Falconry360™

WHITEPAPER

ENTERPRISE GRC / FALCONRY360 INSIGHT SERIES

Regulatory compliance framework

Strategic approaches to managing multi-jurisdictional compliance obligations and supervisory reporting requirements.

Falconry360 · Governance, Risk & Resilience Practice

OVERVIEW / WHAT THIS PAPER ARGUES

Executive summary

Regulated institutions now answer to more supervisors, across more jurisdictions, with shorter reporting cycles than at any point in the past decade. Managing each regime in isolation multiplies cost and erodes assurance.

This paper sets out a framework for consolidating obligations into a single operating model — and for treating supervisory reporting as a governed data discipline rather than a periodic scramble.

01

One obligations register

Consolidate every applicable requirement into a single, jurisdiction-aware inventory.

02

Rationalized controls

Map many obligations to one common control set — test once, satisfy many regimes.

03

Change as a lifecycle

Run horizon scanning and regulatory change through a governed, auditable process.

04

Reporting as data

Build supervisory reporting on governed data with lineage, ownership and quality gates.

CONTEXT

The multi-jurisdictional compliance challenge

Overlapping regimes, duplicated effort

The same underlying control — access management, incident response, outsourcing oversight — is evidenced separately for each regulator, each in its own template and cadence.

Inconsistent answers to supervisors

When registers live in spreadsheets across functions, two regulators can receive two different versions of the truth — the fastest route to a loss of supervisory confidence.

Change absorbed ad hoc

New circulars, rulebooks and consultation papers arrive continuously; without a governed change process, applicability decisions go undocumented and deadlines surface late.

A regional group operating in three GCC markets can face **six or more prudential, conduct, cyber and privacy regulators** — each with its own rulebook, taxonomy and submission calendar.

CONTEXT / WHO REGULATES WHAT

The regulatory landscape

JURISDICTION	KEY SUPERVISORS	REPRESENTATIVE REGIMES
Saudi Arabia	SAMA · CMA · NCA · SDAIA	SAMA CSF & BCM, NCA ECC, PDPL, AML/CFT rules
United Arab Emirates	CBUAE · SCA · DFSA · FSRA	CBUAE rulebooks, DFSA/ADGM regimes, UAE PDPL
Qatar	QCB · QFMA · QFCRA · NCSA	QCB instructions, QFC rules, PDPPL
Bahrain · Kuwait · Oman	CBB · CBK · CMA · CBO	CBB Rulebook, CBK supervision, Oman banking law
Global baseline	BCBS · FATF · IAIS · ISO	Basel III, BCBS 239, FATF 40, ISO 27001/22301, GDPR & DORA for EU-facing groups

Illustrative, not exhaustive. Sector regulators (insurance authorities, telecom, health) add further layers for diversified groups.

Strategic operating model

A single structure that connects obligations, controls, evidence and reporting — so compliance scales with the regulatory perimeter instead of multiplying against it.

SECTION I / OPERATING MODEL

The target compliance operating model

LAYER 1

Obligations register

Every requirement, per jurisdiction and entity, with an accountable owner.

LAYER 2

Common control library

One rationalized control set, mapped many-to-one from obligations.

LAYER 3

Evidence & attestation

Continuous testing, named owners, due dates and a defensible audit trail.

LAYER 4

Supervisory reporting

Regulator-ready outputs generated from the same governed data.

Governance wrapper. Board-approved policy, a compliance charter, defined risk appetite and management information cut across all four layers.

The model's discipline is directional: obligations flow down into controls, and assurance flows up into reporting. Nothing is evidenced twice, and nothing reaches a supervisor that cannot be traced to its source.

Entity structure matters: each layer is segmented by legal entity and jurisdiction, so group-level oversight and local accountability coexist without duplication.

SECTION I / ACCOUNTABILITY

Governance and the three lines of defense

FIRST LINE

Business & operations

Owns obligations and executes controls in the flow of business. Attests to control performance and raises exceptions at source.

SECOND LINE

Compliance & risk

Owns the framework: the obligations register, control mapping methodology, change process, and the supervisory relationship. Challenges the first line with evidence.

THIRD LINE

Internal audit

Provides independent assurance over the framework itself — including whether mappings, attestations and regulatory submissions can withstand scrutiny.

The framework works when the second line owns the **methodology** and the first line owns the **controls**. Compliance functions that try to own everything become the bottleneck they were built to remove.

SECTION I / MAP ONCE, COMPLY MANY

Obligation mapping and control rationalization

1 Normalize

Decompose each rulebook into discrete, testable obligations with consistent language.

2 Cluster

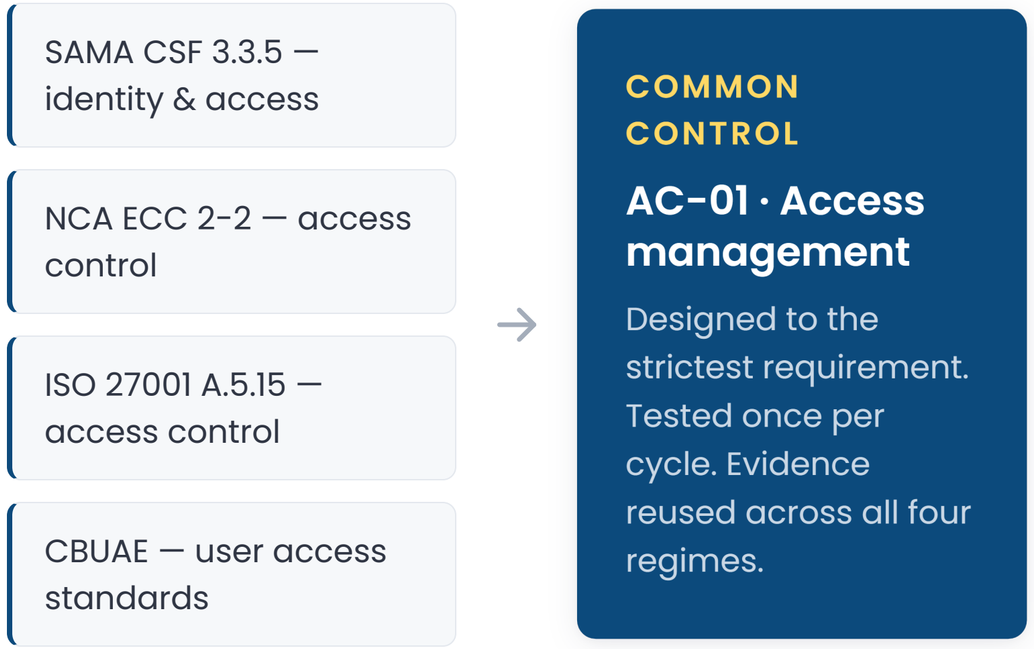
Group obligations that address the same underlying risk across jurisdictions.

3 Harmonize upward

Design each common control to the strictest applicable requirement — meeting it satisfies every lighter regime automatically.

4 Map and maintain

Record the many-to-one mapping and keep it live as rulebooks change — the mapping is an asset, not a project.



Four obligations · one control · one evidence set

II

Regulatory change management

From reactive scramble to governed lifecycle — how leading institutions scan the horizon, assess applicability and land change on time.

SECTION II / A GOVERNED LIFECYCLE

Horizon scanning and the regulatory change lifecycle

1

Monitor

Track regulator publications, circulars and consultations across every jurisdiction in scope.

2

Assess applicability

Decide which entities and businesses are in scope — and document the rationale either way.

3

Analyze impact

Trace the change through the obligations register to affected controls, policies and reports.

4

Implement

Assign actions with owners and deadlines; update controls, procedures and training.

5

Attest & close

Evidence readiness before the effective date; report status to governance committees.

Non-applicability is a decision

Supervisors increasingly ask why a change was judged out of scope. A documented "not applicable, because…" is as important as an implementation plan.

Consultations are early warning

Engaging at consultation stage buys implementation time and shapes proportionate outcomes — mature functions treat responses as a planned activity.

SECTION II / ILLUSTRATIVE SCENARIO

A GCC banking group, before and after

A composite scenario: a group with banking, insurance and payments entities across three GCC markets, answering to seven supervisors.

BEFORE · FRAGMENTED

- ✕ Seven obligation registers in spreadsheets, one per regulator, maintained by different teams
- ✕ The same access-management control evidenced four times a year for four different reviews
- ✕ Regulatory returns compiled by email; late data-quality issues found by the regulator, not the bank
- ✕ New circulars discovered through industry peers rather than a monitored pipeline

AFTER · CONNECTED

- ✓ One group-wide obligations register, segmented by entity and jurisdiction, with named owners
- ✓ A common control library mapped to all seven regimes; each control tested once per cycle
- ✓ Returns generated from governed data with lineage back to source systems and quality gates before submission
- ✓ A single change pipeline with applicability decisions, impact traces and deadline tracking on one dashboard

Illustrative composite drawn from common patterns in regional engagements — not a specific client reference.

III

Supervisory reporting

Every submission is a statement about your data governance. Treating reporting as a data discipline — not a document exercise — is what separates exam-ready institutions.

SECTION III / DATA QUALITY

Supervisory reporting and data quality

The principles of BCBS 239 — written for risk-data aggregation in banks — generalize to every regulated submission: returns, breach notifications, prudential filings and ad hoc supervisory requests.

Accuracy

Figures reconcile to the ledger and to each other. Manual adjustments are logged, justified and approved.

Completeness

All entities, portfolios and exposures in scope are captured — including the awkward ones held outside core systems.

Timeliness

Submission calendars are managed centrally with escalation before deadlines — and capacity for ad hoc supervisory requests.

Lineage

Every reported figure traces to its source system, transformation logic and owner — answerable in an exam within hours, not weeks.

Supervisors read data quality as a proxy for management quality. A late or restated return signals weaknesses far beyond the reporting team.

SECTION III / ARCHITECTURE

Reporting data architecture principles

Source systems

Core banking, policy admin, payments, GL — each with a named data owner and defined golden source.

↓

Governed data layer

Common definitions, quality rules and reconciliation — one version of every regulatory data element.

↓

Report assembly

Regulator templates populated from the governed layer; validations run before anyone signs.

↓

Submission & audit trail

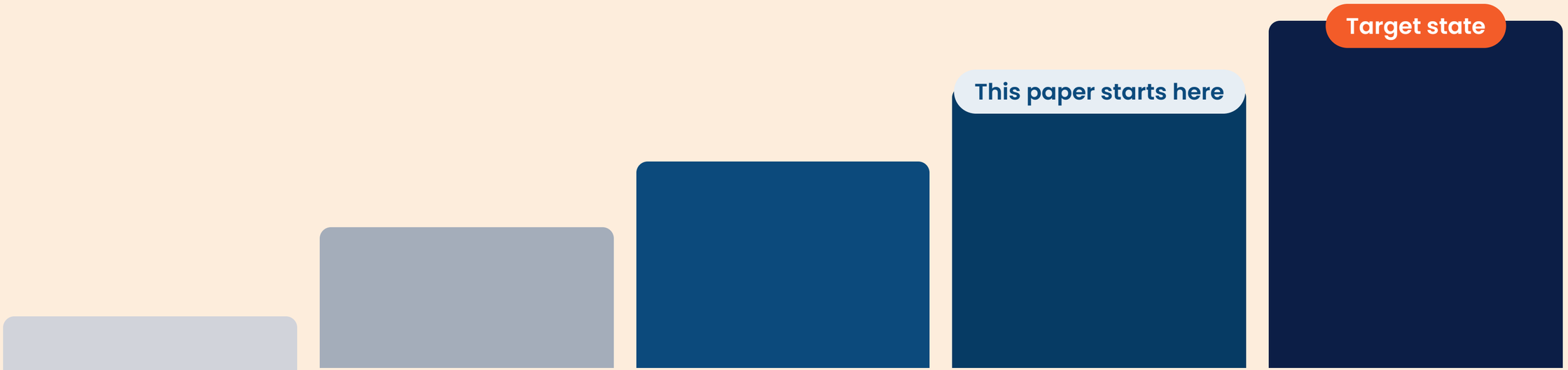
Sign-off workflow, submission record, and the full lineage retained for supervisory examination.

Design principle

If a figure cannot be traced from the submitted return back to a golden source without human archaeology, the architecture — not the analyst — is the finding.

SECTION III / SELF-ASSESSMENT

The compliance maturity model



1 · Initial

Person-dependent. Obligations live in inboxes and institutional memory.

2 · Managed

Registers exist per regulator, in spreadsheets, maintained reactively.

3 · Defined

A documented framework and change process; mapping partial, evidence manual.

4 · Integrated

One register, rationalized controls, governed reporting data, platform-enabled.

5 · Optimizing

Predictive horizon scanning, continuous control monitoring, near-real-time assurance.

Most regulated institutions in the region self-assess at levels 2–3. This paper charts the full path to levels 4 and 5 — where multi-jurisdictional scale reduces unit cost instead of increasing it, and assurance shifts from a periodic exercise to continuous, near-real-time confidence.

IV

Technology enablement

The framework is an operating model, not a software feature — but at multi-jurisdictional scale it cannot be run on spreadsheets. This is where a connected platform earns its place.

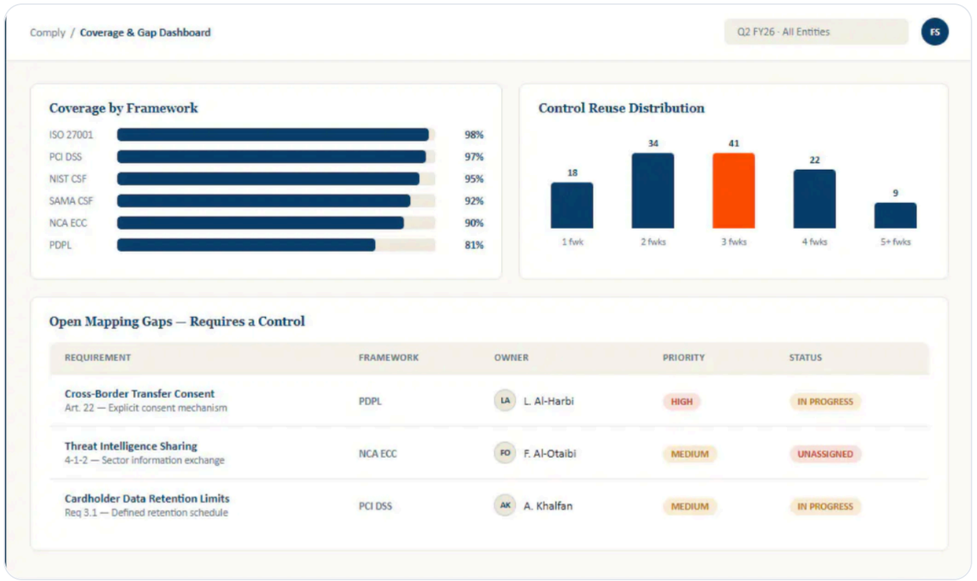
- I · Operating model
- II · Regulatory change
- III · Supervisory reporting
- **IV · Technology enablement**

SECTION IV / COMPLY · GOVERN · ASSURE

How Falconry360 operationalizes the framework

Obligations register	20+ frameworks pre-mapped in one obligation library.
Control rationalization	One control mapped to every applicable framework.
Regulatory change	Change pipeline with impact tracing and deadline workflows.
Supervisory reporting	Regulator-ready reporting generated from live platform data.

FalconryX assists mapping, prioritization and drafting across all pillars — with 100% human approval gates on AI actions.



One connected platform

Framework mapping, control rationalization, regulatory change and supervisory reporting in a single system of record — one version of the truth for every regulator.

SECTION IV / GETTING THERE

Implementation roadmap

PHASE 1 · MONTHS 0–4
Foundation

· Regulatory perimeter and entity scoping

· Consolidated obligations register, priority regimes first

· Governance charter, ownership model, committee cadence

Exit test: one register the board can rely on.

PHASE 2 · MONTHS 4–10
Integration

· Control rationalization and many-to-one mapping

· Regulatory change lifecycle live, with horizon scanning

· Evidence workflows with owners, due dates, attestation

Exit test: one control tested once, satisfying many regimes.

PHASE 3 · MONTHS 10–18
Industrialization

· Supervisory reporting on governed data with lineage

· Continuous control monitoring where data allows

· Board MI and regulator dashboards from live data

Exit test: exam-ready lineage for every submitted figure.

Durations are indicative for a mid-size regional group; sequencing matters more than speed. Each phase produces standalone value.

REFERENCE

Glossary of key terms

Obligations register

The consolidated inventory of every regulatory requirement applicable to the organization, by entity and jurisdiction.

Control rationalization

Consolidating overlapping requirements into a single common control set, designed to the strictest applicable standard.

Horizon scanning

Systematic monitoring of regulator publications, consultations and enforcement trends to anticipate change before it is enacted.

BCBS 239

The Basel Committee's principles for risk-data aggregation and reporting — the reference standard for reporting data quality.

Data lineage

The documented path of a reported figure from source system through every transformation to the submitted return.

Three lines of defense

The accountability model separating business ownership (first), compliance and risk oversight (second), and independent audit (third).

Supervisory reporting

The full set of returns, filings and notifications a regulated entity submits to its supervisors, periodic and ad hoc.

Applicability assessment

The documented decision on whether — and to which entities — a new regulatory requirement applies.

Falconry360™

Governance. Risk. Resilience. Trusted.

Talk to the Falconry team about assessing your compliance maturity, consolidating your obligations register, or seeing the framework live in Falconry360.

contact@falconry.solutions falconry.solutions falconry360.com