

Govern how your people use AI, and how your teams build it

A ready-to-adopt set of policies, standards, procedures and templates. It works with any AI vendor, scales from a 50-person SME to a regulated bank, and maps to Malaysian, Singaporean and international frameworks.

48

templates in Word and Excel

422

auditable controls, each with an ID

3

adoption tiers: Lite, Standard, Regulated

4

vendor annexes: Claude, OpenAI, Microsoft, Google

What it is. Templates for the rules, roles and records an organisation needs to use and build AI safely.

Who it's for. Organisations from about 50 staff to regulated banks in Malaysia and Singapore, on any AI platform.

What to do first. Take the two-minute check below, then open the first document it names.

Start here

Two-minute check

Reading order

Leadership decisions

First 90 days

Document map

How it's built

Frameworks

Shared rules

Day-to-day flows

Who does what

Why now

FAQ

Support

START HERE

Which path are you on?

Pick the description closest to you, or take the two-minute check below. Each path tells you which document to open first.

Starting out with AI

Staff use, or want to use, vendor AI tools. Little or no AI policy yet.

Open AGK-001 Lite Quick Start → follow the 90-day plan

Using AI tools that act

Connectors to email or files, browser agents, or shared skills are on, or about to be.

AGK-001, then Track A: AGK-STD-A03 and A04 before switching features on

Building agents or customer-facing AI

You build AI applications or agents, or AI touches customers or decisions about people.

AGK-000, then Track B (AGK-STD-B01 to B06) and AGK-PRC-02

Regulated or seeking ISO/IEC 42001

Financial institution under BNM or MAS, healthcare, EU exposure, or certification planned.

AGK-000, then the Statement of Applicability in AGK-TPL-08

TWO-MINUTE CHECK

Find your tier and your first five documents

Are you regulated by BNM, MAS or a health regulator, have EU exposure, or plan ISO/IEC 42001 certification?

☐ Yes ☒ No

Do you build AI agents or AI applications, in-house or with a partner?

☐ Yes ☒ No

Do customers interact with your AI, or does AI help make decisions about people (hiring, credit, pricing)?

☐ Yes ☒ No

Do more than 250 staff use AI tools?

☐ Yes ☒ No

Are connectors that can write, browser agents or shared skills switched on, or planned?

☐ Yes ☒ No

Do you already have an approved AI tool and an AI usage policy?

☐ Yes ☒ No

RECOMMENDED TIER

Lite

Because: vendor AI tools, no in-house builds.

Open these first

1. AGK-001 Lite Quick Start
2. AGK-PRC-07 AI Discovery & Shadow AI
3. AGK-P0L-02 Acceptable Use Policy (with AGK-GDL-A01 and AGK-TPL-07)
4. AGK-STD-A02 AI Data Handling
5. AGK-STD-A01 Platform Baseline + your Vendor Annex

Read these in this order

The order matters: each document assumes the ones before it. Times are for a first read.

1	This pre-read	Everyone involved	10 min
2	AGK-001 Lite Quick Start (Standard and Regulated: AGK-000 Framework)	AI sponsor, AI Governance Lead	15 min
3	AGK-PRC-07 AI Discovery & Shadow AI	AI Governance Lead, IT	10 min
4	AGK-POL-02 Acceptable Use Policy and AGK-GDL-A01 Safe AI Use Guide	HR, AI Governance Lead	20 min
5	AGK-STD-A02 AI Data Handling (the data × tool matrix)	DPO, IT Security	10 min
6	AGK-STD-A01 Platform Baseline and the Vendor Annex for your platform	AI Platform Administrator	30 min
7	AGK-GDL-C02 Adoption Roadmap and AGK-GDL-C03 Change & Communication	AI sponsor, HR	25 min

FOR LEADERSHIP

Six decisions to make in week 1

Nothing else moves until these are made. Each takes one conversation, not a project.

Who owns AI?

Name an AI sponsor (executive) and an AI Governance Lead.

AGK-POL-01

Who decides?

Form a three-person committee: sponsor, Governance Lead, DPO.

AGK-POL-01

How much risk is acceptable?

One paragraph of risk appetite: what AI may and may never be used for.

AGK-POL-01

Which AI tool is approved?

Confirm the platform(s) staff should use instead of personal accounts.

AGK-GDL-C01

Time and budget

About half a day a week for the Governance Lead in the first 90 days, plus licences.

AGK-001

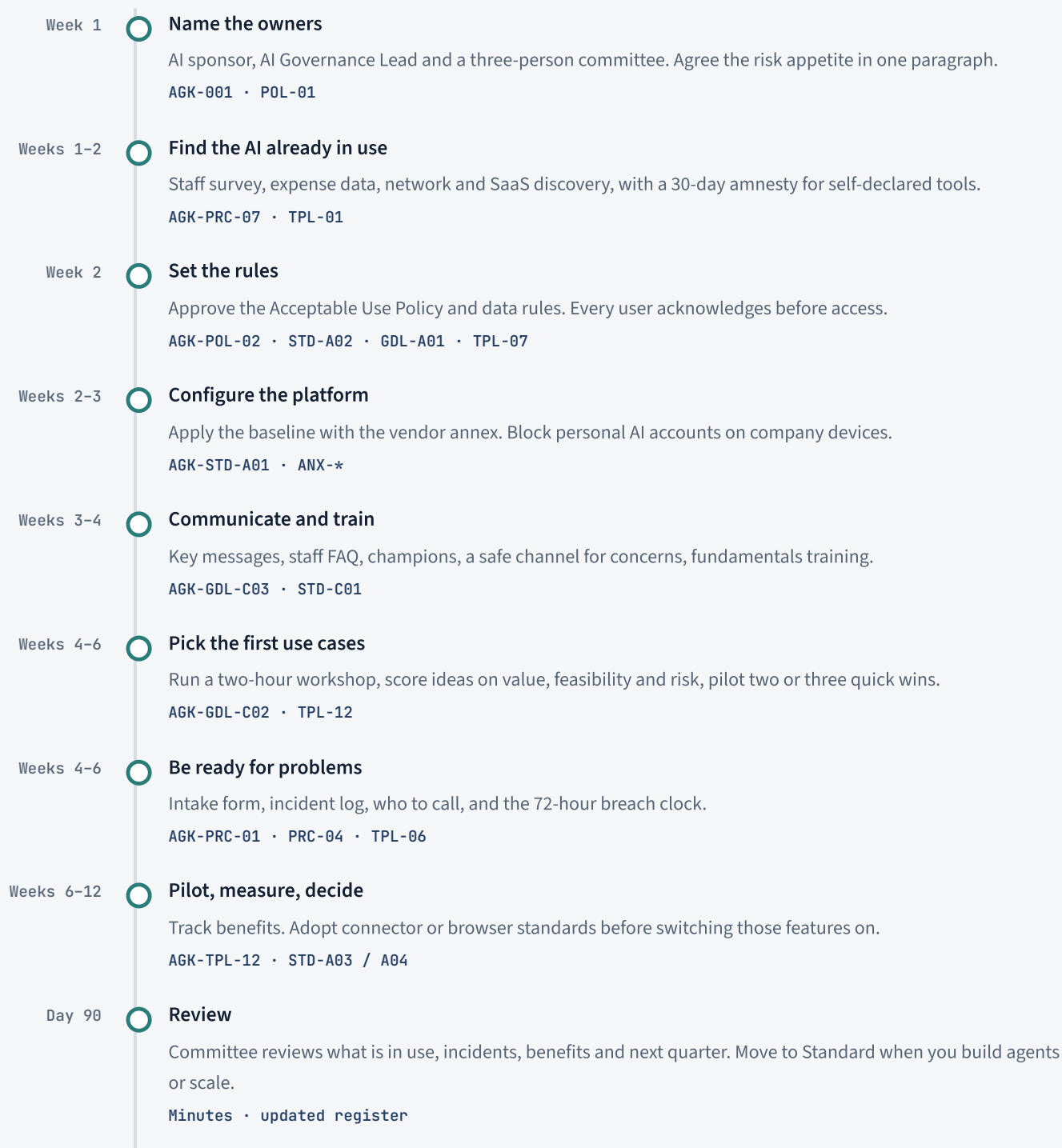
What we say about jobs

A short, honest statement on how AI affects roles, before staff ask.

AGK-GDL-C03

The first 90 days for an organisation starting out

This is the Lite path from AGK-001. Each step ends with something approved, configured or populated. Standard and Regulated adopters follow the same order and add the remaining documents.



TERMS YOU'LL SEE

Ten terms used across the kit

Lite / Standard / Regulated	Adoption tiers. Each control says the lowest tier it applies to.	Control ID	A testable requirement, e.g. AGK-STD-A03-C09 (document, then control number).
AIGC	AI Governance Committee. Can be three people or an existing risk committee.	AI Governance Lead	The person who runs the kit day to day.
T0-T3	AI tool tiers, from consumer tools (T0) to agents that can act (T3).	Data labels	Public, Internal, Confidential, Restricted, Secrets.
A0-A4	How much an agent may do on its own, from suggest-only to high autonomy.	Connector	A link that lets an AI tool read or act in another app, including MCP servers.
Vendor Annex	The only document naming vendor settings; one per AI platform.	Shadow AI	AI tools used without approval, often on personal accounts.

DOCUMENT MAP

Pick a tier to see what you adopt

Select your adoption tier, then select any document to see what it covers. Faded documents are optional at that tier.

26 documents in scope · 53 Lite controls (39 from day one, 14 once features are on) · plus one annex per platform you use

Lite: organisations starting out with vendor AI tools. 53 controls in total; start with AGK-001 Lite Quick Start.

Required Condensed version is fine Once the feature is switched on Optional / if platform used

FRAMEWORK

AGK-000 v1.0

Framework & Document Architecture

AGK-001 v1.0

Lite Quick Start & Checklist

CORE POLICIES

AGK-POL-01 v1.0

Governance Charter & Operating Model

AGK-POL-02 v1.0

AI Acceptable Use Policy

AGK-POL-03 v1.0

AI Risk & Data Governance Policy

CORE PROCEDURES

AGK-PRC-01 v1.0

Use Case Intake & Approval

AGK-PRC-02 v1.0

Risk & Impact Assessment

AGK-PRC-03 v1.0

Vendor & Model Assessment

AGK-PRC-04 v1.0

AI Incident Response

AGK-PRC-05 v1.0

Review & Recertification

AGK-PRC-06 v1.0

Red-Team & Adversarial Testing

AGK-PRC-07 v1.0

AI Discovery & Shadow AI

TRACK A · USE

AGK-STD-A01 v1.0

Platform Configuration Baseline

AGK-STD-A02 v1.0

AI Data Handling

AGK-STD-A03 v1.0

Connector & Integration

AGK-STD-A04 v1.0

Browser & Computer Use

AGK-STD-A05 v1.0

Skills, Plugins & Instructions

AGK-PRC-A01 v1.0

Connector & Tool Request

AGK-GDL-A01 v1.0

Safe AI Use Guide for Staff

	AGK-STD-C01 v1.0 AI Literacy & Training	AGK-GDL-A01-BM v1.0 Panduan Penggunaan AI Selamat (BM)
	AGK-STD-C02 v1.0 Transparency & Disclosure	
	AGK-GDL-C01 v1.0 Platform Selection & Evaluation Guide	
	AGK-GDL-C02 v1.0 Adoption Roadmap & Use-Case Prioritisation	
TRACK B · BUILD	AGK-GDL-C03 v1.0 TEMPLATES Change & Communication Playbook	VENDOR ANNEXES
AGK-STD-B01 v1.0 Agent Development Lifecycle	AGK-TPL-01 v1.0 AI System Register (Excel)	AGK-ANX-C v1.0 Claude (Anthropic)
AGK-STD-B02 v1.0 Agent Identity & Tool Authorization	AGK-TPL-02 v1.0 Connector & Tool Registry (Excel)	AGK-ANX-D v1.0 OpenAI
AGK-STD-B03 v1.0 Evaluation & Release Gates	AGK-TPL-03 v1.0 Use Case Intake Form	AGK-ANX-M v1.0 Microsoft
AGK-STD-B04 v1.0 Guardrails & Security	AGK-TPL-04 v1.0 Risk & Impact Assessment Form	AGK-ANX-G v1.0 Google
AGK-STD-B05 v1.0 Monitoring, Logging & Remediation	AGK-TPL-05 v1.0 Vendor Assessment Checklist (Excel)	
AGK-STD-B06 v1.0 Model, Prompt & Config Lifecycle	AGK-TPL-06 v1.0 Incident, Nonconformity & CAPA Log (Excel)	
	AGK-TPL-07 v1.0 Acceptable Use Acknowledgement	
	AGK-TPL-07-BM v1.0 Pengakuan Dasar Penggunaan AI (BM)	
	AGK-TPL-08 v1.0 Control Library, Lite Checklist & ISO SoA (Excel)	
	AGK-TPL-09 v1.0 Platform Evaluation Scorecard (Excel)	
	AGK-TPL-10 v1.0 Adversarial Test Catalogue (Excel)	
	AGK-TPL-11 v1.0 Incident Tabletop Exercise Pack	
	AGK-TPL-12 v1.0 Use-Case Prioritisation & Benefits (Excel)	

AGK-000 · Framework & Document Architecture

guide

Start here. Hierarchy, document register, tiers and shared definitions.

Owner: AI Governance Lead · At Lite: Required

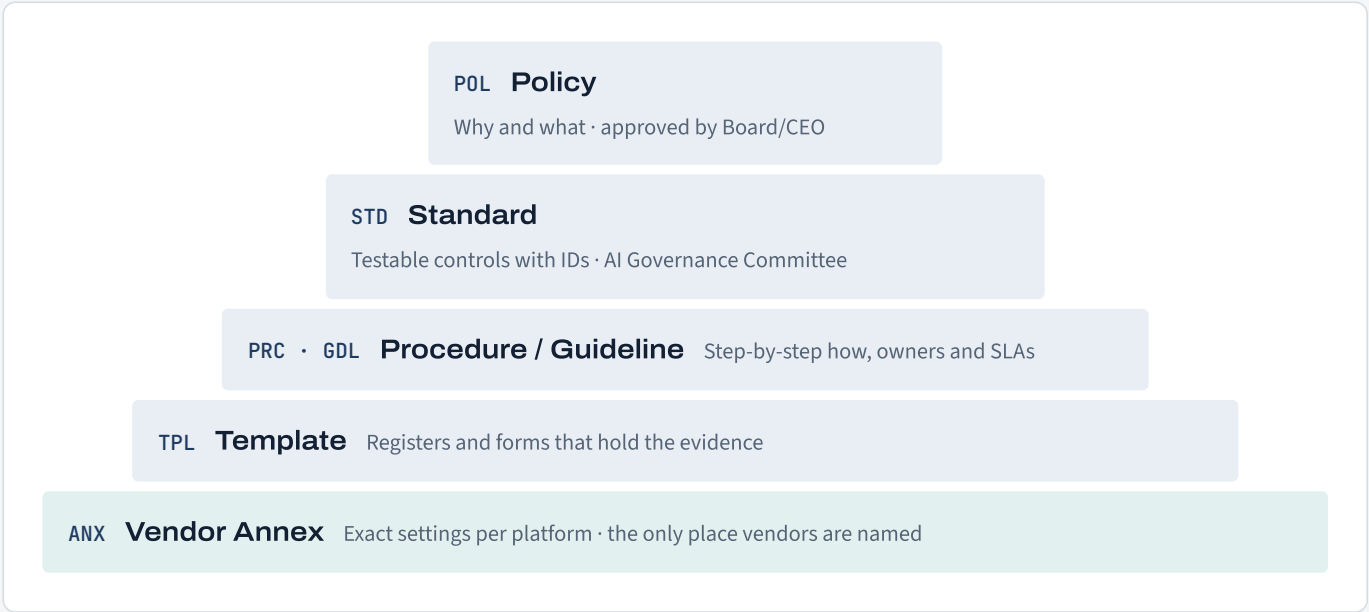
Template v1.0 · 2026-10-31 — Initial release

Kit file: 00_Framework / AGK-000_AI_Governance_Framework_and_Document_Architecture_v1.0.docx

HOW IT'S BUILT

Five levels, from board principle to platform setting

Each level answers a different question and changes at a different speed. Policies stay stable for years. Vendor settings change monthly, so they live at the bottom where updating them never needs board approval.



Follow one requirement down the levels

POLICY	AI agents shall not take irreversible actions without human approval.
STANDARD	AGK-STD-A03-C09 Each write or act tool on a connector is set to "needs approval" or "blocked".
PROCEDURE	AGK-PRC-A01 How a request to enable a write tool is triaged, approved and logged.
TEMPLATE	AGK-TPL-02 Registry row records the tool, its setting and the approver.
ANNEX	AGK-ANX-C On Claude: per-tool permission set to "Needs approval". Each other vendor annex gives its own setting.

Built on ISO/IEC 42001, risk-managed with NIST, mapped to local rules

The kit does not invent its own framework. It follows one international management-system standard for structure, one risk framework for method, and maps every document to the rules that apply in Malaysia, Singapore and beyond.

STRUCTURE

ISO/IEC 42001:2023

The AI management system standard. Gives the kit its plan–do–check–act cycle, the policy and roles at the top, and the 38 Annex A controls. TPL-08 holds a ready Statement of Applicability.

RISK METHOD

NIST AI RMF 1.0 and GenAI Profile

Govern, Map, Measure, Manage. Shapes how risks are identified, assessed and treated in the procedures.

LOCAL RULES

Malaysia and Singapore

Malaysia AIGE principles, PDPA 2010 (as amended), draft AI Governance Bill and JPDP framework; Singapore Model AI Governance Frameworks incl. Agentic AI, and MAS AI risk guidelines for financial institutions.

SECURITY AND REACH

OWASP and EU AI Act

OWASP Top 10 for LLM and Agentic Applications for threats and testing. EU AI Act articles where outputs reach the EU.

The ISO/IEC 42001 cycle, and which documents run each part

<p>Plan</p> <p>Context, policy, risk appetite, objectives, risk and impact assessment, adoption roadmap</p> <p>POL-01 • POL-03 • PRC-02 • GDL-C02</p>	<p>Do</p> <p>Run AI safely: intake, vendors, discovery, training, Track A and Track B controls</p> <p>PRC-01 • PRC-03 • PRC-07 • STD-C01 • STD-A01-A05 • STD-B01-B06</p>
<p>Check</p> <p>Review, recertify, audit, test controls and red-team, measure benefits</p> <p>PRC-05 • PRC-06 • TPL-08 • TPL-10 • TPL-12</p>	<p>Act</p> <p>Handle incidents, correct nonconformities, management review, improve</p> <p>PRC-04 • TPL-06 • PRC-05 (management review)</p>

Where each part of the kit maps

Kit area	ISO/IEC 42001	NIST AI RMF	Malaysia AIGE / PDPA	Singapore MGF	MAS AIRG	EU AI Act
Charter and policies (POL-01–03)	●	●	●	●	●	○
Intake, risk, vendor, discovery (PRC-01–03, 07)	●	●	●	●	●	○
Incidents and testing (PRC-04, 06, TPL-10, 11)	●	●	●	●	○	○
Review, audit, improvement (PRC-05, TPL-06, 08)	●	●	○	○	●	○

Kit area	ISO/IEC 42001	NIST AI RMF	Malaysia AIGE / PDPA	Singapore MGF	MAS AIRG	EU AI Act
Training, transparency, change (STD-C01–02, GDL-C03)	●	●	●	●	○	●
Track A: using AI tools (STD-A01–A05)	●	○	●	●	○	○
Track B: building agents (STD-B01–B06)	●	●	○	●	●	●

● directly addressed · ○ partly or indirectly. Every document ends with a "Framework alignment" table, and AGK-TPL-08 maps all 422 controls individually.

How every document is laid out

All documents share the same anatomy, so a reader who knows one can navigate any of them.

1 Document control

ID, template version, your client version, owner, approver, review cycle, parent documents, and the tier status

2 Template guidance

Yellow boxes explaining how to adapt the document; deleted before issue

3 Purpose and scope

Why the document exists and what it covers

4 Requirements

Controls with IDs (e.g. AGK-STD-A03-C09), each tagged for the tiers it applies to

5 Roles and responsibilities

Who does what, often as a RACI table

6 Compliance and exceptions

How compliance is checked and how time-bound exceptions are approved

7 Framework alignment

The ISO, NIST, Malaysian, Singaporean, EU and OWASP references the document supports

8 Version history and approval

Template version history from Anchor Sprint, then your sign-off and client revision record

TWO TRACKS, ONE CORE

Using AI and building AI are governed separately

Track A is for everyone who uses AI tools. Track B is for teams that build agents and AI systems. Both share one core, so a SaaS assistant and an in-house agent sit in the same register, use the same risk tiers and follow the same incident procedure.

Track A · AI use

all staff · admins

How do our people use AI tools safely?

- Platform configuration baseline
- What data can go into which tool
- Connectors and MCP servers
- Browser and computer-use agents
- Skills, plugins and custom instructions

Track B · AI build (AgentOps)

engineering · platform

How do we build and run AI systems and agents safely?

- Agent development lifecycle and design gates
- Agent identity, access and tool authorisation
- Evaluation and release gates
- Guardrails and security

Core · applies to both

governance · risk · privacy

Charter and operating model · Acceptable Use Policy · Risk & Data Policy · AI discovery · adoption roadmap · change & communication · use-case intake · risk & impact assessment · vendor assessment · incident response · red-team testing · periodic review and management review · training · transparency

SHARED RULES

One vocabulary across every document

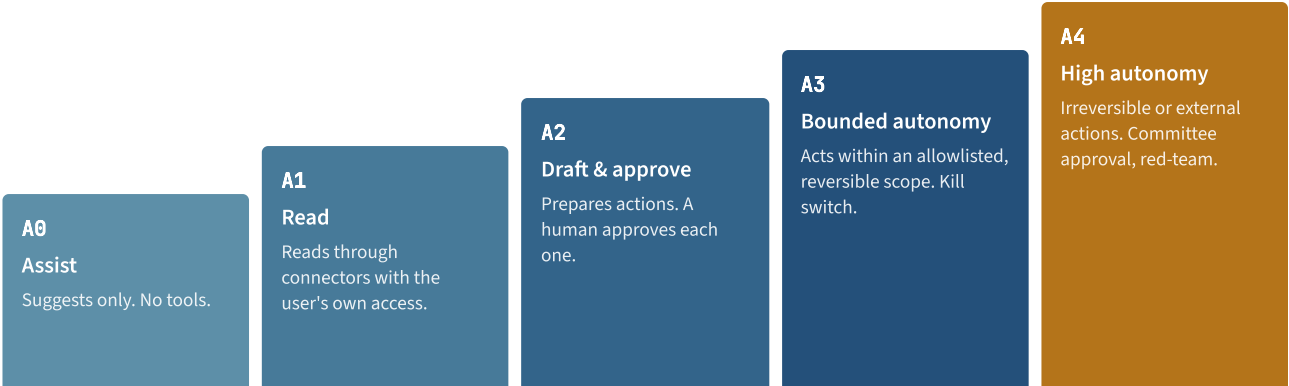
Four definitions do most of the work. They let a staff member, an engineer and an auditor talk about the same risk in the same words.

Which data can go into which AI tool

Tool tier ↓ · Data label →	Public	Internal	Confidential	Restricted	Secrets
T0 Consumer / unapproved AI	Yes	No	No	No	Never
T1 Approved enterprise AI SSO, no training on our data, audit logs	Yes	Yes	Yes	With approval DPIA + use case	Never
T2 Hardened enterprise AI + retention, transfer assessment, keys/residency	Yes	Yes	Yes	Approved uses	Never
T3 Agentic AI that can act write connectors, browser, autonomous	Per agent	Per agent	Approval tools	Committee human on every irreversible step	Never

Full matrix in AGK-STD-A02. Secrets means passwords, API keys, tokens and private keys.

How much an agent may do on its own



Every agent declares its level at design time. Higher levels need more controls (AGK-STD-B01).

Use-case risk tiers

- **Prohibited:** not permitted (e.g. manipulative or social-scoring uses)
- **High:** decisions about people, material harm, A3–A4 agents → AI Governance Committee
- **Medium:** Confidential data, contained risk → AI Governance Lead
- **Low:** productivity with human review → self-service within the AUP

Data labels

- **Public:** published material
- **Internal:** everyday business information
- **Confidential:** contracts, pricing, financials, most code
- **Restricted:** personal data at scale, regulated or client-secret data
- **Secrets:** credentials, never entered into any AI tool

DAY-TO-DAY FLOWS

What the kit looks like in practice

Someone asks for a new connector

STAFF Submits request Business need, data involved, account type AGK-PRC-A01	PLATFORM ADMIN Triages into a lane Green, Amber or Red within agreed SLA AGK-STD-A03	APPROVER Decides Read-only by default. Write tools set to needs-approval AGK-STD-A03-C08/C09	PLATFORM ADMIN Configures & records Registry row before enabling AGK-TPL-B02	MONTHLY Reconciles Enabled vs approved. Gaps become incidents AGK-STD-A03-C18
---	---	---	---	--

Green · pre-approved

Read-only, up to Internal data, company account, vetted publisher

Amber · review

Write actions, Confidential data, new vendor or broad scopes

Red · decline or escalate

Restricted data without T2, personal accounts, unvetted publisher

A team builds an agent

INTAKE Register the use case Triage and risk tier AGK-PRC-B01 · TPL-B03	DESIGN Declare autonomy A0–A4 Threat model, identity, tool allowlist AGK-STD-B01 · B02	EVALUATE Pass release gates Accuracy, safety, privacy, injection tests AGK-STD-B03	OPERATE Monitor & log Daily safety scans, weekly drift review AGK-STD-B05	IF IT MISBEHAVES Remediate Suspend → lockout → repair → reintegrate AGK-STD-B05 · PRC-B04
--	---	---	--	--

WHO DOES WHAT

Named people, not committees alone

Board / CEO

Approves the charter and AI risk appetite. Receives an annual report.

AI Governance Committee

Approves standards, high-risk use cases, A3–A4 agents and exceptions. Can be your existing risk committee.

AI Governance Lead

Runs the kit day to day: intake, registers, reviews, training.

AI System Owner

The named business owner accountable for each AI system or agent.

AI Platform Administrator

Configures platforms to the baseline. Keeps registries and annexes current.

CISO / IT Security

Security review of connectors and agents. Leads incident response.

Data Protection Officer

PDPA compliance, impact assessments, transfer assessments, breach notification.

Every employee

Uses approved tools, follows the data rules, reviews AI output, reports problems.

WHY NOW • STATUS AS AT OCTOBER 2026

AI rules in Malaysia and Singapore are moving from voluntary to expected

Most organisations already use AI tools, and many now connect them to email, files and business systems, or let agents act in a browser. That moves AI risk from "what did someone type" to "what can this system do on our behalf".

Regulators are converging on the same expectations: know what AI you run, classify its risk, name a human owner, control third parties, and report incidents. The kit gives you those building blocks on day one.

Instrument	Status (Oct 2026)	What it expects
Malaysia: National Guidelines on AI Governance & Ethics	Voluntary, in effect	Seven principles incl. accountability, transparency, privacy
Malaysia: PDPA as amended 2024	In force	DPO, 72-hour breach notification, cross-border transfer rules
Malaysia: AI Governance Bill	Draft (consultation)	Developer and deployer duties, harm tiers, incident and near-miss reporting
Malaysia: JPDP AI & Personal Data Framework	Draft (consultation)	Privacy by design and impact assessment across the AI lifecycle
Singapore: Model AI Governance Framework for Agentic AI	Voluntary, in effect	Bound agent risks upfront, human accountability, technical controls
Singapore: MAS AI Risk Management Guidelines	Final, applies from 2027	Inventory, risk materiality, lifecycle controls (financial institutions)

FAQ

▼ Do we need all 48 documents?

No. A Lite adopter uses about 20 of them and 53 controls. The rest are added when you switch on connectors or browser agents, build agents, or become regulated. The two-minute check above tells you where you are.

▼ How long does it take?

Lite: about 90 days to be in a stable state, with the most important steps (policy, data rules, approved tool) done in the first three weeks. Standard: three to six months depending on how much AI you build.

▼ Is this legal compliance?

It is a governance framework mapped to Malaysian and Singaporean laws and guidelines, ISO/IEC 42001, NIST and the EU AI Act. It is not legal advice. Regulated organisations should have their pack reviewed by counsel.

▼ Do we need ISO/IEC 42001 certification?

Not to start. The kit follows the standard's structure, so if certification becomes necessary (often because a customer asks), the Statement of Applicability in AGK-TPL-08 is already started.

▼ Does it only work with Claude?

No. Policies and standards are vendor-neutral. Vendor Annexes cover Claude, OpenAI, Microsoft and Google; you use the ones for the platforms you run.

▼ Will this slow AI adoption down?

It should do the opposite. Clear rules and an approved tool remove the uncertainty that stops people trying AI, and the adoption roadmap (AGK-GDL-C02) picks the use cases worth doing first.

▼ What does it cost to run?

Mainly time: about half a day a week for the AI Governance Lead and an hour a month for the committee at Lite. Some controls need platform licences with admin features (single sign-on, audit logs).

WORKING WITH THE TEMPLATES

What to keep, what to change

Keep unchanged

- Document structure and IDs
- Control IDs and their intent
- The shared definitions: labels, tiers, autonomy levels

Keeping IDs lets you reuse the control library and adopt future kit updates without re-mapping.

Tailor to your organisation

- Names, roles, committee membership
- Thresholds, SLAs and review periods
- Approved tools and vendor annexes
- Sector overlays (BNM, MAS, healthcare)

Two versions on every document

Template version

Set by Anchor Sprint, for example AGK-POL-02 v1.0.
Shown under the title, in Document control, in the footer and in the file name, with a full change history at the end.
Minor (1.0 → 1.1) for wording and defaults; major (1.x → 2.0) when a mandatory control or approval rule changes.

Client version

Yours, starting at 0.1 for a draft and 1.0 when approved.
The first row of your revision history records which template version you adopted, so you can see what changed when a new template is released.

The full register of document versions is in AGK-000 (Section 4) and on the Documents & Versions sheet of AGK-TPL-08.

Reading the templates. Yellow highlighted [placeholders] are values you set. Yellow "Template guidance" boxes explain how to adapt a section and are deleted before issue. Controls marked "All tiers", "Standard + Regulated" or "Regulated only" tell you whether they apply to you.

Where to start

1. Read AGK-001

Lite Quick Start, or AGK-000 for the full framework

2. Run AGK-PRC-07

Find the AI already in use

3. Draft POL-02

The Acceptable Use Policy is the first thing staff see

4. Configure with the annex

For each AI platform you use

This kit is not legal advice. Status of draft laws reflects October 2026. Regulated-tier adopters should have their pack reviewed by Malaysian or Singaporean counsel.

SUPPORT

How Anchor Sprint can help

You can adopt the kit yourselves. If you want help, these are the usual starting points.

Starter

Lite pack set up for your organisation, shadow-AI discovery and two workshops (leadership and use cases).

Implement

Standard pack, AI platform hardened to the baseline, connector and browser-agent controls, audit logs to your monitoring.

Assure

Regulated pack, BNM or MAS gap assessment, ISO/IEC 42001 Statement of Applicability, red-team testing.

Managed

Monthly Vendor Annex updates, regulatory watch, quarterly reviews and tabletop exercises.

Contact: general@anchorsprint.com

