Falconry360™

WHITEPAPER

Enterprise Risk Management in the GCC

A practitioner's guide to implementing modern risk frameworks across regulated industries in the Gulf.

Framework-aligned
COSO · ISO 31000 · Basel

Structured around
Five connected pillars

ABOUT THIS WHITEPAPER

Risk, made connected

Gulf enterprises are being asked to govern more risk, across more domains, under sharper regulatory scrutiny — with the same fragmented tools they have always used.

This whitepaper sets out how boards and risk teams in regulated GCC industries can move from siloed, reactive controls to a single, connected operating model — grounded in the global standards, mapped to regional regulators, and built to last.

WRITTEN FOR

Boards & C-suite
CROs, CFOs and CEOs setting risk strategy

Risk & compliance teams
Practitioners operationalising frameworks

Regulators & auditors
Assessing governance and assurance maturity

CONTENTS

Six parts, one operating model

01

The case for connected risk

Diversification, digitisation and a tighter regulatory climate are reshaping what "managing risk" means for Gulf enterprises.

A region rewriting its risk profile

Regulators are raising the bar

The cost of fragmentation

ANTICIPATE · REGIONAL CONTEXT

A region rewriting its risk profile

Economic diversification

National visions are pushing capital into tourism, logistics, manufacturing and technology — new sectors carry unfamiliar risk.

Rapid digitisation

Cloud, open banking and AI expand the attack surface and the pace at which risk materialises.

Deepening capital markets

IPOs, sovereign funds and foreign investors raise the bar for disclosure, governance and controls.

Geopolitical exposure

Regional dynamics, energy transition and supply-chain concentration keep resilience on the board agenda.

COMPLY · SUPERVISORY LANDSCAPE

Regulators are raising the bar

Across the six GCC states, financial and sector supervisors have converged on stronger governance, risk-data and disclosure expectations aligned to Basel, IOSCO and IAIS standards.

SAMA

Saudi Central Bank

Cyber-security, operational-risk and business-continuity frameworks for banks, insurers and finance companies.

CBUAE

Central Bank of the UAE

Corporate-governance, risk-management and outsourcing standards; AML and consumer-protection regimes.

QCB

Qatar Central Bank

Prudential and ICAAP requirements; strategic focus on fintech and financial-sector resilience.

CBB

Central Bank of Bahrain

A single integrated rulebook spanning risk, governance, cyber and crypto-asset supervision.

CMA

Capital Market Authorities

Listing, disclosure and internal-control obligations for issuers and market participants.

CBO / Sector

Oman & sector regulators

Health, energy, telecom and data-protection authorities extending risk duties beyond finance.

GOVERN · THE PROBLEM

The cost of fragmented risk

FRAGMENTED TODAY

- Risk, compliance, audit and cyber run on separate spreadsheets and tools
- No single view of exposure; the same control is tested many times
- Board packs are manual, backward-looking and weeks out of date
- Regulatory change is tracked reactively, framework by framework

CONNECTED TARGET

- One taxonomy links risks, controls, obligations and evidence
- A live enterprise view with drill-down from board to control
- Real-time dashboards; test once, satisfy many frameworks
- Regulatory change flows to the controls it affects automatically

02

Foundations of modern ERM

The globally recognised frameworks and governance structures every GCC risk programme should be built on.

COSO ERM | ISO 31000 | Risk appetite | Three lines model

GOVERN · DEFINITION

What enterprise risk management is

> Enterprise risk management is the culture, capabilities and practices — integrated with strategy and performance — that organisations rely on to **manage risk in creating, preserving and realising value.**

Integrated

Embedded in strategy, decisions and day-to-day performance — not a parallel exercise.

Enterprise-wide

A portfolio view across every risk type and business unit, not isolated silos.

Value-focused

Balances protecting value with the risk-taking needed to create it.

Continuous

A dynamic, iterative cycle that adapts as context and information change.

GOVERN · FRAMEWORK

The COSO ERM framework

Five interrelated components, supported by twenty principles, connect enterprise risk to strategy and performance across the organisation.

01

Governance & culture

Board oversight, operating structures, tone and desired behaviours.

02

Strategy & objectives

Risk appetite set alongside strategy and business objectives.

03

Performance

Identify, assess, prioritise and respond to risk against objectives.

04

Review & revision

Assess how ERM is functioning and revise as changes arise.

05

Information & reporting

Communicate risk information across the organisation and up to the board.

ANTICIPATE · PROCESS

The ISO 31000 process

Where COSO frames governance, ISO 31000 gives the repeatable operational cycle — a core sequence wrapped by communication, monitoring and recording throughout.

SCOPE, CONTEXT & CRITERIA

Define objectives, boundaries and how risk is judged

RISK ASSESSMENT

Identify | Analyse | Evaluate

RISK TREATMENT

Avoid, reduce, share or accept the risk

Communication & consultation — throughout

Monitoring & review — continuous

Recording & reporting — evidence

GOVERN · COMPARISON

COSO and ISO 31000, side by side

COSO ERM

Integrating with strategy & performance

- Strong on **governance, culture and strategy**
- Prescriptive: 5 components, 20 principles
- Widely used for internal control & assurance
- Board- and reporting-oriented language

ISO 31000

Guidelines for risk management

- Strong on a **concise, universal process**
- Principles-based and non-prescriptive
- Applies to any risk type, sector or size
- Easy to certify against and operationalise

Leading GCC programmes run COSO for governance and reporting, and ISO 31000 for the working process — one taxonomy underneath both.

GOVERN · APPETITE & TOLERANCE

Defining risk appetite and tolerance

A clear appetite turns risk from an abstract idea into a decision rule the whole organisation can act on — cascading from the boardroom to the front line.

01 · BOARD

Risk appetite

The amount and type of risk the organisation is willing to pursue in creating value.

02 · OBJECTIVE

Risk tolerance

Acceptable variation in performance around a specific objective.

03 · CONTROL

Risk limits

Hard thresholds and triggers that keep exposure within tolerance.

04 · FRONT LINE

Everyday decisions

Consistent choices made within limits, evidenced and escalated by exception.

ASSURE · ACCOUNTABILITY

The three lines model

Clear roles remove the ambiguity of "who owns this risk" — the foundation regulators expect to see behind any governance structure.

FIRST LINE

Own & manage

Business and operational management own risks and run the controls in their processes day to day.

SECOND LINE

Oversee & advise

Risk and compliance functions set policy, monitor exposure and challenge the first line.

THIRD LINE

Independent assurance

Internal audit provides objective assurance to the board on governance, risk and control.

Overseen by the **governing body** and complemented by **external assurance** — regulators, external audit and independent reviewers.

03

Risk across regulated industries

The same frameworks, applied to very different risk profiles — from Basel-regulated banks to critical national infrastructure.

Banking & financial services

Insurance · Energy · Public sector · Health · Telecom

COMPLY · DEEP DIVE

Banking & financial services

The Gulf's most mature ERM sector. Basel II/III anchors capital, supervision and disclosure — but operational, cyber and financial-crime risk are where the frontier now sits.

PILLAR 1
Minimum capital
Credit, market & operational risk

PILLAR 2
Supervisory review
ICAAP & stress testing

PILLAR 3
Market discipline
Public risk disclosure

Core risk types under management

- Credit risk
- Market risk
- Liquidity risk
- Operational risk
- Financial crime & AML
- Cyber & technology risk

ANTICIPATE · SECTOR VIEW

A cross-industry risk lens

INDUSTRY	DOMINANT RISK	LEADING STANDARD	GCC PRESSURE POINT
Insurance	Underwriting & solvency risk	Risk-based capital · IAIS ICPs	Actuarial data quality & reserving
Energy & utilities	HSE & operational risk	ISO 31000 · ISO 45001	Asset integrity & energy transition
Public sector	Delivery & fiscal risk	COSO · national frameworks	Mega-project & Vision delivery
Healthcare	Patient safety & clinical risk	ISO 31000 · accreditation	Data privacy & rapid expansion
Telecom	Cyber & continuity risk	NIST CSF · ISO 22301	Critical infrastructure protection

04

The expanding risk universe

Five domains that have moved from the technology footnote to the top of the board agenda.

Cyber | Third-party | Resilience | ESG & climate | AI governance

WITHSTAND · DIGITAL TRUST

Cyber and digital risk

The NIST Cybersecurity Framework gives boards a common language for cyber — six functions that turn a technical concern into a governed enterprise risk.

Govern
Strategy, roles & oversight

Identify
Assets & risks

Protect
Safeguards & controls

Detect
Monitor & alert

Respond
Contain & manage

Recover
Restore & learn

In the GCC, SAMA and CBUAE cyber frameworks map closely to these functions — making NIST CSF a practical bridge between global practice and local supervision.

COMPLY · TPRM

Third-party and supply-chain risk

You can outsource the activity, not the accountability. GCC supervisors expect risk to be managed across the full third-party lifecycle — from onboarding to exit.

01

Assess & onboard

Due diligence, risk tiering and contractual controls before engagement.

02

Monitor & manage

Ongoing performance, SLA, concentration and fourth-party oversight.

03

Respond to issues

Incident escalation, remediation and continuity for critical suppliers.

04

Exit & offboard

Planned transition, data return and removal of access with evidence.

WITHSTAND · CONTINUITY

Operational resilience and continuity

Resilience reframes continuity around **important business services** and the impact tolerance for disruption — not just recovering individual systems.

- Map the services that matter and the assets they depend on
- Set impact tolerances — how much disruption is bearable
- Test against severe-but-plausible scenarios, then remediate

Anchored on ISO 22301 — business continuity management

ANTICIPATE · SUSTAINABILITY

Climate, ESG and transition risk

As Gulf economies pursue net-zero commitments and green finance, climate risk is becoming a financial and disclosure risk the board must own.

Physical risk

Extreme heat, water stress and weather events affecting assets, operations and supply chains.

Transition risk

Policy, technology and market shifts as economies decarbonise — acute for energy-linked portfolios.

Disclosure risk

Meeting exchange and investor expectations on ESG reporting, with credible, auditable data.

GOVERN · RESPONSIBLE AI

Governing artificial intelligence

AI is now both a source of risk and a means of managing it. ISO/IEC 42001 gives boards a management-system standard to govern it responsibly.

Transparency
Explainable, documented decisions

Human oversight
Approval gates on material actions

Data governance
Quality, lineage and privacy

Accountability
Clear ownership of outcomes

Risk management
Assess models before and in use

Continual improvement
Monitor drift and retrain

05

Implementing ERM that lasts

Frameworks do not manage risk — people, process and data do. A pragmatic path from intent to operating capability.

Roadmap | Taxonomy & register | KRIs | Culture

GOVERN · IMPLEMENTATION

A phased implementation roadmap

PHASE 1

Baseline

Assess maturity, map obligations and agree scope, sponsorship and governance.

PHASE 2

Design

Set appetite, build the taxonomy, framework and policies, and define the target operating model.

PHASE 3

Operationalise

Stand up the register, controls and KRIs on a single platform; embed workflows and reporting.

PHASE 4

Optimise

Automate evidence, add analytics and continuously improve as risks and regulation evolve.

Treat this as a loop, not a line — each cycle deepens coverage, automation and assurance.

COMPLY · STRUCTURE

Building the risk taxonomy and register

A shared taxonomy is the backbone of connected risk — it lets one risk link to its controls, obligations, owners and evidence. The register is where that structure becomes a living record.

Risk register — anatomy of an entry RISK-OPS-014

RISK Core banking outage	CATEGORY Operational · Technology
OWNER Head of Technology	APPETITE Low
INHERENT High	RESIDUAL Medium
LINKED CONTROLS 4 · mapped to 3 frameworks	EVIDENCE Current

ANTICIPATE · MEASUREMENT

Quantifying risk and setting KRIs

Mature programmes move beyond colour-coded heat maps to monitored indicators with thresholds — turning risk into something you can see coming.

KRI

Key risk indicator

Leading signals that exposure is rising toward a threshold.

KCI

Key control indicator

Whether the controls that mitigate a risk are working as designed.

KPI

Key performance indicator

Performance context that risk is judged against.

A good KRI is:

- Measurable
- Predictive & leading
- Linked to a risk & appetite
- Threshold-based
- Owned & actionable

GOVERN · CULTURE

Embedding a risk culture

Frameworks describe how risk should be managed; culture decides whether it actually is. It is the strongest — and most overlooked — control an organisation has.

Tone from the top
Leaders model that raising risk is valued, not penalised.

Psychological safety
Bad news travels fast, early and without fear.

Aligned incentives
Reward and accountability reflect risk behaviour, not just results.

ASSURE · LESSONS LEARNED

Common implementation pitfalls

Compliance theatre

Registers maintained for the auditor, not for decisions. **Fix:** tie risk to real choices.

Tool before operating model

Buying software to fix a process gap. **Fix:** design the model, then enable it.

Risk as a silo

A function that sits apart from the business. **Fix:** embed in the first line.

Static assessments

An annual workshop and nothing between. **Fix:** monitor with live KRIs.

Data everywhere, insight nowhere

Fragmented sources no one trusts. **Fix:** one source of truth.

No board line of sight

Reporting too dense to act on. **Fix:** role-based, drill-down views.

06

Connected execution with Falconry360

One platform to govern, manage, assure and improve enterprise GRC performance — organised around five connected pillars.

Falconry360™

THE OPERATING MODEL

Five pillars of connected oversight

Every theme in this whitepaper maps to one of five connected pillars — a single spine from governance to assurance.

Govern

Structure, appetite, policy and accountability.

Anticipate

Identify, assess and monitor emerging risk.

Comply

Map obligations to controls and evidence.

Withstand

Cyber, continuity and operational resilience.

Assure

Audit, testing and independent confidence.

CONNECTED COVERAGE

Mapping frameworks to the platform

PILLAR	FRAMEWORKS & STANDARDS	WHAT IT DELIVERS
Govern	COSO ERM · ISO 31000 · ISO 42001	Appetite, policy & accountable oversight
Anticipate	ISO 31000 · climate & ESG frameworks	Assessment, KRIs & emerging-risk radar
Comply	Basel II/III · SAMA · CBUAE · AML	Obligations mapped to controls & evidence
Withstand	NIST CSF · ISO 22301 · ISO 27001	Cyber, continuity & resilience testing
Assure	Three lines model · internal audit	Independent testing & board confidence

THE INTELLIGENCE LAYER

FalconryX — intelligence across every pillar

An AI layer that runs across governance, risk and assurance — accelerating the work while keeping people accountable for every material decision.

Control mapping

Suggests how one control satisfies many frameworks.

Prioritisation

Surfaces the risks and gaps that matter most now.

Regulatory change

Reads change and routes it to affected controls.

Executive reporting

Drafts board-ready narrative from live data.

Human approval gates on every material action — aligned to ISO/IEC 42001 principles.

THE MODEL, BY CONSTRUCTION

Connected risk, by the numbers

5

Connected pillars

Govern · Anticipate · Comply · Withstand · Assure

20+

Frameworks pre-mapped

Global standards and GCC regulators

3

Lines of defence

Own · oversee · independently assure

1

Source of truth

One taxonomy for risk, control and evidence

100%

Human approval gates

On every material AI-assisted action

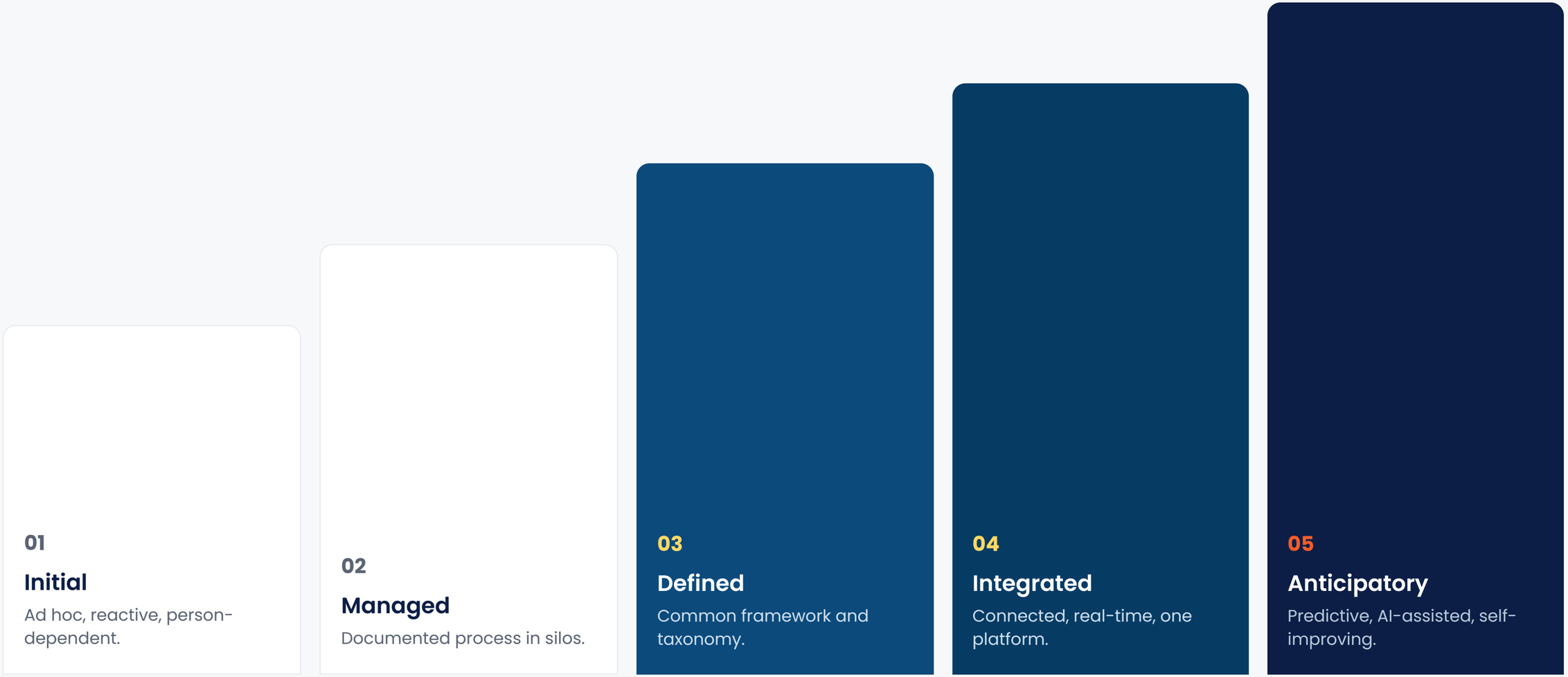
6

GCC states in scope

Built for the Gulf regulatory landscape

WHERE DO YOU STAND

An ERM maturity model



FIRST MOVES

Where to begin

01

Benchmark maturity

Place yourself honestly on the maturity model and identify the two pillars with the widest gap.

02

Unify the taxonomy

Agree one shared language for risks, controls and obligations before choosing any tooling.

03

Connect on one platform

Bring risk, compliance, resilience and assurance together — then let intelligence do the heavy lifting.

Falconry360™

GOVERN · PROTECT · ENABLE · TRUST

From fragmented processes to connected execution.

One platform to govern, manage, assure and improve enterprise GRC performance across the GCC.

falconry360.com contact@falconry.solutions

A Falconry Solutions company