

GCC ERM Implementation Checklist

COSO ERM Framework — UAE & KSA Regulatory Context

Majid Mumtaz · CIA · ACA · FCCA | Director of Internal Audit | 20+ Years GCC

Developed from implementing COSO ERM frameworks across a KSA JSC holding group operating under Saudi Corporate Governance Regulations (2017) and UAE entities governed by SCA requirements. Generic COSO checklists do not account for GCC-specific structural realities: family ownership concentration, board composition constraints, regulatory fragmentation across jurisdictions, and the practical challenge of implementing enterprise risk processes in organisations where informal authority frequently overrides formal governance.

COMPONENT 1 — GOVERNANCE & CULTURE

- ☐ **Board-level risk appetite statement approved and documented — in specific, measurable terms**

- ☐ **Risk appetite differentiated by category: strategic, financial, operational, compliance, reputational**
"We have a low appetite for compliance risk" is not a risk appetite statement — quantify it

- ☐ **Risk governance structure defined: Board oversight, Risk Committee (if any), Management Risk function, IA**

- ☐ **Three Lines of Defence model documented and communicated across the organisation**

- ☐ **Chief Risk Officer or equivalent role defined — or explicit decision that IA performs this function**

- ☐ **ERM policy approved by Board — covers scope, ownership, review frequency, escalation**

- ☐ **Informal authority structures mapped: who has decision power that is not reflected in the org chart?**
GCC reality: founder/family authority often operates outside formal governance — document and escalate

COMPONENT 2 — STRATEGY & OBJECTIVE-SETTING

- ☐ **Strategic objectives documented at organisational level — specific, measurable, time-bound**

- ☐ **Risk tolerance defined for each strategic objective — what variance is acceptable?**

- ☐ **External environment analysis completed: regulatory, competitive, macroeconomic, geopolitical (GCC)**

-
- ☐ **Business context documented: sector, ownership structure, regulatory requirements, key stakeholders**
-
- ☐ **Performance targets and risk tolerance reviewed for alignment — excessive targets create risk-taking pressure**
-

COMPONENT 3 — RISK IDENTIFICATION & ASSESSMENT

-
- ☐ **Risk universe constructed from top-down (strategic) and bottom-up (operational) perspectives**
-
- ☐ **Inherent risk rated independently of controls — do not allow strong controls to mask high inherent risk**
-
- ☐ **Control effectiveness assessed separately from risk rating**
-
- ☐ **Residual risk calculated and explicitly accepted by appropriate authority**
Residual risk = what remains after applying existing controls. This is what the Board accepts.
-
- ☐ **Emerging risk process defined: how are new risks identified and added to the register mid-cycle?**
-
- ☐ **Risk owner assigned for every item in the risk register — not a department, a named individual**
-

- ☐ For each high and critical risk: response strategy documented (accept, avoid, reduce, share)

- ☐ Risk response cost-benefit assessed: cost of control vs. expected loss reduction

- ☐ Residual risks above appetite explicitly accepted in writing — not just implicitly tolerated
Accepted risks must be documented with rationale and Board-level acknowledgment

- ☐ Risk response owners different from risk owners where possible — segregation of assessment and response

- ☐ Insurance and risk transfer instruments reviewed for adequacy against key risk exposures

COMPONENT 5 — CONTROL ACTIVITIES

- ☐ Key controls mapped to highest-rated risks — every high/critical risk has at least one key control

- ☐ Control design assessed: is the control capable of mitigating the risk as designed?

- ☐ Control operating effectiveness tested at frequency proportionate to risk rating

- ☐ Automated controls identified and tested separately from manual controls

- ☐ Segregation of duties analysis completed for all financially significant processes

- ☐ IT general controls reviewed as infrastructure for all automated business controls

COMPONENT 6 — INFORMATION & COMMUNICATION

- ☐ Risk reporting cadence established: Board quarterly, Risk Committee monthly, operational weekly

- ☐ Risk reporting format standardised: consistent metrics, trending, limit vs. actual comparisons

- ☐ Escalation triggers defined: which risk events require immediate Board notification?

- ☐ Risk culture assessment conducted: do employees understand the risk framework and their role in it?
- ☐ External risk communication reviewed: regulatory disclosures, investor communications, public statements

COMPONENT 7 — GCC REGULATORY ALIGNMENT

- ☐ Saudi CMA Corporate Governance Regulations Article requirements mapped to ERM framework (KSA entities)
- ☐ UAE SCA Governance Rules and Corporate Discipline Standards reviewed for listed entities
- ☐ DFSA / ADGM requirements reviewed if applicable
- ☐ Zakat and VAT risk included in tax risk category of the risk register
- ☐ Shari'ah compliance risk assessed where applicable to business model or financing
Common gap in GCC ERM: Shari'ah compliance risk not formally assessed despite material exposure
- ☐ Vision 2030 / UAE National Agenda strategic risks considered: localisation requirements, sector disruption
- ☐ Multi-jurisdiction risk aggregation: if operating in both UAE and KSA, risks consolidated at Group level

From Practice: The most common ERM failure in GCC family businesses is the risk register that exists for regulatory compliance but has no connection to actual decisions. The test: did the risk register change any decision in the last 12 months? If the answer is no, the framework is documentation, not risk management.