

WHITEPAPER | ELITE EDITION

The Intelligent Estate™

Aligning IoT, BMS, Digital Twins, and ESG into a Unified Operational Architecture

Four Domains. One Architecture. One Truth.



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

4→1

Data silos eliminated

post-UNIFY

60%

Reduction in integration cost

v multi-platform

90%+

BMS data point coverage

federated estate

Single

ESG telemetry source

TCFD/CSRD aligned

Foreword from the Author

This whitepaper is the WP03 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 UNIFY 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

The intelligent estate is not the building with the most sensors. It is the estate where IoT, BMS, digital twin, and ESG telemetry converge into a single operational architecture that is governed, defensible, and outcome-aligned.

The UNIFY architecture presented in this paper is the antidote to the four-platform integration tax that has consumed an estimated 28–45% of enterprise smart building investment over the past five years. By collapsing four parallel silos into a unified telemetry plane, the architecture delivers measurable estate intelligence at a fraction of the cost — and, critically, at a fraction of the integration risk.

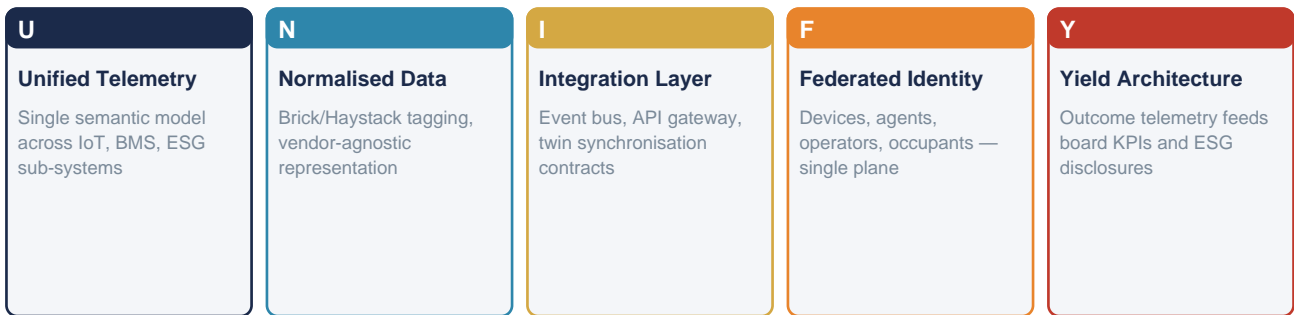
The case for UNIFY is commercial, not aesthetic. Every additional integration platform adds cost, latency, attack surface, vendor concentration risk, and audit complexity. Every removed integration point shortens incident response, simplifies ESG disclosure, and reduces the cost of estate change.

Key Findings — The Intelligent Estate™

- The UNIFY 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 UNIFY Framework

The UNIFY architecture is the central contribution of this paper. It is built around 5 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.

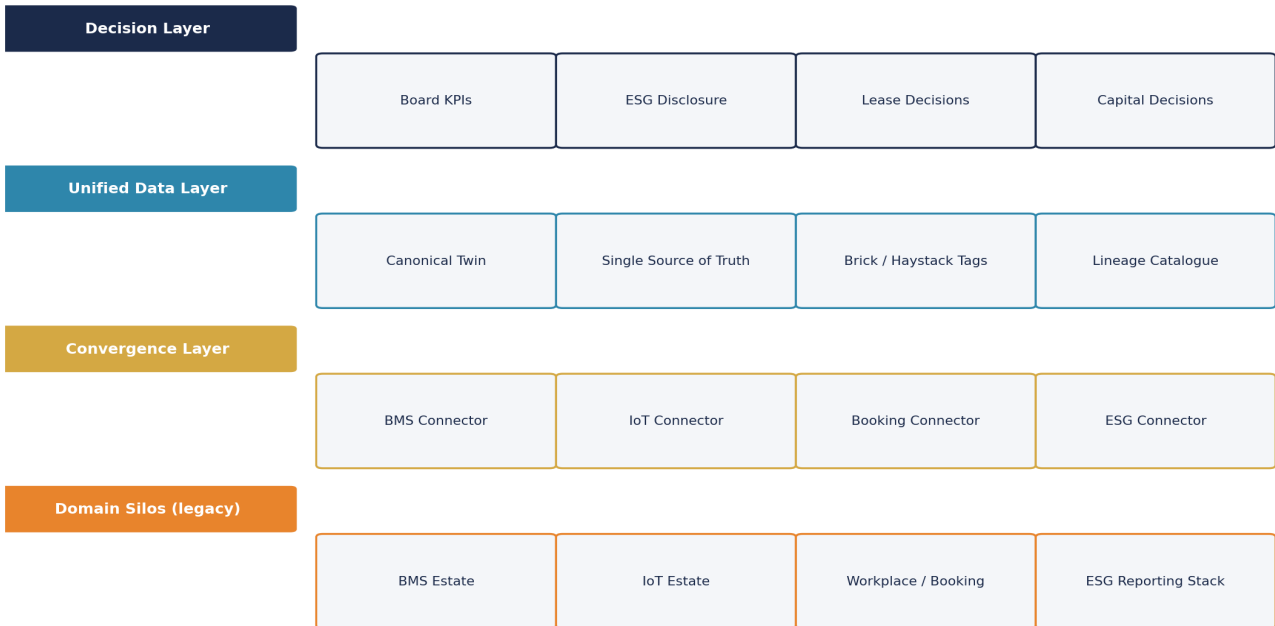


	Pillar	Mandate
U	Unified Telemetry	Single semantic model across IoT, BMS, ESG sub-systems
N	Normalised Data	Brick/Haystack tagging, vendor-agnostic representation
I	Integration Layer	Event bus, API gateway, twin synchronisation contracts
F	Federated Identity	Devices, agents, operators, occupants — single plane
Y	Yield Architecture	Outcome telemetry feeds board KPIs and ESG disclosures

Reference Architecture

The UNIFY reference architecture spans four institutional layers — *Domain Silos (legacy)* at the foundation, *Convergence Layer* mediating cross-layer flow, *Unified Data Layer* producing decision-grade signal, and *Decision Layer* 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 — UNIFY

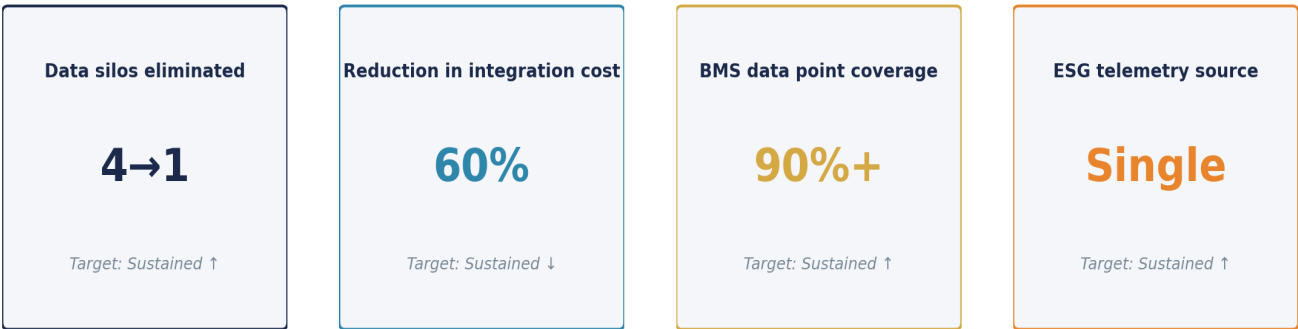


Convergence Discipline. The most common anti-pattern is parallel domain dashboards — facilities reporting from BMS, sustainability reporting from a separate ESG stack, real estate reporting from booking systems, and the board comparing four versions of 'occupancy' that don't reconcile. The fix is not 'one more dashboard'; it is a single canonical data model with explicit ontology (Brick / Haystack), a single data lineage catalogue, and tested reconciliation between domains. If two domains report different numbers for the same building, the architecture has failed regardless of how good each individual dashboard looks.

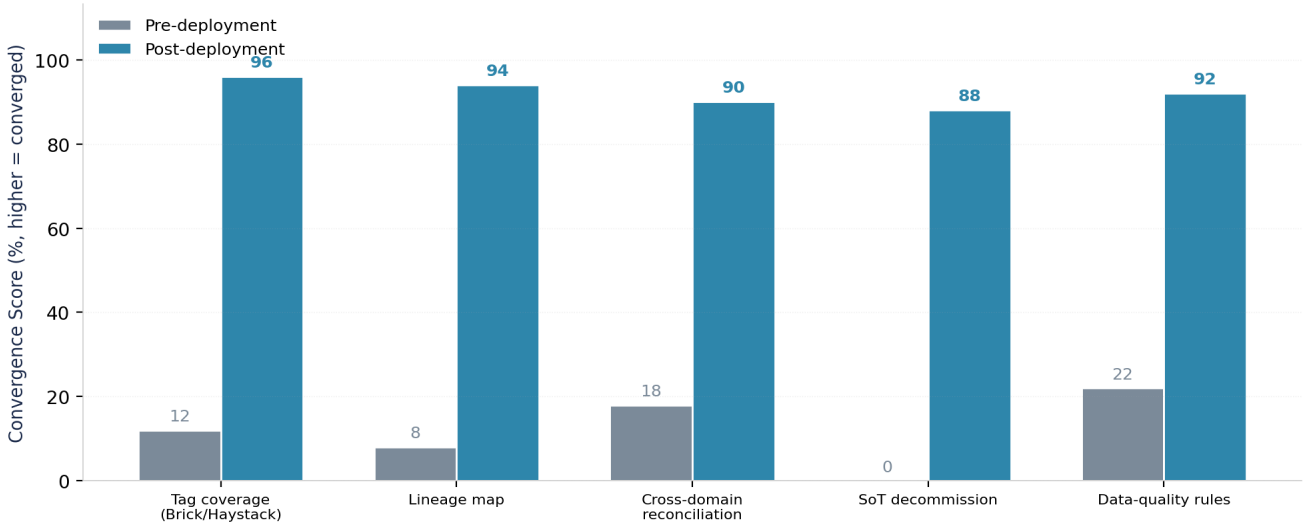
Outcomes & Board KPIs

Convergence is measured at the data layer, not at the dashboard layer. The indicators below show how UNIFY consolidates four domain silos (BMS, IoT, booking, ESG) into a single auditable canonical model. The lineage and reconciliation metrics are the ones that matter; once they pass, every downstream KPI is defensible.

The Intelligent Estate™ — Outcome KPIs



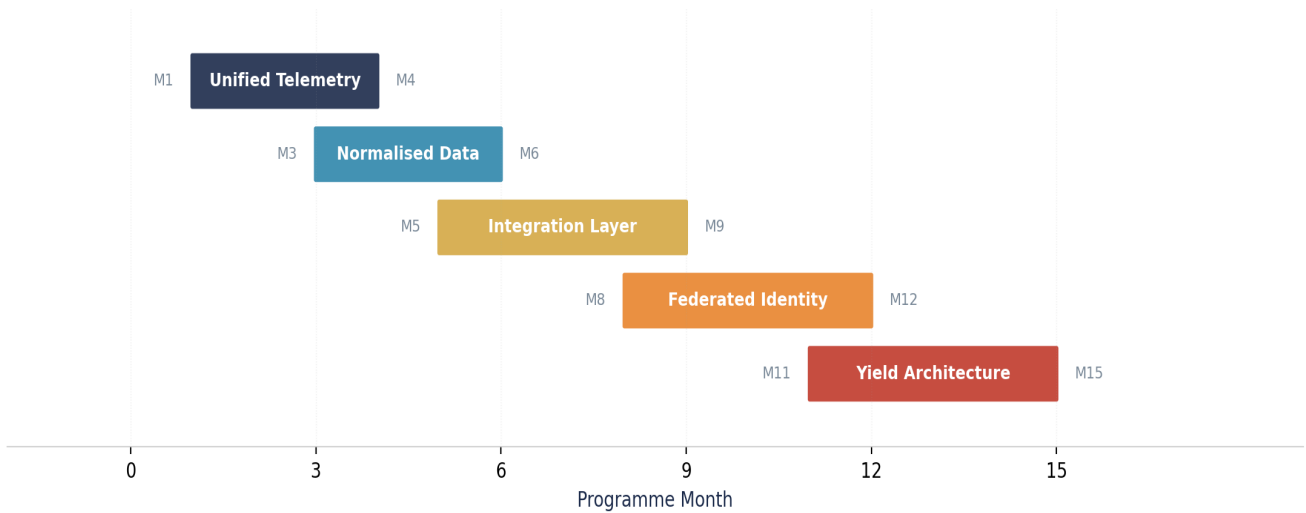
UNIFY Convergence Indicators



Implementation Roadmap

The UNIFY roadmap delivers the canonical model first and the dashboards second. Convergence stalls when programmes invert this — unifying dashboards above un-unified data. Gates 1-3 produce the ontology, lineage and reconciliation engine; gates 4-5 decommission the parallel domain stacks.

Implementation Roadmap – The UNIFY Framework



Gate	Deliverable	Evidence
G1 - Discover	Domain audit: BMS, IoT, booking, ESG, FM systems	System inventory; data quality baseline; reconciliation gap log
G2 - Canonical Model	Ontology, naming convention, point-mapping standard	Canonical data model; Brick/Haystack tag library; reconciliation rules
G3 - Connector Pilot	Two-domain convergence: BMS + ESG, fully reconciled	Lineage map; reconciliation test; auditor walkthrough
G4 - Estate Convergence	All domains converged; 90%+ point coverage	Coverage report; lineage catalogue; single-source-of-truth attestation
G5 - Decision Embed	Board, ESG and lease decisions all draw from unified layer	Decision-trace evidence; quarterly reconciliation review

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 · UK Insurer · 18 buildings · 1.6M sq ft

Four parallel platforms (BMS, IoT, ESG, twin) consolidated into UNIFY architecture. Annual integration cost reduced from £4.2m to £1.6m. Single board-reportable telemetry plane delivered within 9 months.

Case Study 2 · Government Estate · 22 buildings · 2.4M sq ft

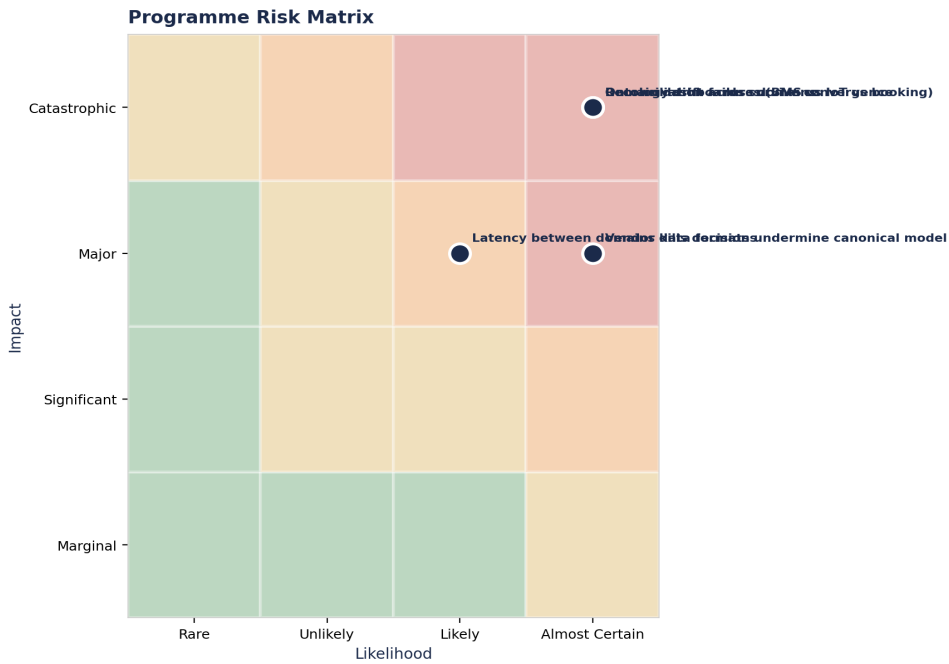
ESG reporting previously dependent on manual sub-meter reads. UNIFY architecture connected sub-metering to BMS/IoT telemetry; TCFD disclosure cycle reduced from 14 weeks to 3 weeks; auditor confidence rating improved 2 grades.

Case Study 3 · Bank HQ · 1.1M sq ft

Digital twin platform deployed without underlying telemetry contracts. UNIFY retro-fit delivered consistent semantic tagging across 187,000 data points, enabling twin to update from BMS in <30s rather than 6h batch.

Programme Risk Architecture

The UNIFY programme risk architecture spans 12 explicit risk entries across architectural, data, performance, regulatory, commercial, resilience 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

- Four domain silos generate four versions of the same KPI; boards, regulators and auditors will increasingly reject this and the cost of reconciliation rises every year.
- Ontology is the single most under-invested capability in smart-estate programmes; without Brick or Haystack tagging, convergence is theoretical not operational.
- Lineage from sensor → telemetry → KPI → board pack is now an audit expectation, not an aspiration; ESG assurers will require it from 2026.
- Single source of truth becomes a single point of failure unless it is explicitly engineered for resilience.
- Convergence stalls at 60% coverage in most programmes because the last 40% is ESG/booking/legacy-FM data; that is the hard yards.
- Decision drift back to domain dashboards is the most common reason convergence fails 12 months after go-live; usage telemetry must be a board KPI.

UNIFY Risk Register — Full Architecture

The full UNIFY 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	Domain dashboards survive convergence	Architectural	4	4	16	Decommission programme; single SoT mandate; exec sponsorship
2	Ontology drift across domains	Data	4	4	16	Central tag library; validation gate; ontology council
3	Reconciliation failures (BMS vs IoT vs booking)	Data	4	4	16	Reconciliation rules; daily check; exception triage
4	Latency between domains kills decisions	Performance	3	3	9	Latency SLA per domain; monitoring; tier design
5	Lineage gap blocks ESG audit	Regulatory	3	5	15	Per-KPI lineage map; auditor walkthrough; method note
6	Vendor data formats undermine canonical model	Commercial	4	3	12	Procurement clauses; canonical export requirement
7	Single SoT becomes single point of failure	Resilience	2	5	10	Replication; failover; DR test
8	Convergence stalls at 60% coverage	Programme	4	3	12	Coverage roadmap; per-domain owner; quarterly review
9	Ownership disputes between IT, FM, ESG	Governance	4	3	12	Data ownership matrix; arbitration path; exec sponsor
10	Personal-data leakage in unified layer	Privacy	3	4	12	DPIA; aggregation thresholds; access control
11	Twin diverges from physical estate	Data	3	3	9	Reconciliation cadence; drift alarms; reset playbook
12	Decision drift back to domain dashboards	Adoption	4	3	12	Decommission deadline; BAU monitoring; usage telemetry

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 Canonical Data Model & Ontology Standard on the following page.

Annex A — Canonical Data Model & Ontology Standard

The UNIFY canonical data model defines the single naming, tagging and unit standard across the estate. The extract below shows representative entries; the full standard covers 240 entities, 480 properties and 32 relationship types, aligned to Brick Schema 1.4 and Project Haystack 4.

Entity	Type (Brick)	Properties	Source domain	Unit	Owner
AHU	Air_Handler_Unit	supply_temp, return_temp, fan_speed, valve_position	BMS	°C, %, %	FM
Chiller	Chiller	kW_input, kW_output, COP, run_hours	BMS	kW, dimensionless, h	FM
Sub-meter	Electrical_Meter	kWh, kW, voltage, current, hierarchy_parent	BMS / IoT	kWh, kW, V, A	Energy
Workspace	Workspace	capacity, type, occupancy_count, booking_state	Booking + IoT	count, enum	Real Estate
CO2 sensor	CO2_Sensor	ppm, location, timestamp	IoT	ppm	ESG / FM
Lift	Elevator	state, run_count, fault_code, energy	BMS	enum, count, code, kWh	FM
PV array	PV_Array	kW_generated, kWh_today, irradiance	IoT / BMS	kW, kWh, W/m ²	Energy
Lease zone	Lease_Zone	sqm, tenant, contract_id, billable	Booking / Finance	sqm, enum	Real Estate
Carbon factor	Emission_Factor	Scope, region, year, gCO2e/kWh	ESG	gCO2e/kWh	ESG

Extract from the full UNIFY 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 — UNIFY

The UNIFY 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	Mandate Brick or Haystack Tagging at G1 Ontology is the single most under-invested capability. Without it, convergence is theoretical not operational.
02	Decommission Domain Dashboards by Calendar Date If parallel domain dashboards survive convergence, decisions drift back to them within 12 months. Set a hard decommission date by sponsor signature.
03	Build Lineage From Sensor to Board Pack Every board KPI must trace to a meter, sensor, or log. Lineage maps are now an ESG audit expectation.
04	Run Daily Cross-Domain Reconciliation Booking vs sensor vs Wi-Fi vs badge reconciliation runs daily, with alarm thresholds. Variance > 15% triggers exception triage.
05	Treat the Single Source of Truth as Critical Infrastructure Replicate, fail-over, DR-test. SoT becoming a single point of failure is a self-inflicted resilience exposure.
06	Publish a Data Ownership Matrix Every entity in the canonical model has an explicit owner across IT, FM, ESG and Real Estate. Ownership ambiguity is the leading cause of convergence stall.

90-Day Action Plan — UNIFY

The first 90 days set the programme's defensibility ceiling. The plan below sequences the highest-leverage actions specific to UNIFY, 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 · Domain Audit	Inventory of all source systems; data-quality baseline; reconciliation gap log; decommission targets identified	System inventory; quality baseline report; gap log; decommission roadmap
Days 31-60 · Canonical Model & Ontology	Brick/Haystack tag library v1; canonical model defined; data-quality rules; lineage map skeleton	Tag library; canonical model document; quality rules; lineage v1
Days 61-90 · Two-Domain Pilot	BMS + ESG converged through unified layer; daily reconciliation live; lineage map for first 5 KPIs	Two-domain pilot live; reconciliation report; KPI lineage maps

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: Sensor → Board KPI Lineage Trace (Anonym)

Below is the live lineage trace for one ESG board KPI — Scope 2 emissions from chiller plant — from raw BACnet point to auditor-signed disclosure. The trace covers eight transformations across four systems. Every line is a discrete data contract with named owner; the auditor walks this lineage in 11 minutes.

Step	Source	Identifier	Operation	Output	Owner
1	BMS (Vendor A)	AHU-13.CHW.kW (BACnet objId 4194)	Read raw kW at 1Hz	kW (1Hz time series)	FM
2	Gateway	BACnet→MQTT bridge	Tag with Brick + sample to 1min	1-min kW with brick:Chiller_Power tag	Data Lead
3	Schema registry	schema:chiller_power _v3	Validate against contract	Validated kW message	Data Lead
4	Data lake	fact_chiller_power	Persist + join asset hierarchy	kWh per asset per hour	Data Lead
5	Energy service	energy.kwh_chiller_q1	Aggregate to Scope 2 daily	Scope 2 location-based daily kWh	Energy Lead
6	Carbon engine	factor:DEFRA_2025_a vg	Apply versioned factor (191 gCO ₂ e/kWh)	gCO ₂ e per day	ESG Lead
7	ESG dashboard	kpi_scope2_chiller	Aggregate to quarterly board figure	Q1 Scope 2 chiller (tCO ₂ e)	ESG Lead
8	Disclosure pack	discl_2026_Q1_S2	Auditor walkthrough + method note	Signed quarterly disclosure	ESG + Assurer

Outcome. The same lineage pattern is applied to the other 11 board KPIs in scope. The 'one truth' claim is operational only when the lineage map exists and the auditor can walk it. Without lineage, convergence is theoretical.

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

The Intelligent Estate™

Four platforms is not architecture. Four platforms is technical debt with a cost centre. The intelligent estate is unified by design or it is intelligent by accident — and accidental intelligence does not survive board scrutiny.

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**