GOVERNANCE PORTFOLIO

Technology Risk · Control Assurance · Third-Party Risk · AI Governance

Md. Abdullah Al Owasi · 2026

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

An executive governance portfolio built for inspection: systems, decision logic, evidence structures, ownership models, exception treatment and residual-risk decisions across assurance, third-party risk and AI governance.

01 — Executive Thesis

Governance earns value when material requirements become accountable controls, inspectable evidence, visible exceptions and explicit decisions. The portfolio applies that operating model across assurance, third-party risk and AI governance.

10	15	25	20
Governance systems	AI use cases	Buyer diligence paths	Vendor-risk questions

02 — Decision Architecture

Stage	Operating question	Primary output
Requirement	What obligation, risk expectation or business need is material?	Scoped requirement
Control	What behavior, configuration or process should manage it?	Control objective
Evidence	What proves the control exists or is operating?	Evidence object / source
Exception	What is unmet, uncertain or dependent on remediation?	Exception / gap state
Residual Risk	What remains after current controls are considered?	Residual-risk assessment
Decision	Who accepts, remediates, escalates, approves or rejects?	Owned decision

03 — Flagship Architecture

Enterprise Assurance Evidence Fabric

Control-to-evidence architecture connecting trust claims to owners, framework references, evidence, exception state and remediation decisions.

Evidence architecture: 15 control/evidence domains · 25 buyer-diligence paths

AI Governance Decision Architecture

AI-use-case register connecting purpose, data classes, stakeholders, human oversight, NIST AI RMF functions, controls, residual risk, monitoring and transparency decisions.

AI governance architecture: 15 mapped AI use cases

Third-Party Risk Decision Engine

Criticality-driven model connecting data exposure, assurance evidence, contractual obligations and residual risk to scrutiny depth and decision state.

TPRM architecture: 20-question assessment · 10 vendor-risk profiles

04 — Governance Systems

System	Decision focus	Inspectable artifact
Enterprise Trust & Customer Assurance	Reusable, evidence-backed assurance responses	Trust evidence matrix
AI Governance Operating System	Inventory, risk ownership, oversight and monitoring	AI risk register
Third-Party Risk Management	Criticality and evidence-driven vendor decisions	Vendor risk register + assessment
SOC 2 + ISO 27001 Control Evidence	Control intent, evidence and test state	Control inventory
Executive Technology Risk	Residual risk, KRIs, thresholds and escalation	Executive risk register
AI Transparency & Article 50	Transparency applicability and accountable action	Transparency register
Shadow AI & Prompt DLP	Unsanctioned AI and sensitive-data controls	Control standard
Procurement Security Triage	Consistent diligence answers and evidence paths	Question library
GDPR Article 28 Processor Governance	Processor/subprocessor obligation tracking	DPA control set
Continuous Audit Operations	Evidence requests, review, remediation and retest	Audit operations tracker

05 — AI Risk & Oversight Sample

Selected use cases from the 15-use-case AI governance register. Risk values structure assessment across exposure, oversight depth, control treatment and transparency decisions.

Use case	Inherent risk	Human oversight	Residual state
Customer chatbot	12	Escalation for material issues	Medium
Security questionnaire assistant	15	GRC approval	Medium
Contract review assistant	15	Legal review	Medium
Code assistant	15	Developer review + CI tests	Medium
Fraud alert prioritizer	15	Analyst decision	Medium
Executive risk summarizer	10	CISO/GRC approval	Low

06 — Third-Party Risk Decision Logic

Signal	Higher-scrutiny condition	Decision consequence
Criticality	Tier 1 / material dependency	Deeper assurance evidence and owner approval
Data exposure	Sensitive, regulated or customer data	Privacy/security terms + evidence depth

Signal	Higher-scrutiny condition	Decision consequence
Evidence quality	Partial or stale assurance evidence	Gap treatment or conditional decision
Residual risk	Above appetite / unresolved material gap	Remediate, escalate, accept or reject with owner

07 — Technical Foundation

Python for structured governance workflows · SQL/data modeling for risk and evidence inventories · TypeScript/React/Next.js for typed decision interfaces · Git/GitHub for version control and traceability.

Education: Bachelor of Computer Science (Hons) — AI & Cybersecurity Specialization, SEGi University, Malaysia.

08 — Framework Basis

Framework / source	How it is used in the portfolio
NIST AI RMF 1.0	Govern · Map · Measure · Manage structure for AI risk work.
ISO/IEC 27001:2022	ISMS/control-assurance lens and evidence ownership.
SOC 2 Trust Services Criteria	Security, Availability, Processing Integrity, Confidentiality and Privacy assurance lens.
ISO/IEC 42001:2023	AI management-system governance concepts.
EU AI Act — Article 50	Transparency decision logic for relevant provider/deployer scenarios.
GDPR Article 28	Processor/subprocessor contractual-governance lens.

09 — Verification

Website: https://aaowasi369v7.pages.dev

Primary evidence: Governance_Evidence_Workbook.xlsx · Governance_Evidence_Matrix.xlsx

Framework sources: nist.gov · iso.org · aicpa-cima.com · digital-strategy.ec.europa.eu · eur-lex.europa.eu