MD. ABDULLAH AL OWASI

TECHNOLOGY RISK & AI GOVERNANCE ARCHITECT

Governance architecture built for scrutiny.

I design the operating infrastructure behind enterprise trust: controls, evidence lineage, ownership, exceptions, remediation, monitoring and residual-risk decisions.

10	15	25	20
governance systems	AI use cases	buyer questions	vendor-risk questions

Requirement → Control → Evidence → Exception → Residual Risk → Decision

Kuala Lumpur, Malaysia · abdullahalowasi369@gmail.com
linkedin.com/in/md-abdullah-al-owasi · github.com/abdullahalowasi369-dev

01 / OPERATING MODEL

Trust becomes useful when it produces a decision.

The portfolio is organized around a single operating chain. Each stage answers a different executive question and creates the evidence needed for the next decision.

Requirement	What obligation, risk or business question exists?
Control	What operating expectation addresses it?
Evidence	What proves the control exists and operates?
Exception	Where is the control incomplete, ambiguous or failing?
Residual risk	What exposure remains after treatment?
Decision	Who accepts, remediates, escalates or rejects?

Executive value

Revenue-sensitive assurance Evidence-backed customer assurance designed to keep diligence moving without unsupported claims.	**Audit-ready evidence operations** Control evidence tied to owner, cadence, test logic, exceptions, remediation and retesting.
Decision-grade AI governance AI inventories connected to oversight, evaluation, monitoring, transparency and residual-risk decisions.	**Risk-based TPRM** Vendor scrutiny prioritized by criticality, data exposure, assurance evidence, contractual obligations and residual risk.

02 / ENTERPRISE ASSURANCE & TPRM

Governance systems built for scrutiny.

Enterprise Trust & Customer Assurance Architecture

15 evidence domains · 25 buyer-diligence questions

Maps recurring customer trust questions to evidence paths, owners, review cadence, exceptions and remediation. Coverage includes identity, encryption, incident response, subprocessors, retention and AI data use.

SOC 2 TSC · ISO/IEC 27001 · GDPR Art. 28 · NIST AI RMF

Third-Party Risk & AI Provider Decision System

10 vendors · 20 vendor-risk questions · 4 decision states

Structures vendor criticality, data exposure, assurance evidence, processor obligations and residual-risk treatment into approve, remediate, accept or reject decisions.

TPRM · GDPR Art. 28 · SOC 2 · ISO/IEC 27001

Control-to-Evidence & Continuous Audit Architecture

15 control domains · 15 audit requests

Connects control intent to evidence, owner, cadence, test procedure, exception, remediation and retest state. Designed so assurance work has an explicit operating rhythm instead of point-in-time collection.

SOC 2 TSC · ISO/IEC 27001 · Continuous assurance

Portfolio artifacts

Evidence matrix · customer assurance knowledge base · vendor risk register · control inventory · audit tracker · executive risk register

03 / AI GOVERNANCE

AI governance needs operating mechanics, not principles alone.

The AI architecture connects business purpose, data, stakeholders, human oversight, evaluation, monitoring, transparency and residual risk. NIST AI RMF provides the primary lifecycle through Govern, Map, Measure and Manage.

Govern	Ownership, policy, accountability, escalation and governance structure
Map	Business context, affected stakeholders, data, dependencies and risk context
Measure	Evaluation, testing, monitoring signals and evidence
Manage	Risk treatment, acceptance, prioritization, monitoring and response

15-use-case AI governance register

Use cases are modeled across purpose, stakeholder exposure, human oversight, inherent risk, controls, residual risk, monitoring and transparency decision fields. The architecture also includes Article 50 applicability and transparency actions for relevant interactive and synthetic AI cases.

Framework basis

NIST AI RMF 1.0 · NIST Generative AI Profile · ISO/IEC 42001:2023 · EU AI Act Article 50

Sources: https://www.nist.gov/itl/ai-risk-management-framework · https://www.iso.org/standard/42001 · https://digital-strategy.ec.europa.eu/en/policies/guidelines-ai-transparency-obligations

04 / MARKET ALIGNMENT

Built around the work current Malaysia roles actually ask for.

Recent Kuala Lumpur / Malaysia postings repeatedly emphasize technology risk assessment, ISO/IEC 27001, control effectiveness, audit/evidence coordination, third-party risk, remediation, executive reporting and AI-governance stakeholder work.

Current role signal	Portfolio evidence
Technology / cyber risk assessments	15-risk executive register with treatment, KRI and escalation logic
ISO/IEC 27001 and compliance gap analysis	15-domain control-to-evidence architecture
Audit readiness and evidence collection	Evidence ownership, audit request and exception/retest workflows
Third-party risk and vendor due diligence	10-vendor register and 20-question assessment
Management / executive reporting	Residual-risk, KRI threshold and escalation structures
AI governance and regulatory monitoring	15-use-case AI register and transparency decision logic
Cross-functional stakeholder work	Ownership modeled across Security, Legal, Risk, Procurement, Product and Business

Selected 2026 market sources

Razer — Senior IT Risk & Compliance Specialist · TIME dotCom — IT Risk & Compliance Analyst · AIA — Technology Risk Governance & Control, Principal · Maybank — AI Governance Specialist · Standard Chartered — Manager, Risk Management - AI

Source URLs are included in the companion Trust Architecture Evidence Matrix workbook.

05 / TECHNICAL FOUNDATION

Systems thinking makes governance more executable.

My computer science foundation strengthens the technical side of technology risk work: software engineering, data structures, databases, automation, typed interfaces and disciplined problem decomposition.

Technical toolkit

Python · SQL / data modeling · TypeScript · React · Next.js · Git / GitHub · structured evidence data · governance artifact generation

Framework depth

NIST AI RMF · NIST Generative AI Profile · ISO/IEC 27001:2022 · AICPA Trust Services Criteria · ISO/IEC 42001:2023 · EU AI Act Article 50 · GDPR Article 28

The conversation

Bring the governance problem that cannot stay ambiguous.

I am open to high-ownership opportunities across Technology Risk, GRC, Security Compliance, Third-Party Risk and AI Governance. Send the role, business context and hardest unresolved risk question; the portfolio shows the architecture and decision logic I would bring to the conversation.

abdullahalowasi369@gmail.com
personal-portfolio-website-e13.pages.dev
linkedin.com/in/md-abdullah-al-owasi
github.com/abdullahalowasi369-dev