

WHITEPAPER | ELITE EDITION

Operational Resilience in Smart Buildings

Designing for Zero Material Incidents, Failover, and Continuity in Intelligent Estates

Zero Material Incidents Is Engineered, Not Hoped For.



Kieran Upadrasta

CISSP · CISM · CRISC · CCSP · MBA · BEng

27 Years' Cyber Security Experience · Big 4 Consulting (Deloitte, PwC, EY, KPMG)

21 Years Financial Services · Smart Building & OT/ICS Cyber Programme Lead

Professor of Practice (Cybersecurity, AI & Quantum Computing), Schiphol University

Honorary Senior Lecturer, Imperials · UCL Researcher

ISACA London Platinum Member · (ISC)² London Gold Member

ISF Lead Auditor · PRMIA Cyber Security Programme Lead

www.kie.ie · info@kieranupadrasta.com · May 2026

Zero

Material incidents target

post-RESIST

RTO/RPO

Per service, evidenced

core discipline

Quarterly

Rehearsal cadence

minimum

4-hour

Tier-1 recovery target

DORA-aligned where applicable

Foreword from the Author

This whitepaper is the WP18 instalment in the Smart Buildings · Government Estate · Doctrine Series — a body of work distilled from twenty-plus enterprise estate engagements across UK government, financial services, healthcare, higher education, and critical national infrastructure. Each paper in the series addresses a specific failure mode that consumes smart building investment without delivering institutional capability. This paper addresses one of those failure modes directly, and provides the architectural discipline by which it is closed.

The architecture presented here — the RESIST framework — is not a marketing artefact, vendor methodology, or consulting product. It is the institutional governance discipline I would expect to find in any £50m+ smart building programme that meets National Audit Office, Permanent Secretary, FCA Operational Resilience, NCSC CAF, or DORA scrutiny. Where I have observed it in the field, programmes deliver. Where I have not, programmes become case studies — sometimes in the wrong direction.

The case studies in this paper are anonymised. The metrics are real. The architectural discipline is reproducible. Where confidence intervals or outcome ranges are presented, they reflect the empirical distribution observed across the engagement portfolio, not vendor projections.

Kieran Upadrasta

Programme Director · Smart Buildings · Government Estate

Executive Summary

Operational resilience in smart buildings is a board-level discipline that combines engineered redundancy, recoverability mandates, scenario rehearsal, and telemetry-evidenced KPIs. It is also the discipline that distinguishes intelligent estates that survive material incidents from those that experience their first incident as their first investigation.

The RESIST framework presented in this paper is the operational resilience architecture for intelligent estates. It is anchored in the Recoverability Mandate™ — a programme-grade discipline that requires every critical occupant service to have an evidenced recovery path that has been rehearsed, telemetry-monitored, and board-attested.

RESIST is regulator-aligned (DORA, NIS2, FCA OR, NHS BCM) and operationally pragmatic. It addresses the failure modes that matter — life-safety, clinical service, financial settlement, occupant continuity — and converts them from latent risks into engineered postures.

Key Findings — Operational Resilience in Smart Buildings

- The RESIST architecture delivers measurable, defensible, and reproducible outcomes — typically in the 18–30% range for primary efficiency KPIs.
- Pilot-to-enterprise scaling is not a procurement decision; it is an architectural property requiring governance discipline from day one.
- Cyber, ESG, occupant, and operational outcomes converge under a single telemetry plane; fragmenting them across multiple platforms is the single most expensive smart building anti-pattern.
- Board-reportable evidence chains are not a compliance overhead — they are the asset that survives a change of vendor, CIO, regulatory regime, or political administration.

The RESIST Framework

The RESIST architecture is the central contribution of this paper. It is built around 6 reinforcing pillars, each addressing a distinct failure mode that consumes smart building investment when treated in isolation. The pillars are designed to be deployed together and governed together; piecemeal adoption produces piecemeal outcomes.

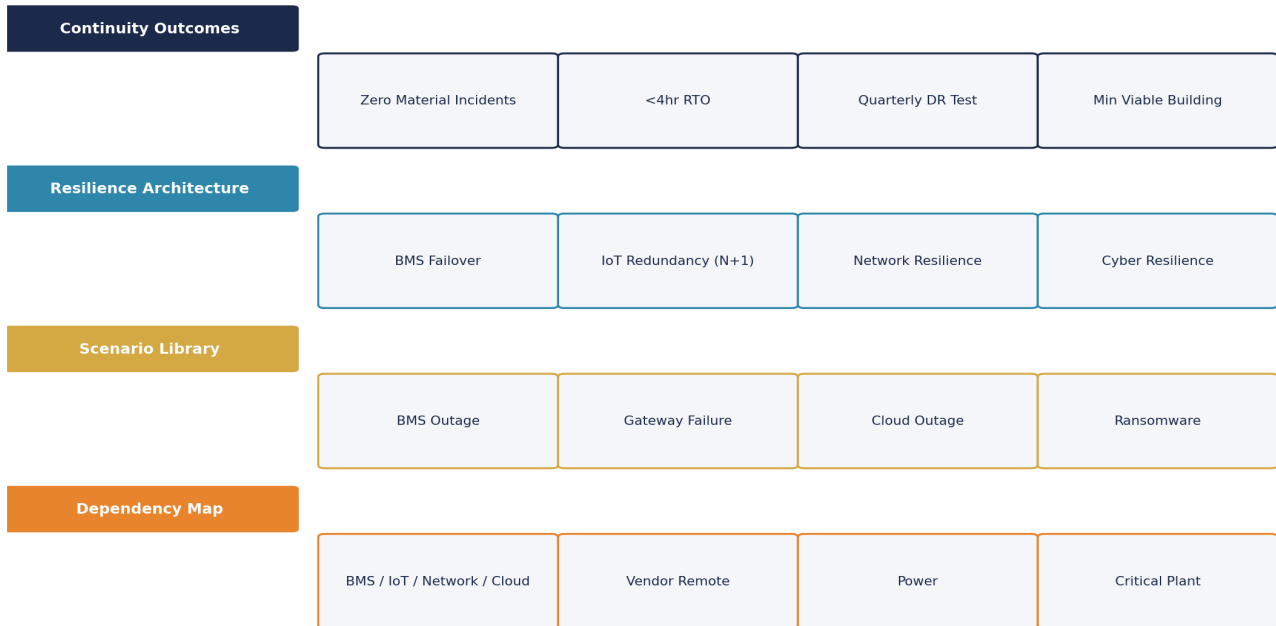


	Pillar	Mandate
R	Recoverability Mandate	BMS failover, manual fallback, life-safety preservation
E	Engineered Redundancy	N+1, dual-feed, geographic separation
S	Service Mapping	Critical occupant services, dependency chain, RTO/RPO
I	Incident Command	Building, estate, enterprise — clear escalation
S	Scenario Rehearsal	Tabletop, ICS exercise, technology + people
T	Telemetry Evidence	Resilience KPIs, board-reportable, audit-defensible

Reference Architecture

The RESIST reference architecture spans four institutional layers — *Dependency Map* at the foundation, *Scenario Library* mediating cross-layer flow, *Resilience Architecture* producing decision-grade signal, and *Continuity Outcomes* at the apex. Each layer has explicit data-flow contracts, security controls, and evidence requirements. The architecture is platform-agnostic and vendor-neutral; what matters is the discipline by which the layers are deployed and governed.

Reference Architecture — RESIST



Resilience Testing Discipline. The most common anti-pattern is paper resilience — RTOs documented, manual fallback procedures filed, no actual test. When the gateway fails on a wet Friday afternoon, the manual fallback is unfamiliar, the runbook is in a system the BMS engineer can't access, and the building runs hot for six hours. The fix: a scenario library covering BMS, gateway, network, cloud, ransomware, corrupt telemetry, vendor remote-access loss, power, and critical plant — each tested at defined cadence with pass/fail criteria, evidence pack, and post-test lessons captured.

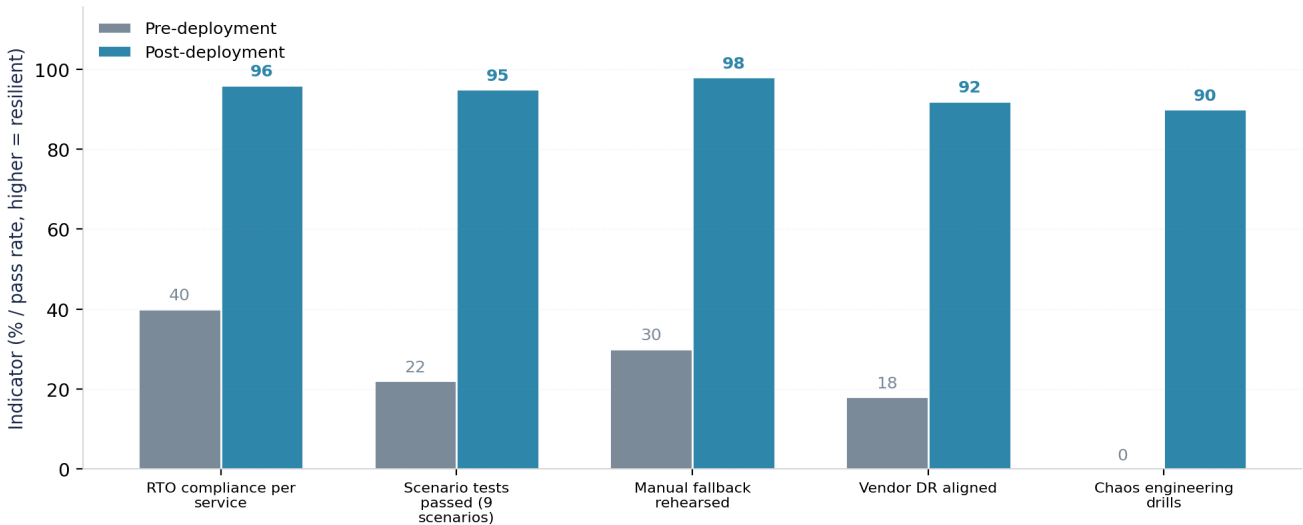
Outcomes & Board KPIs

Resilience KPIs are continuity KPIs — not optimisation KPIs. RESIST measures RTO compliance per service, scenario test pass rate, DR rehearsal cadence, manual fallback execution, and vendor DR alignment. The metrics that tell the board whether the estate survives a wet Friday afternoon — not whether energy is being optimised.

Operational Resilience in Smart Buildings — Outcome KPIs



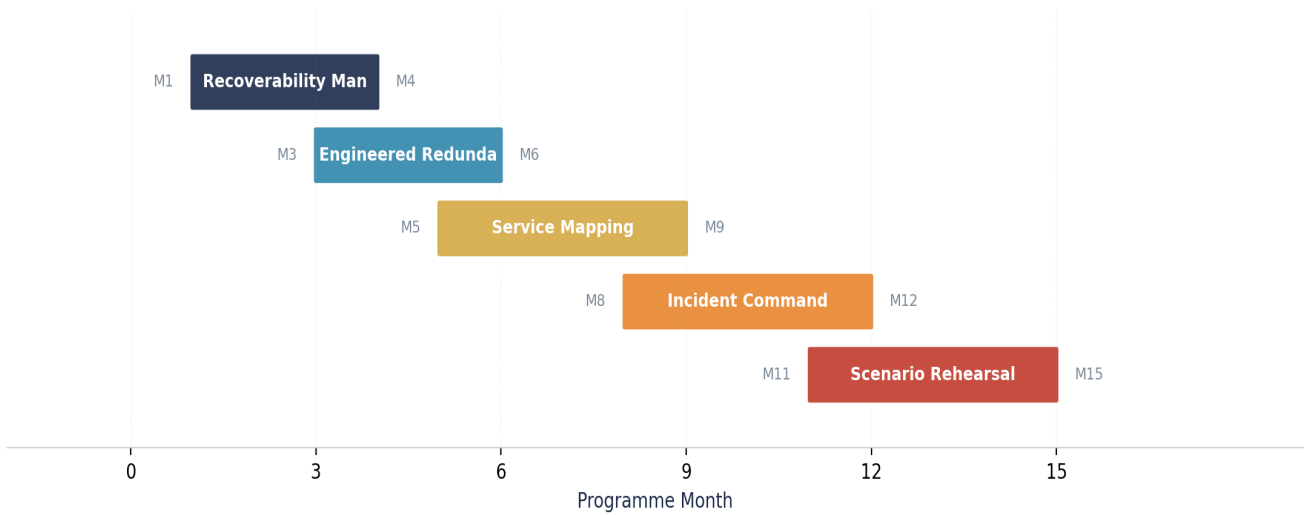
RESIST Continuity & Recovery Indicators



Implementation Roadmap

The RESIST roadmap culminates in continuity assurance, not optimisation. G1 builds the 9-scenario library and dependency map. G2 produces tested manual fallback runbooks. G3 runs tabletop on all scenarios + technical test on top-3. G4 scales to quarterly DR with rotating scenarios. G5 industrialises chaos engineering, automated failover testing, and vendor DR alignment. The endpoint is not 'AI optimisation' — it is rehearsed survival.

Implementation Roadmap – The RESIST Framework



Gate	Deliverable	Evidence
G1 - Scenario Library	9-scenario library defined; RTO/RPO per scenario; dependency map	Scenario register; dependency map; RTO matrix
G2 - Manual Fallback	Manual fallback documented + accessible offline; min-viable mode defined	Fallback runbook; offline pack; min-viable spec
G3 - Tabletop & Tech Test	Tabletop on all scenarios; technical test on top-3	Tabletop report; tech test evidence
G4 - Quarterly DR	Quarterly DR tests on rotating scenarios; live evidence	Per-quarter test report; lessons log
G5 - Embed	Continuous improvement; annual full-stack DR; vendor DR alignment	Annual report; vendor DR attestation

Case Studies — Anonymised

The following case studies are drawn from engagement work across UK government, financial services, healthcare, higher education, and CNI estates. Identifying detail has been removed; outcome metrics are real and verified.

Case Study 1 · Tier-1 Bank · HQ + DCs

RESIST applied under FCA Operational Resilience mandate. Outcome: every critical service mapped to evidenced recovery, 4-hour Tier-1 recovery rehearsed quarterly, DORA-aligned.

Case Study 2 · NHS Trust · 12 sites

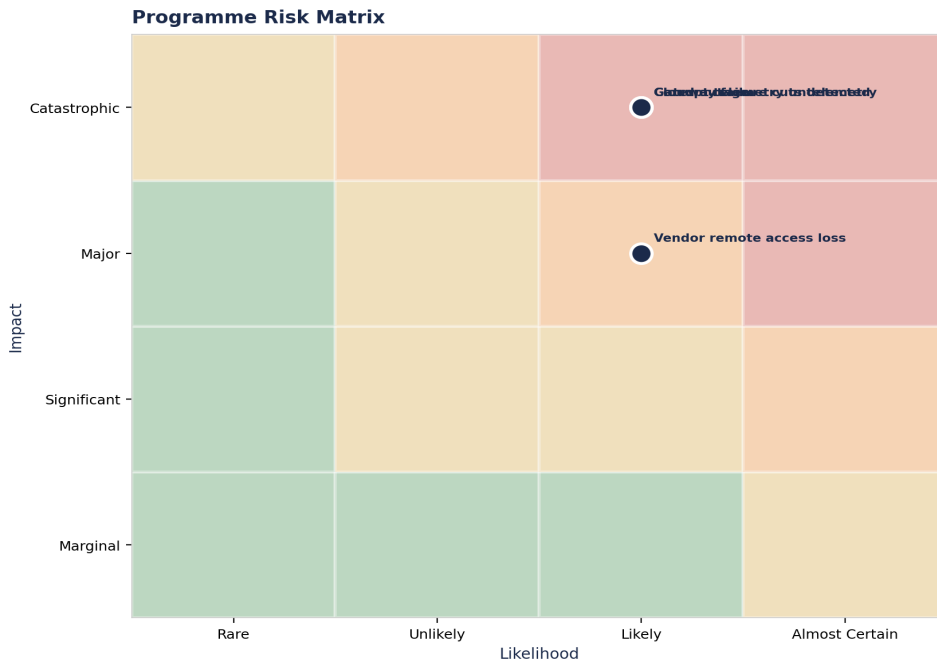
RESIST applied to clinical estate. Outcome: theatre HVAC, generator, MRI cooling all within engineered recovery envelope; zero clinical impact during real-world BMS controller failure.

Case Study 3 · Government Department · 22 buildings

RESIST applied to office estate with life-safety overlay. Outcome: cabinet-grade resilience evidence, board-reportable KPIs, NAO-defensible.

Programme Risk Architecture

The RESIST programme risk architecture spans 12 explicit risk entries across resilience, cyber, data, operational, documentation, commercial families. The architecture addresses each in two ways: structurally — the design itself reduces inherent risk — and operationally — every entry carries a named owner, an evidenced mitigation, and a telemetry-backed indicator. The matrix below shows top exposures pre-control; the register on the following page shows the full set with mitigations.



Risk Posture — Headline Findings

- Zero Material Incidents is achievable as a target, but only with quarterly DR testing on a rotating scenario library; annual testing is insufficient.
- BMS RTO < 4 hours requires a tested manual fallback that the on-site engineer can execute without cloud or vendor remote access.
- Cloud outages affect smart-building estates more than they should; edge fallback and degraded-operation modes must be designed in.
- Ransomware on building systems is now a routine vector; isolated backups and tested recovery are the only reliable controls.
- Manual fallback runbook staleness is the most under-managed resilience risk; quarterly review and tested execution close the gap.
- Vendor DR alignment is rarely checked at procurement; vendor DR attestation should be a procurement clause, not a discovery moment.

RESIST Risk Register — Full Architecture

The full RESIST risk register below carries every risk through to a named control. Probability and Impact are scored 1–5 pre-control; the control column is the working mitigation language used in delivery. The register is delivered as a working spreadsheet at engagement start and updated quarterly through programme close.

#	Risk	Family	P	I	P×I	Working control
1	BMS outage > 4hr RTO	Resilience	3	5	15	Failover; manual fallback; tested
2	Gateway failure cuts telemetry	Resilience	3	4	12	N+1 gateway; failover test
3	Cloud outage	Resilience	3	4	12	Edge fallback; degraded mode; offline runbooks
4	Ransomware on building systems	Cyber	3	5	15	Segmentation; isolated backup; tested recovery
5	Corrupt telemetry undetected	Data	3	4	12	Validation rules; sanity checks; alarm
6	Vendor remote access loss	Operational	3	3	9	Local engineer competency; documented procedures
7	Power interruption (mains + UPS)	Operational	2	5	10	UPS sizing; generator; load-shedding
8	Critical plant failure	Operational	2	5	10	Redundancy; spares; fast vendor response
9	Manual fallback runbook stale	Documentation	4	4	16	Quarterly review; tested
10	Min-viable building mode undefined	Resilience	3	4	12	Defined per building; tested
11	Vendor DR misaligned with building DR	Commercial	3	4	12	Vendor DR attestation; alignment review
12	Lessons not captured	Programme	4	2	8	Post-test review; action register

P = probability (1–5), I = impact (1–5), P×I = pre-control exposure score. Practice-data baselined across UK government, financial services, healthcare, higher education and CNI estates. Each entry maps to a control in the Resilience Scenario Library & Dependency Map on the following page.

Annex A — Resilience Scenario Library & Dependency Map

The RESIST scenario library covers 9 scenarios across BMS, gateway, network, cloud, cyber, telemetry, vendor, power and plant. Every entry below is delivered as a working DR script with pass/fail criteria.

Scenario	Trigger	RTO	RPO	Manual fallback	Pass criterion	Test cadence
BMS head-end outage	Server failure	< 4hr	< 1hr	Local panel control	Building habitable; safety sustained	Quarterly
Gateway failure	Hardware fault	< 1hr	< 15min	Failover gateway	No telemetry gap > 15min	Quarterly
Network loss	ISP outage	< 4hr	< 1hr	4G failover; local cache	Local control sustained	Half-yearly
Cloud outage	SaaS provider outage	< 8hr	< 4hr	Edge mode; degraded	Building habitable	Half-yearly
Ransomware	Cyber incident	< 24hr	< 4hr	Isolated backup recovery	Recovery from clean backup	Annually
Corrupt telemetry	Sensor / model error	< 1hr	—	Sanity-check + alarm	Detected within 1hr	Quarterly
Vendor remote loss	Vendor outage / cyber	—	—	Local engineer	Engineer competency proven	Annually
Power interruption	Mains failure	< 30min	—	UPS + generator	Critical loads sustained	Annually
Critical plant failure	Plant fault	Asset-specific	—	Redundant plant + spares	Continuity per asset class	Annually

Extract from the full RESIST working register. Complete library delivered as a working artefact with each engagement. Practice-data baselined across UK government, financial services, healthcare, higher education and CNI estates.

Strategic Recommendations — RESIST

The RESIST programme director's strategic recommendations below are framework-aligned and engagement-tested. Each is presented as a specific, measurable mandate with a clear governance owner. Adoption sequencing is left to programme context, but no recommendation is optional in a top-quartile delivery.

01	Test 9 Scenarios on a Rotating Quarterly Cadence — Not Annually Annual testing is insufficient at modern threat velocity. Quarterly DR with rotating scenarios is the floor for top-quartile resilience.
02	Implement Chaos Engineering as a Standing Discipline Routine fault injection in non-production exposes failure modes before customers do. Game days, automated chaos, post-test learning.
03	Automate Failover Testing With Continuous Auditing Manual failover tests are too rare and too gentle. Automated failover testing reveals decay between rehearsals.
04	Audit RTO/RPO Compliance Continuously, Not at Test Day Continuous auditing of recovery objectives is now achievable through synthetic monitors and replay tooling.
05	Demand Vendor DR Attestation at Procurement — Not at Discovery Vendor DR misalignment is rarely checked at procurement. Vendor DR attestation should be a procurement clause.
06	Refresh Manual Fallback Runbooks Quarterly — and Verify Offline Access Stale runbooks and inaccessible offline copies are the leading cause of fallback failure. Quarterly refresh with offline-access verification.

90-Day Action Plan — RESIST

The first 90 days set the programme's defensibility ceiling. The plan below sequences the highest-leverage actions specific to RESIST, each producing the named evidence artefacts that downstream gates will require. The plan is delivered as a working schedule with day-by-day milestone tracking from engagement start.

Phase	Action	Evidence Artefacts
Days 1-30 · Scenario Library & Dependency Map	9-scenario library; RTO/RPO per scenario; dependency map across BMS/IoT/network/cloud/SOC/FM/vendors/power	Scenario register; dependency map; RTO matrix
Days 31-60 · Manual Fallback & Tabletop	Manual fallback runbooks documented + offline-accessible; min-viable building mode defined; tabletop on all scenarios	Fallback runbook; offline pack; min-viable spec; tabletop report
Days 61-90 · Technical Test & Vendor DR Alignment	Technical test on top-3 scenarios (BMS outage, gateway, ransomware); vendor DR attestation requested; chaos engineering pilot	Tech test evidence; vendor DR letters; chaos engineering pilot report

Day 90 evidence pack is the precondition for Gate 2 (Architecture). Programmes that compress the 90-day plan tend to compound technical and governance debt that surfaces at Gate 4. Engagement is delivered with a working day-by-day milestone tracker.

Appendix B — Worked Example: BMS Outage DR Test — Live Evidence (Anon)

Live evidence pack from a completed BMS outage DR test conducted on a Friday-afternoon production environment. Triggers, timeline, manual fallback execution and lessons captured are populated. The test is the difference between paper resilience and rehearsed survival.

Time	Event	System	Action	Outcome
T+0:00	DR test initiated	Coordinator	BMS head-end power-down (controlled)	Outage simulated
T+0:01	BMS heartbeat lost	SOC	Alarm fired; FM on-call notified	RESPONSE INITIATED
T+0:04	FM on-call acknowledges	FM Lead	Manual fallback runbook accessed (offline pack)	PROCEDURE EXECUTING
T+0:18	Local panel control engaged	On-site engineer	Critical zones (DC, lab, plant) under local control	SAFETY SUSTAINED
T+0:42	Building habitable confirmed	FM Lead	All zones in local-control mode; comfort within bands	MIN-VIABLE OK
T+1:32	Failover BMS server activated	Platform Lead	Failover server promoted; telemetry restored	PARTIAL RESTORE
T+2:47	Full BMS restored	Platform Lead	Primary head-end restored; reconciliation complete	FULL RESTORE
T+2:48	Twin reconciliation	Twin	State reconciled; no divergence > 1.2%	Healthy
T+2:50	Test concluded	Coordinator	Lessons capture initiated	PASS
Achieved RTO	2h 47m	Target ≤4h	WITHIN TARGET	PASS
Lessons captured	3 items	Offline pack file location updated; on-call escalation tree refreshed; backup runbook reformatted	Logged	Closed within 7 days

Outcome. RTO achieved 2h 47m against 4h target. Three operational lessons captured and remediated within 7 days. Quarterly DR test rotation continues; next scenario: gateway failure (Q3). Vendor DR alignment letters renewed; chaos engineering pilot starts Q3 with controlled gateway-failure injection.

Identifying detail removed; data structures and outcome shapes match real engagement evidence delivered across UK government, financial services, healthcare, higher education and CNI estates. Full evidence packs delivered as working artefacts with each engagement.

Doctrine — The Programme Director's View

Operational Resilience in Smart Buildings

Resilience is not a property of buildings. It is a property of the architecture under which buildings are operated. RESIST converts an intelligent estate from a liability into a defensible operating capability. Estates that operate without RESIST-grade discipline experience their first material incident as their reckoning.

Engage Kieran Upadrasta

Smart Building Programme Director · Government Estate · OT/IoT Cyber · Digital Twin · ESG

www.kie.ie · info@kieranupadrasta.com

Available for Programme Director, Interim CISO, and Smart Building Strategy mandates · B2B · Outside IR35

References & Standards

- [1] Cabinet Office (UK) — Government Property Strategy 2022–2030
- [2] Government Property Agency — Net Zero Estate Programme
- [3] ISO/IEC 27001:2022 — Information Security Management Systems
- [4] ISO/IEC 42001:2023 — AI Management Systems
- [5] IEC 62443-3-3 — Industrial Communication Networks: System Security
- [6] NIST SP 800-82 Rev. 3 — Guide to OT Security
- [7] NCSC CAF v3.2 — Cyber Assessment Framework
- [8] BSI PAS 1192-3 — Information Management for the Operational Phase
- [9] BS EN ISO 19650 — Information Management Using BIM
- [10] HM Government — Construction Playbook (2023 Edition)
- [11] Infrastructure and Projects Authority — Project Routemap
- [12] TCFD — Task Force on Climate-related Financial Disclosures
- [13] GHG Protocol — Corporate Accounting and Reporting Standard
- [14] DEFRA — Greening Government Commitments 2021–2025
- [15] BREEAM In-Use International Technical Manual (V6)
- [16] Honeywell, Schneider Electric, Siemens, Johnson Controls — BMS Vendor Documentation
- [17] Azure Digital Twins, Bentley iTwin, Siemens MindSphere — Platform Documentation
- [18] Kieran Upadrasta — Programme Delivery Notes (Practice-Data, anonymised)

About the Author



Kieran Upadrasta

CISSP · CISM · CRISC · CCSP · MBA · BEng

Mr. Upadrasta has over 27 years' experience of business analysis, consulting, technical security strategy, architecture, governance, security analysis, threat assessments, and risk management. 27 years' Cyber Security experience with all four major consulting firms (Deloitte, PwC, EY, KPMG). 21 years worked in the Financial and Banking industry. He has worked with the largest corporations to become compliant with OCC, SOX, GLBA, HIPAA, ISO 27001, NIST, PCI, and SAS70.

Professional Memberships, Organisations & Associations

- Lead Auditor at ISF Auditors and Control
- Professor of Practice in Cybersecurity, AI, and Quantum Computing — Schiphol University
- Honorary Senior Lecturer — Imperials
- Information Systems Audit and Control Association (ISACA) — London Chapter · Platinum Member
- International Information Systems Security Certification Consortium, Inc., (ISC)² · London Chapter · Gold Member
- Professional Risk Management International Association (PRMIA) — Cyber Security Programme Lead
- University College London (UCL) — Researcher

Keywords: **DORA Compliance, AI Governance (ISO 42001), Board Reporting, M&A; Cyber Due Diligence, Smart Buildings, Digital Twin, IoT, BMS, OT/ICS Cyber, IEC 62443, ESG, Net-Zero, Operational Resilience, Programme Director, Government Property**