

Internal Audit Function Setup Checklist

Building from Zero — Charter, Independence, Methodology, Board Reporting

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

Developed from direct experience building IA functions from zero at three GCC organisations across different ownership structures: pre-IPO tech, KSA family holding group, and regional F&B franchise. Use at function inception or when conducting a structural review of an existing function. Sequence matters: charter and independence (Phase 1) must precede methodology design (Phase 3).

PHASE 1 — CHARTER & INDEPENDENCE

☐ **IA charter drafted covering: mandate, authority, access rights, independence, scope, responsibilities**

☐ **CAE reporting line established: functional reporting to Audit Committee, administrative to CEO**
Independence is a structural condition, not a professional posture — document it before the first audit begins

☐ **Charter approved by Board / Audit Committee — signed copy on file**

☐ **Unrestricted access to all records, personnel, and systems documented in charter**

☐ **Objectivity safeguards defined: cooling-off periods, conflict of interest policy, rotation schedule**

☐ **IA function scope boundary agreed: which entities, subsidiaries, and geographies are in scope**

PHASE 2 — AUDIT COMMITTEE RELATIONSHIP

☐ **Private session cadence established — CAE meets Audit Committee without management present, minimum twice per year**

☐ **Reporting format agreed with Audit Committee — what they want to see and at what frequency**

☐ **Escalation protocol defined — what issues reach the Audit Committee immediately vs. periodic reporting**

☐ **CAE performance evaluation criteria agreed — who assesses, on what basis, and how often**

☐ IA budget approval process established — Audit Committee approves, not management

PHASE 3 — RISK-BASED AUDIT PLANNING

☐ Risk universe constructed — all auditable entities mapped to strategic, operational, financial, compliance risks

☐ Risk ratings applied — inherent risk, control environment, and residual risk for each entity

☐ Annual audit plan approved by Audit Committee before year start
Dynamic plan: new risks emerging mid-year should trigger plan revision, not be ignored until next cycle

☐ Audit plan coverage rationale documented — why high-risk areas are prioritised, why others are deferred

☐ Regulatory and compliance audit requirements identified and built into plan

☐ Management input to risk assessment captured — but auditor retains independent judgment on ratings

- ☐ Audit methodology documented: planning, fieldwork, reporting, follow-up phases
- ☐ IIA Standards compliance confirmed — or gap assessment completed with remediation plan
- ☐ Working paper templates created: planning memo, risk and control matrix, test workpapers, issue summary
- ☐ Finding classification defined: critical, high, medium, low — with escalation thresholds for each
- ☐ Quality review process established — who reviews each workpaper before report issuance
- ☐ Technology stack selected: audit management system, data analytics tool, document storage

PHASE 5 — TEAM & CAPABILITY

- ☐ Staffing model defined: in-house vs. co-source vs. outsource, by skill area
- ☐ Competency framework documented — required skills per audit area and development path
- ☐ Workload capacity calculated and matched to audit plan scope
Coverage expectation: one senior auditor can realistically deliver 3–4 full audits per year
- ☐ Continuing professional education (CPE) requirements tracked per IIA standards
- ☐ Succession and knowledge transfer plan in place — IA function must not depend on one person

PHASE 6 — PERFORMANCE MEASUREMENT

- ☐ KPIs defined: audit plan completion %, findings closure rate, report cycle time, Audit Committee satisfaction
- ☐ Quality Assurance and Improvement Programme (QAIP) established
- ☐ External quality assessment scheduled — IIA peer review every 5 years minimum



Baseline metrics captured at function inception for year-over-year comparison

Benchmarks: 90-day finding closure rate, 85% plan completion, 60-day max report issuance

PHASE 7 — GCC CONTEXT



Language capability assessed — can function operate effectively in Arabic if required?



Local regulatory landscape mapped: UAE IA requirements, Saudi CMA internal audit rules, ESCA



Family business dynamics documented if applicable: informal authority, succession risk, governance gaps



Cross-border coordination model defined for multi-jurisdiction GCC entities

From Practice: The most common failure mode in new IA functions is methodology before independence. Audit committees sign charters, approve plans, and then are surprised when management overrides findings. The reporting line and charter are the foundation. Everything else is technique.