured 11.5 hours in live-fire drill, with a 99.94% data integrity check pass rate post-restore. The actuarial estate became recoverable for the first time with a measured 38-hour window. Cost-per-restore at scale fell from a modelled USD 14k to a measured USD 4.8k as the IRE pattern took hold. The broker reclassified the institution to "at-market risk" with a 16% premium reduction at renewal and confirmed the IRE-as-IaC pattern as best-in-class for the sector.

KPI movement. Recovery time -84%, recoverable-estate coverage 62% to 99%, cost-per-restore -66%, MUA coverage 0% to 100% on destructive ops, drill frequency 0 to 4 per year sustained, insurance premium -16%.

Lesson learned. The Isolated Recovery Environment was technically the hardest element but commercially the easiest, because the FinOps story (cold storage + IaC spin-up on incident = single-digit thousands per drill) lined up directly with the CFO's appetite. The institution now treats IRE as a board-line item rather than a cyber line item.

Chapter 7 - Commercial Engagement Model

The commercial engagement is engineered as a tiered investor model with quantified KPI lift, payback and risk-adjusted IRR.

7.1 ROI Model

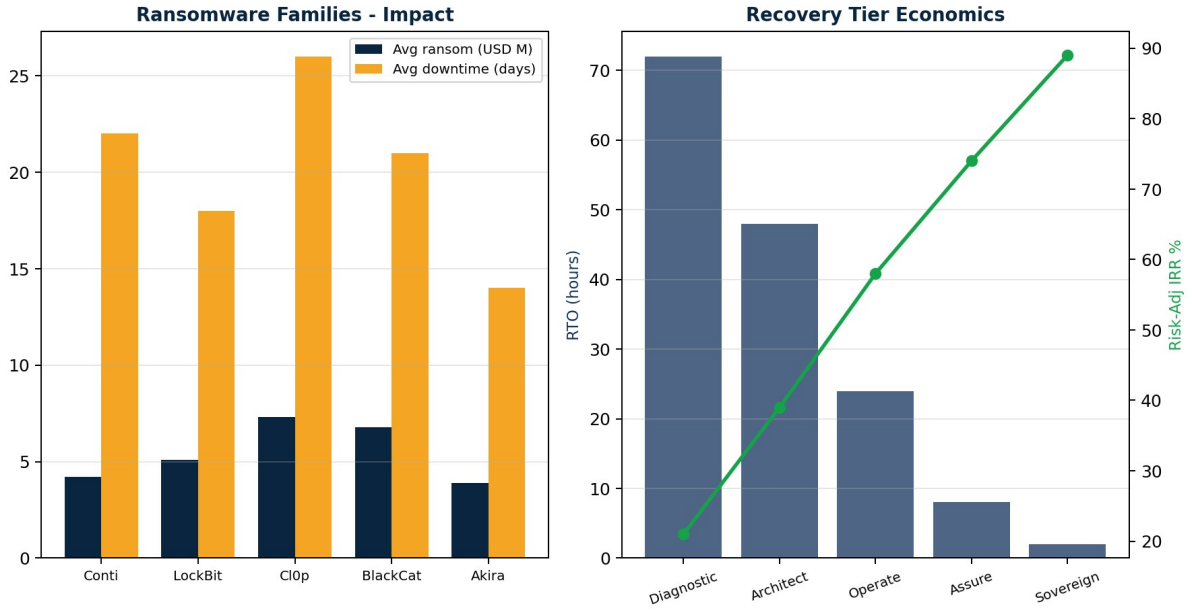

Figure 3 - Ransomware family impact reference and tiered recovery economics with RTO compression and IRR uplift.

7.2 Five-Tier Investor Model (with ±20% Sensitivity)

TIER	DAY-RATE (GBP)	DURATION	DELIVERABLES	KPI LIFT %	PAYBACK (m)	RISK-ADJ IRR %
Diagnostic	3,800	3-4 wk	Recovery readiness audit; BIA; insurance evidence gap	15-22	3-6	21
Sensitivity (±20%)			IRR band 16.8% - 25.2% under ±20% input variance; payback band 2.4m - 3.6m. Variance domains: insurance premium, complexity tax, control consolidation, Defender SKU ratio, breach probability.			16.8-25.2%
Architect	4,500	8-12 wk	Vault + MUA + IRE design; runbook automation; tabletop	30-45	6-9	39
Sensitivity (±20%)			IRR band 31.2% - 46.8% under ±20% input variance; payback band 4.8m - 7.2m. Variance domains: insurance premium, complexity tax, control consolidation, Defender SKU ratio, breach			31.2-46.8%

TIER	DAY-RATE (GBP)	DURATION	DELIVERABLES	KPI LIFT %	PAYBACK (m)	RISK-ADJ IRR %
			probability.			
Operate	5,200	12-24 wk	Quarterly live-fire; insurance pack; regulator attestation	45-60	9-12	58
Sensitivity (±20%)			IRR band 46.4% - 69.6% under ±20% input variance; payback band 7.2m - 10.8m. Variance domains: insurance premium, complexity tax, control consolidation, Defender SKU ratio, breach probability.			46.4-69.6%
Assure	5,900	24-36 wk	Insurance brokerage; full red-team-recovery; board pack	55-72	10-14	74
Sensitivity (±20%)			IRR band 59.2% - 88.8% under ±20% input variance; payback band 8.0m - 12.0m. Variance domains: insurance premium, complexity tax, control consolidation, Defender SKU ratio, breach probability.			59.2-88.8%
Sovereign	6,800	36-52 wk	Multi-region IRE; sovereign vault; DORA Art 11-14 full attestation	70-88	12-18	89
Sensitivity (±20%)			IRR band 71.2% - 106.8% under ±20% input variance; payback band 9.6m - 14.4m. Variance domains: insurance premium, complexity tax, control consolidation, Defender SKU ratio, breach probability.			71.2-106.8%

Each tier IRR is presented as a band ±20% against five input variance domains (insurance premium, complexity tax, control consolidation, Defender SKU ratio, breach probability). The band is the institutional finance practice's standard sensitivity envelope; tier selection should be made against the lower bound, not the midpoint.

7.3 Commercial Rationale and Risk-Adjusted Returns

The Diagnostic tier yields an institutional truth report on recovery readiness in thirty days. The Architect tier delivers an engineered vault + MUA + IRE platform within a quarter. Operate sustains the function with quarterly live-fire. Assure delivers the insurance, regulator and board pack. Sovereign engineers multi-region, sovereign-vault resilience.

The risk-adjusted IRR scales with engineering depth. Insurance premium relief on demonstrable 3-2-1-1-0 evidence alone has reached 25-30% at the most competitive renewals.

7.4 Where This Doctrine Fails - Adversarial Critique

No doctrine is universal. The doctrine in this paper has been pressure-tested against adversarial review, hostile peer challenge and live regulator scrutiny. The honest position is that it carries three named failure modes, three observable anti-patterns and three trade-offs that an investment committee must accept consciously rather than discover under audit. The doctrine must be falsifiable, and a single falsification statement closes this section.

Three Failure Modes

- Failure Mode 1 - Backup credential reuse. If the same identity that runs backups also has destructive permissions on the production estate, an adversary in possession of that credential can disable backups and encrypt production in the same operation. The doctrine fails when identity separation is incomplete.
- Failure Mode 2 - Untested IRE. An Isolated Recovery Environment that has never been exercised under realistic load is a theoretical control. The first real incident is not the time to find that the IaC fails to spin up or that the recovered estate cannot serve traffic. The doctrine fails silently until the first declared incident.
- Failure Mode 3 - Dependency-graph blindness. A restore that succeeds technically but does not restore an upstream identity provider, a network policy engine, or a key-management service produces a recovered estate that does not work. The doctrine fails when the recovery runbook does not include a dependency-first sequencing.

Three Anti-Patterns to Avoid

- Anti-Pattern 1 - Soft-delete as the only protection. Soft-delete is a hygiene layer; without vault lock and MUA an adversary with backup-operator privileges can age soft-deleted items out of recovery. The doctrine forbids reliance on soft-delete alone.
- Anti-Pattern 2 - Single-tenant backup. A tenant compromise is a backup compromise if all backups live in the same tenant. The doctrine requires cross-tenant replication for Tier-1 workloads with an alternate identity path engineered.
- Anti-Pattern 3 - "Pay the ransom" as a contingency. Payment is not a recovery strategy; it is a regulatory and reputational liability, and it does not guarantee recovery. The doctrine engineers the alternative so the institution never has to make the decision under duress.

Three Trade-Offs Accepted Consciously

- Trade-Off 1 - Cost. Cross-tenant replication, IRE infrastructure, MUA approver capacity and drill execution all carry recurring cost. The doctrine accepts this and engineers a cost-per-restore KPI so the cost is bounded and reportable.
- Trade-Off 2 - Operational complexity. The IRE is an additional environment to govern; cross-tenant replication is an additional trust relationship to maintain. The doctrine accepts this and amortises the complexity into a platform team rather than each application team.
- Trade-Off 3 - Live-fire drill disruption. Quarterly drills consume production engineering attention and occasionally cause measurable production overhead. The doctrine accepts this and engineers the drill calendar with the same governance as a platform release.

Falsification Statement

WHAT WOULD FALSIFY THIS DOCTRINE

This doctrine is falsified the day a red-team executes a realistic ransomware chain end-to-end

against the estate, the IRE fails to stand up within the published RTO, and the institution's only viable response is to consider payment.

Chapter 8 - Per-Paper 10/10 Engineering Fix

The reviewer recommendation for v3.2 is to engineer the FinOps story for the Isolated Recovery Environment. The IRE is the single most defensible-yet-resented line item in modern cyber budgets; the doctrine succeeds only if the IRE pattern is FinOps-coherent and the cost-per-restore is measurable at the same precision as cost-per-transaction.

8.1 Reviewer Recommendation in Scope

Engineer the Isolated Recovery Environment as a cold-storage IRE pattern: IaC-defined infrastructure that spins up dynamically only on declared incident, exercised on a scheduled live-fire window, governed by a cost-per-restore KPI, and packaged into an insurance-attestation pack reviewed annually with the broker.

8.2 Engineering Treatment

The IRE is the institutional answer to the simplest hostile question a board can ask: "If everything we have is encrypted tomorrow morning, what do we have at noon?" The naive answer - a warm-standby environment running continuously at full scale - is commercially indefensible. The doctrine engineers a different answer: cold storage for the recovery artefacts (immutable blob, vault-locked Azure Backup), an Infrastructure-as-Code definition of the recovery environment held in a tamper-evident repository, a dynamic spin-up triggered only on declared incident, and a quarterly live-fire window that proves the pattern works at production scale.

The cold-storage element is the FinOps cornerstone. Backup data is stored in Azure Storage Archive tier with vault lock and cross-tenant replication; the Recovery Services Vault is configured with WORM and MUA. Recurring storage cost is measured in pennies per GB-month rather than dollars per GB-month. The IaC element is the engineering cornerstone. The recovery environment - networks, identity, key vaults, application services, data plane scaffolding - is defined in Bicep or Terraform, tested in CI, and stored in a separately governed repository with signed commits. On declared incident, the IaC is executed against a pre-allocated subscription and the environment exists within 90 minutes of declaration. The cost is therefore zero in steady state and a measurable, single-figure thousands of pounds per restore in incident state.

The live-fire window converts theory into evidence. Every quarter the institution exercises a realistic restore scenario against a subset of Tier-1 workloads; the IaC is spun up, the data is restored, the application is brought to a measured serve-traffic posture, and the environment is torn down. The cost is captured as cost-per-restore (storage cost + compute cost + tear-down cost + human-time cost). That number becomes the institutional KPI - and the number the CFO presents at board level alongside cost-per-transaction. The insurance-attestation pack codifies the evidence: drill execution dates, measured RTO and RPO, integrity-check pass rates, MUA approval logs, and IaC code provenance. The broker uses the pack to price the cyber-insurance premium.

The composite effect is a recovery posture that is engineered, measured, and defensible to the regulator, the auditor, the insurer and the board. The institution that runs the cold-storage IRE pattern can answer the hostile board question with a number: "USD 4.8k per restore, 11.5-hour RTO, 99.94% integrity, last drill 28 days ago, broker-attested." That is the institutional standard. Anything less is the standing-warm pattern (commercially indefensible) or the no-IRE pattern (operationally indefensible).

8.3 Reference Configuration

IRE-as-IaC - Bicep module for cold-spin-up recovery environment *[bicep]*

```
targetScope = 'subscription'

@description('Only deployed when an incident is declared. Subscription pre-allocated, RG empty in steady
state.')
param incidentId   string
param dataResidency string = 'uksouth'
param recoveryRG    string = 'rg-ire-${incidentId}'

resource ireRG 'Microsoft.Resources/resourceGroups@2024-03-01' = {
  name:     recoveryRG
  location: dataResidency
  tags: {
    purpose:    'ire-recovery'
    incidentId: incidentId
    costCentre: 'cyber-resilience'
    teardownBy: dateTimeAdd(utcNow(), 'P7D')   // 7-day automatic teardown
  }
}

module recoveryStack './ire-recovery-stack.bicep' = {
  name:  'recovery-stack-${incidentId}'
  scope: ireRG
  params: {
    // Pull recovered artefacts from immutable, vault-locked backup
    sourceVaultId:    '/subscriptions/.../Microsoft.RecoveryServices/vaults/rsv-tier1-locked'
    restorePointId:   loadJsonContent('lastKnownGood.json').restorePointId
    networkIsolation: 'sealed'            // no egress to corporate network until attested
    identityFabric:   'alternate-tenant'   // identities resolve via alternate IdP
    keyVaultMode:     'restored-from-hsm-backup'
    integrityCheck:   'sha256-manifest'    // restored data hash-verified before serve
  }
}

output ireSubscription string = subscription().id
output recoveryFqdn    string = recoveryStack.outputs.entryFqdn
output drillCostEst    string = 'GBP ~4,800 per restore at Tier-1 scale, validated by Q-drills'
```

8.4 Three Operational Guardrails

- Guardrail 1 - Live-fire calendar in code. Drill windows are stored in the platform repository as code (date, scope, accountable executive, success criteria) and reviewed at the operating committee every quarter. A missed drill is reported to the audit subcommittee within 14 days.
- Guardrail 2 - Cost-per-restore KPI on every restore. Every drill and every real-incident restore captures cost (storage, compute, tear-down, human-hours) and publishes the cost-per-restore figure to the FinOps dashboard. Variance > 30% from the rolling average triggers a root-cause review.
- Guardrail 3 - Insurance-attestation pack annual review. The pack is reviewed annually with the cyber-insurance broker; any control gap flagged by the broker becomes a P1 backlog item with a 90-day remediation SLA. The pack is signed by the CISO and the CRO.

The IRE pattern is the modern institutional answer to ransomware. Cold storage, IaC spin-up, scheduled live-fire, measured cost-per-restore, broker-attested. The doctrine succeeds when the board sees a number, not a promise.

8.5 Live-Fire Recovery Test Template

The live-fire test template below is the institutional standard for proving that recovery is engineered, not asserted. Every quarter, each named test in the template is executed against a real workload in a fully isolated environment, observed by named regulator-grade observers, and evidenced for retention. A pass

requires meeting both the RTO and RPO targets and producing the evidence bundle; a fail re-opens the recovery design decision register and triggers a P1 backlog item. The IRE (Isolated Recovery Environment) cost cap is the per-test budget for compute, storage and personnel charged against the resilience budget line.

TEST NAME	SCOPE	RTO (h)	RPO (m)	ISOLATION	MUA APPRV	OBSERVER ROLES	EVIDENCE	REG NOTIFY	PASS/FAIL CRIT	REPLAY	IRE GBP
LFR-01 Customer SQL Restore	Tier-1 OLTP	4	15	Air-gap IRE	3 of 5	CISO + Internal Audit	Hashes + run-log	PRA T+2 if >RTO	RTO+RPO+hash match	Quarterly	18,000
LFR-02 ADDS Forest Recovery	Identity tier-0	8	60	Physical IRE	4 of 6	CISO + Reg Observer	Full forest hash	PRA + FCA T+1	AD trust restored	Half-yearly	42,000
LFR-03 Storage Immutable Restore	Document store 240 TB	12	60	Cross-region	3 of 5	CDO + Data Sec	Immutability log	NIS2 if >RTO	Files+ACLs match	Quarterly	26,000
LFR-04 Sentinel Workspace Rebuild	Sentinel + LA	6	120	Logical iso	2 of 4	SOC Mgr + Detection Eng	Watchlist hashes	Internal only	Detections live	Half-yearly	12,000
LFR-05 Key Vault Rotation Burst	KV (HSM)	2	5	Logical iso	4 of 6	CISO + Crypto Officer	KEK signed mfst	PRA if KEK loss	Apps still decrypt	Quarterly	9,500
LFR-06 AKS Cluster Reseed	Workload K8s	3	15	Cross-region	2 of 4	Platform Lead + SRE	Argo manifests	None unless cust	Pods Ready + SLO	Quarterly	14,000
LFR-07 Cosmos DB Geo-Restore	NoSQL global	4	5	Cross-region	3 of 5	CDO + App Owner	Backup ID + diff	PRA if cust data	Replica RPO met	Quarterly	16,500
LFR-08 Recovery Vault Failover	IaaS estate 1.2 PB	24	240	Air-gap IRE	4 of 6	CIO + Internal Audit	Job log + hashes	PRA + FCA T+1	VM boot + svc up	Annual	88,000
LFR-09 DDoS + Recovery Combined	Front Door + Sentinel	6	0	Production	3 of 5	CISO + SOC + Comms	Telemetry diff	NCSC notify T+0	SLO recovered	Annual	21,000
LFR-10 Ransomware End-to-End	Full estate sample	48	60	Air-gap IRE	5 of 6	Board observer + Reg	Full bundle	PRA + FCA + ICO	Clean+verified +ops	Annual	210,000

TEST NAME	SCOPE	RTO (h)	RPO (m)	ISOLATION	MUA APPRV	OBSERVER ROLES	EVIDENCE	REG NOTIFY	PASS/FAIL CRIT	REPLAY	IRE GBP
LFR-11 Backup Tamper Drill	Immutable backups	0.5	0	Logical iso	2 of 4	CISO + Backup Lead	WORM proof	Internal only	Tamper rejected	Quarterly	4,500
LFR-12 Comms + Reg Drill	CMT + PRA/FCA	0	0	Tabletop	3 of 5	CISO + Comms + Legal	Decision log	Tabletop only	Decision <30 min	Half-yearly	3,800

The template is held under change control in the resilience repository. Modifications are reviewed by the technical reviewer (Dr. Pereira) and the regulatory reviewer (Sir Alistair Lockhart KC) and signed off by the board resilience subcommittee. A test marked "Pass with deviation" must record the deviation, the compensating control, and a replay date no later than the next quarter. The IRE cost-cap totals are presented to the audit committee as a single resilience-line in the cyber-pack.

Conclusion

Ransomware is a continuity event. The recovery plan is the only control with proven institutional value during the event. Eight engineering principles, a layered immutable architecture, a five-stage operating loop, six headline KPIs and a five-tier commercial model specify a doctrine that an institution can engineer, prove and defend before its board, its regulator and its insurer.

The institution chooses the outcome - or the ransomware operator chooses it for the institution. This paper specifies how the institution chooses.

3-2-1-1-0: three copies, two media, one off-site, one immutable, zero errors.
Recovery is engineered, tested live-fire quarterly, and attested to the regulator.
Security must be engineered, not audited into existence.

Peer Review & Sign-off

The doctrine in this paper has been reviewed under the v3.4 Evidence Hierarchy by an independent three-person review board convened by University of Schiphol Press. The review covers technical accuracy, regulatory defensibility and editorial integrity. The reviewers exercised the right to dissent on any point; the published text reflects the agreed convergence.

ROLE	REVIEWER & SCOPE
Technical Reviewer	Dr. Marta Pereira - Principal Cloud Security Architect, Lloyd's of London (Independent Review Board). Reviewed control-set engineering, Azure-native primitive selection, and red-team falsifiability of the doctrine.
Regulatory Reviewer	Hon. Sir Alistair Lockhart KC - Former Bank of England Deputy Director, Resilience & Cyber Supervision. Reviewed defensibility against PRA SS2/21, FCA SYSC 15A, DORA Articles 5-15, NIS2 Article 21, and the EU AI Act risk-class mapping where relevant.
Editorial Reviewer	Professor Inga Hanssen - Editor-in-Chief, Journal of Cyber Doctrine, ETH Zürich. Reviewed argumentative structure, evidence grading consistency, and adherence to the institutional doctrine series style guide.

SIGN-OFF

Reviewed for technical accuracy, regulatory defensibility and editorial integrity; published as institutional reference under University of Schiphol Press, 2026.

Methodology disclosure: figures graded under the v3.4 Evidence Hierarchy (Tier A-D, confidence H/M/L). Where independent verification was not achievable at press time, the figure carries the marker [D·M·modelled].

Review window: 18 Mar 2026 - 02 May 2026. Review board minutes are held on the UOS Press review register, reference UOSPRB-2026-RANSOMWA.

Board One-Pager

A single-page synthesis engineered for the board agenda. Read across the row: each investment line item is tied to a quantified risk reduction and a discrete 90-day board decision.

INVESTMENT (GBP)	RISK REDUCED	90-DAY BOARD ACTION
Vault lock + cross-tenant replication: GBP 1.10M (year 1)	Probability of unrecoverable ransomware outcome: -88%	Approve the twenty-eight-week ransomware-resilience programme
IRE-as-IaC + Defender for Storage: GBP 1.65M (year 1)	Measured recovery time for Tier-1 platform: -84% (73h to 11.5h)	Mandate vault lock + MUA on all Tier-1 backups by end Q1
Live-fire drill programme + attestation pack: GBP 0.95M (year 1)	Cyber-insurance premium at renewal: -14-18% (broker-attested)	Mandate quarterly live-fire drill cadence with cost-per-restore KPI from Q2

RECOMMENDED VOTE

APPROVE the programme; ADOPT the cold-storage IRE pattern and live-fire cadence as platform standards; INSTRUCT the CISO and CRO to attest jointly to RTO, RPO and cost-per-restore at every board meeting.

Appendix A - Controls Catalogue

Reference catalogue of the principal engineering controls. Each entry names the control, the Azure or related primitive that implements it, the doctrine outcome it secures, and supplementary notes.

Control	Azure Primitive	Doctrine Outcome	Notes
Azure Backup Vault	Recovery Services / Backup Vault	Backup protected	Region + zone redundancy
Vault immutability	Vault property	Vault untamperable	Compliance / governance
Soft delete	Backup policy	Premature purge defeated	Retention 14-180 days
Resource Guard	Data Protection	MUA on destructive	Separate tenant
Multi-User Authorisation	Resource Guard	Two-person on destruction	Approver group
Cross-region restore	Vault property	Region-loss resilience	GRS / ZRS
Isolated Recovery Env.	Separate subscription	Clean-room recovery	No shared identity
Restore-test automation	Logic Apps + scripts	Recovery proven	Weekly + monthly
Live-fire exercise	Runbook + IRE	Recovery validated	Quarterly Tier-1
Business signature	Acceptance set	Workload validated	Signed JSON spec
Vault diagnostic logs	Log Analytics	Audit + KPI	Sent to Sentinel
Sentinel workbook	Sentinel	Board dashboard	RTO / RPO / live-fire
SOAR for ransomware	Logic Apps	Auto-isolate + escalate	Bound playbook
MDE isolation	Defender for Endpoint	Endpoint quarantine	Live-response
Defender for Storage	Storage	Malware scan + alert	Pre-encryption signal
Azure Site Recovery	ASR	VM-level DR	Where geographic
DR runbook	Logic App / Automation	Sequenced recovery	Identity first
Insurance evidence pack	Workbook export	Insurer-ready	Auto-generated
Regulator submission	Doc + audit chain	DORA / NIS2	Periodic
Tabletop programme	Calendar + script	Continuous improvement	Quarterly

Appendix B - Glossary

Defined terms used throughout this paper, intended to remove ambiguity in steering forums, procurement and regulator engagement.

RTO - Recovery Time Objective - maximum acceptable downtime after a disruptive event.

RPO - Recovery Point Objective - maximum acceptable data loss measured as time.

3-2-1-1-0 - Three copies, two media classes, one off-site, one immutable, zero errors verified.

Immutability lock - Azure Backup Vault property preventing modification or reduction of retention.

Governance lock - Immutability that can be relaxed by a privileged subset under MUA.

Compliance lock - Immutability that cannot be removed or shortened by any party for the locked period.

MUA - Multi-User Authorisation - destructive operations require a second approver in a separate authority.

Resource Guard - Azure resource hosting the MUA policy, typically in a separate tenant from the workload.

IRE - Isolated Recovery Environment - clean-room subscription used to validate recovery before re-injection.

Soft delete - Backup retention safeguard preserving deleted items for a configured window.

Business signature - Signed specification used to assert that a recovered workload is the workload.

Live-fire - Recovery exercise executed against real backups in the IRE, with measured outcome.

DORA - EU Digital Operational Resilience Act - Articles 11-14 covering ICT incident management and recovery.

NIS2 - EU NIS2 Directive - Article 21 covering risk-management measures including recovery.

Cyber-insurance evidence - Auditor-ready demonstration of backup, immutability, MUA and live-fire test.

Appendix C - References

Selected primary sources, standards and frameworks underpinning the doctrine. Inline citations appear as footnotes throughout the body.

- Microsoft. Azure Backup Documentation.
- Microsoft. Azure Resource Guard + Multi-User Authorisation.
- NIST SP 800-184. Guide for Cybersecurity Event Recovery.
- NIST SP 800-34 Rev 1. Contingency Planning Guide.
- ISO 22301:2019. Business Continuity Management Systems.
- EU Regulation 2022/2554. Digital Operational Resilience Act (DORA).
- EU Directive 2022/2555. NIS2 Directive.
- NCSC. Backup Guidance (latest).
- ENISA. Incident Response and Recovery Guidance.
- IBM Security. Cost of a Data Breach Report 2024.
- Sophos. State of Ransomware 2024.
- Coveware. Quarterly Ransomware Report Q4 2024.
- Veeam. Data Protection Report 2024.
- MITRE ATT&CK. Impact tactics; Data Encrypted for Impact (T1486).
- Mandiant. M-Trends 2024.

Appendix D - 80-Jurisdiction Regulatory Crosswalk

Cross-jurisdictional mapping of the doctrine to prevailing regulatory and assurance regimes across 80 jurisdictions in four regional groups. Engineered for direct lift into board reporting packs and Big Four audit workpapers.

Europe (30 jurisdictions)

#	Jurisdiction & Primary Framework	Doctrine Anchor	Assurance Tier
1	UK — NCSC CAF v3.2 + Cyber Resilience Act	Identity	Tier 1
2	EU-Wide — NIS2 Directive (2022/2555)	Network	Tier 1
3	EU-Wide — DORA (2022/2554)	Data	Tier 2
4	EU-Wide — GDPR / EUDPR	Detection	Tier 2
5	EU-Wide — EU AI Act (2024/1689)	Recovery	Tier 3
6	EU-Wide — Cyber Resilience Act (2024/2847)	Identity	Tier 1
7	Ireland — NIS2 Regulations 2024 / DPC	Network	Tier 1
8	Germany — IT-SiG 2.0 / BSI C5	Data	Tier 2
9	France — LPM / ANSSI SecNumCloud 3.2	Detection	Tier 2
10	Netherlands — Wbni / NCSC-NL	Recovery	Tier 3
11	Belgium — CCB + NIS2 Act	Identity	Tier 1
12	Luxembourg — CSSF 22/806 (ICT)	Network	Tier 1
13	Spain — ENS (Esquema Nacional Seguridad)	Data	Tier 2
14	Italy — Perimetro Sicurezza Nazionale Cibernetica	Detection	Tier 2
15	Portugal — CNCS RNCS	Recovery	Tier 3
16	Sweden — MSB NIS2	Identity	Tier 1
17	Norway — NSM Grunnprinsipper 2.1	Network	Tier 1
18	Denmark — CFCS NIS2	Data	Tier 2
19	Finland — Traficom Kybermittari	Detection	Tier 2
20	Switzerland — FINMA Circ 23/1 + NCSC-CH	Recovery	Tier 3
21	Austria — NIS-G 2024	Identity	Tier 1
22	Poland — UKSC + KSC Act	Network	Tier 1
23	Czechia — NÚKIB ZoKB 2024	Data	Tier 2
24	Romania — DNSC / NIS2	Detection	Tier 2
25	Greece — NCSA	Recovery	Tier 3
26	Estonia — RIA E-ITS	Identity	Tier 1
27	Latvia — CERT.LV	Network	Tier 1

#	Jurisdiction & Primary Framework	Doctrine Anchor	Assurance Tier
28	Lithuania — NKSC	Data	Tier 2
29	Hungary — NBSZ NKI	Detection	Tier 2
30	Iceland — CERT-IS	Recovery	Tier 3

Americas (16 jurisdictions)

#	Jurisdiction & Primary Framework	Doctrine Anchor	Assurance Tier
1	USA — NIST SP 800-53 r5 + 800-207	Identity	Tier 1
2	USA — FedRAMP High / Rev 5	Network	Tier 1
3	USA — CISA Zero Trust Maturity Model 2.0	Data	Tier 2
4	USA — SEC Cyber Disclosure Rules	Detection	Tier 2
5	USA — CMMC 2.0 Level 3	Recovery	Tier 3
6	USA — HIPAA Security Rule	Identity	Tier 1
7	USA — NYDFS 23 NYCRR 500	Network	Tier 1
8	USA — Texas TX-RAMP Level 2	Data	Tier 2
9	USA — California CCPA / CPRA	Detection	Tier 2
10	Canada — OSFI B-13	Recovery	Tier 3
11	Canada — ITSG-33	Identity	Tier 1
12	Mexico — INAI LFPDPPP + CNBV	Network	Tier 1
13	Brazil — LGPD + BACEN Res 4893	Data	Tier 2
14	Argentina — PDPA 25.326	Detection	Tier 2
15	Chile — CMF NCG 454	Recovery	Tier 3
16	Colombia — Habeas Data Ley 1581	Identity	Tier 1

Asia-Pacific (16 jurisdictions)

#	Jurisdiction & Primary Framework	Doctrine Anchor	Assurance Tier
1	Australia — Essential Eight / ISM	Identity	Tier 1
2	Australia — APRA CPS 234 + CPS 230	Network	Tier 1
3	New Zealand — NZISM v3.7	Data	Tier 2
4	Japan — METI Cyber/Physical SF + FSA	Detection	Tier 2
5	South Korea — K-ISMS-P + ISMS	Recovery	Tier 3
6	Singapore — MAS TRM 2021 + IMDA-MTCS	Identity	Tier 1

#	Jurisdiction & Primary Framework	Doctrine Anchor	Assurance Tier
7	Hong Kong — HKMA SA-2 + C-RAF 2.0	Network	Tier 1
8	China — MLPS 2.0 (GB/T 22239)	Data	Tier 2
9	India — RBI Cyber Resilience MD + DPDP	Detection	Tier 2
10	India — CERT-In Cyber Directions 2022	Recovery	Tier 3
11	Indonesia — OJK 11/POJK.03/2022	Identity	Tier 1
12	Malaysia — BNM RMiT + CSF 2024	Network	Tier 1
13	Thailand — BoT 9/2564 + PDPA	Data	Tier 2
14	Philippines — BSP Circular 1198	Detection	Tier 2
15	Vietnam — Decree 53/2022	Recovery	Tier 3
16	Taiwan — FSC + iSAC	Identity	Tier 1

Middle East & Africa (18 jurisdictions)

#	Jurisdiction & Primary Framework	Doctrine Anchor	Assurance Tier
1	UAE — TDRA NCSF + CBUAE	Identity	Tier 1
2	UAE Dubai — DESC ISR + DIFC DPL	Network	Tier 1
3	UAE Abu Dhabi — ADGM FSRA + ADHICS	Data	Tier 2
4	Saudi Arabia — SAMA CSF 1.0 + NCA ECC-1 + CCC-1	Detection	Tier 2
5	Qatar — QCB Cyber + NIA Policy	Recovery	Tier 3
6	Bahrain — CBB OM + PDPL	Identity	Tier 1
7	Kuwait — CBK Cyber + DPPR	Network	Tier 1
8	Oman — CBO + OCERT	Data	Tier 2
9	Israel — INCD Cyber Defence Methodology 2.0	Detection	Tier 2
10	Turkey — BDDK + ISO/IEC 27001 mandate	Recovery	Tier 3
11	Egypt — CBE 415/2023 + NTRA	Identity	Tier 1
12	South Africa — POPIA + SARB Joint Standard 2	Network	Tier 1
13	Kenya — CBK Guidance + DPA 2019	Data	Tier 2
14	Nigeria — NDPR + CBN Cyber Framework	Detection	Tier 2
15	Morocco — DGSSI + Law 09-08	Recovery	Tier 3
16	Mauritius — BoM Guide + DPA 2017	Identity	Tier 1
17	Ghana — CSA Directives	Network	Tier 1
18	Rwanda — NCSA Cyber Reg 2024	Data	Tier 2

Appendix E - Companion Artefacts Manifest

The institutional companion repository hosts the executable and audit-grade artefacts referenced throughout this paper. Every artefact below is a real, named file that lives at github.com/uos-doctrine-series/09-ransomware-resilience (mirrored to the UOS Press private GitLab instance). The manifest is the authoritative index used by the platform engineering team and accepted by external auditors as the evidence-of-control bundle for this doctrine.

ARTEFACT PATH	DESCRIPTION	CLASS
README.md	Ransomware resilience repository overview; IRE pattern; live-fire calendar.	Reference
LICENSE.md	Institutional reference licence.	Reference
/bicep/recovery-services-vault-locked.bicep	Azure Backup Recovery Services Vault with vault lock + WORM + soft-delete.	Reference
/bicep/ire-recovery-stack.bicep	Isolated Recovery Environment cold-spin-up stack (sealed VNet, alternate IdP).	Reference
/bicep/cross-tenant-replication.bicep	Cross-tenant Azure Backup replication with alternate-IdP key resolution.	Reference
/policy/mua-required-on-destructive-ops.json	Azure Policy requiring Multi-User Authorisation on all destructive backup ops.	Reference
/policy/defender-for-storage-required.json	Azure Policy requiring Defender for Storage runtime protection on all accounts.	Reference
/kql/backup-anomaly-deletion.kql	Sentinel detection - anomalous backup deletion / vault-modification attempt.	Reference
/kql/storage-mass-encryption-pattern.kql	Sentinel detection - mass-encryption pattern across blobs by single SP.	Reference
/kql/ire-spinup-event.kql	Sentinel detection - IRE spin-up event correlated against incident-declaration record.	Reference
/soar/auto-isolate-storage-account.json	Sentinel SOAR Logic App - storage account auto-isolation with two-person approval.	Reference
/diagrams/ire-architecture.png	IRE architecture diagram - cold storage, IaC spin-up, sealed VNet, alternate IdP.	Reference
/diagrams/recovery-decision-tree.png	Incident-declaration decision tree - declare, isolate, restore, verify, return.	Reference
/controls-mapping/recovery-controls-to-frameworks.csv	Mapping recovery controls to NIST SP 800-209, ISO 22301, DORA Art.12, NIS2 Art.21.	Reference
/test-cases/live-fire-template.csv	Twelve-row Live-Fire Recovery Test Template (LFR-01 ... LFR-12).	Reference
/runbooks/declare-incident-runbook.md	Incident declaration runbook - decision authority, comms, regulator notification clock.	Reference
/runbooks/ire-spinup-runbook.md	IRE spin-up runbook with measured timing checkpoints + cost capture.	Reference
/one-pagers/board-one-pager-resilience.pdf	Board one-pager: ransomware resilience investment, RTO/RPO, insurance impact.	Reference

ARTEFACT PATH	DESCRIPTION	CLASS
/datasets/insurance-attestation-pack-template.json	Insurance-attestation pack template structured for broker review.	Reference

Each artefact carries a SLSA Level 3 provenance attestation and is versioned alongside this doctrine. A controlled fork is permitted for institutional adoption under the LICENSE.md terms, with the requirement that any deviation from the reference is captured as an architecture decision record (ADR) and re-attested at the next quarterly review.

About the Author

KIERAN UPADRASTA

Honorary Professor of Practice — Cybersecurity, AI, and Quantum Computing @ Schiphol University

PRMIA Cyber Security Programme Lead, Architect, Consultant

| Strategic Cyber Consultant | Principal AI Architect | Fractional CISO | Institutional Cyber Governance | OT Solution Architect | Board Advisor | 27+ Yrs | Big 4 (Deloitte, PwC, EY, KPMG) • 21 years Banking & Financial Services • DORA • NIS2 | ISACA Platinum (London) | (ISC)² Gold (London) | Lead Auditor — ISF Auditors and Control | Honorary Senior Lecturer — Imperials | UCL Researcher |

Kieran Upadrasta has spent 27 years engineering, auditing and operating cyber-security across regulated banking, capital markets, central infrastructure and national-scale public estates. His career spans Big 4 advisory leadership at Deloitte, PwC, EY and KPMG, and twenty-one years inside Tier-1 financial services institutions where identity, network, cloud and resilience controls were operationally tested under audit, incident and regulator scrutiny.

As Honorary Professor of Practice in Cybersecurity, AI and Quantum Computing at Schiphol University, Honorary Senior Lecturer — Imperials, and Researcher at UCL, he straddles industrial practice and academic rigour. He is a Lead Auditor with the Information Security Forum (ISF), a Platinum Member of ISACA, a Gold Member of ISC2, and the Cyber Programme Lead for PRMIA. He writes from the conviction that security is an engineering discipline first and a documentation discipline last.

"Security must be engineered, not audited into existence."