EVIDELIS

Preview the toolkit

See how Evidelis AI Governance turns policies, inventories, risk decisions and evidence into one operating system.

Evidelis AI Governance • Package v1.1

01 Control Center
A populated dashboard and system of record.

02 Approval
A pre-use AI tool approval form.

03 Risk
A six-dimension use-case risk assessment.

04 Implementation
A practical 30-day rollout path.

05 Routing
A decision tree for tools and use cases.

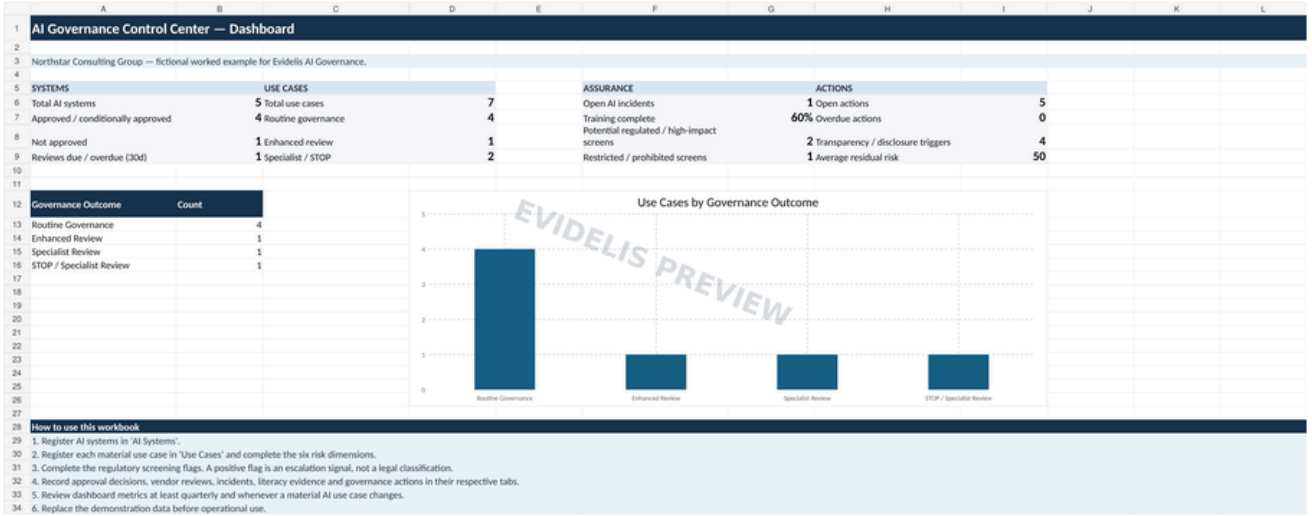
06 Worked example
A fully populated fictional SME example.

Preview only • Not legal advice • Full editable toolkit available at evidelis.com

SYSTEM OF RECORD

AI Governance Control Center

- Track AI systems, use cases, approvals, incidents, actions and review dates in one workbook.
- See governance outcomes and assurance indicators in a management dashboard.
- The preview uses fictional Northstar Consulting data.



AI Governance Control Center — Dashboard

Northstar Consulting Group — fictional worked example for Evidelis AI Governance.

SYSTEMS		USE CASES		ASSURANCE		ACTIONS	
Total AI systems	5	Total use cases	7	Open AI incidents	1	Open actions	5
Approved / conditionally approved	4	Routine governance	4	Training complete	60%	Overdue actions	0
Not approved	1	Enhanced review	1	Potential regulated / high-impact screens	2	Transparency / disclosure triggers	4
Reviews due / overdue (30d)	1	Specialist / STOP	2	Restricted / prohibited screens	1	Average residual risk	50

Governance Outcome	Count
Routine Governance	4
Enhanced Review	1
Specialist Review	1
STOP / Specialist Review	1

Use Cases by Governance Outcome

EVIDELIS PREVIEW

How to use this workbook

1. Register AI systems in 'AI Systems'.
2. Register each material use case in 'Use Cases' and complete the six risk dimensions.
3. Complete the regulatory screening flags. A positive flag is an escalation signal, not a legal classification.
4. Record approval decisions, vendor reviews, incidents, literacy evidence and governance actions in their respective tabs.
5. Review dashboard metrics at least quarterly and whenever a material AI use case changes.
6. Replace the demonstration data before operational use.

WHY THIS MATTERS

Shows the operational layer behind the policies - not just a folder of documents.

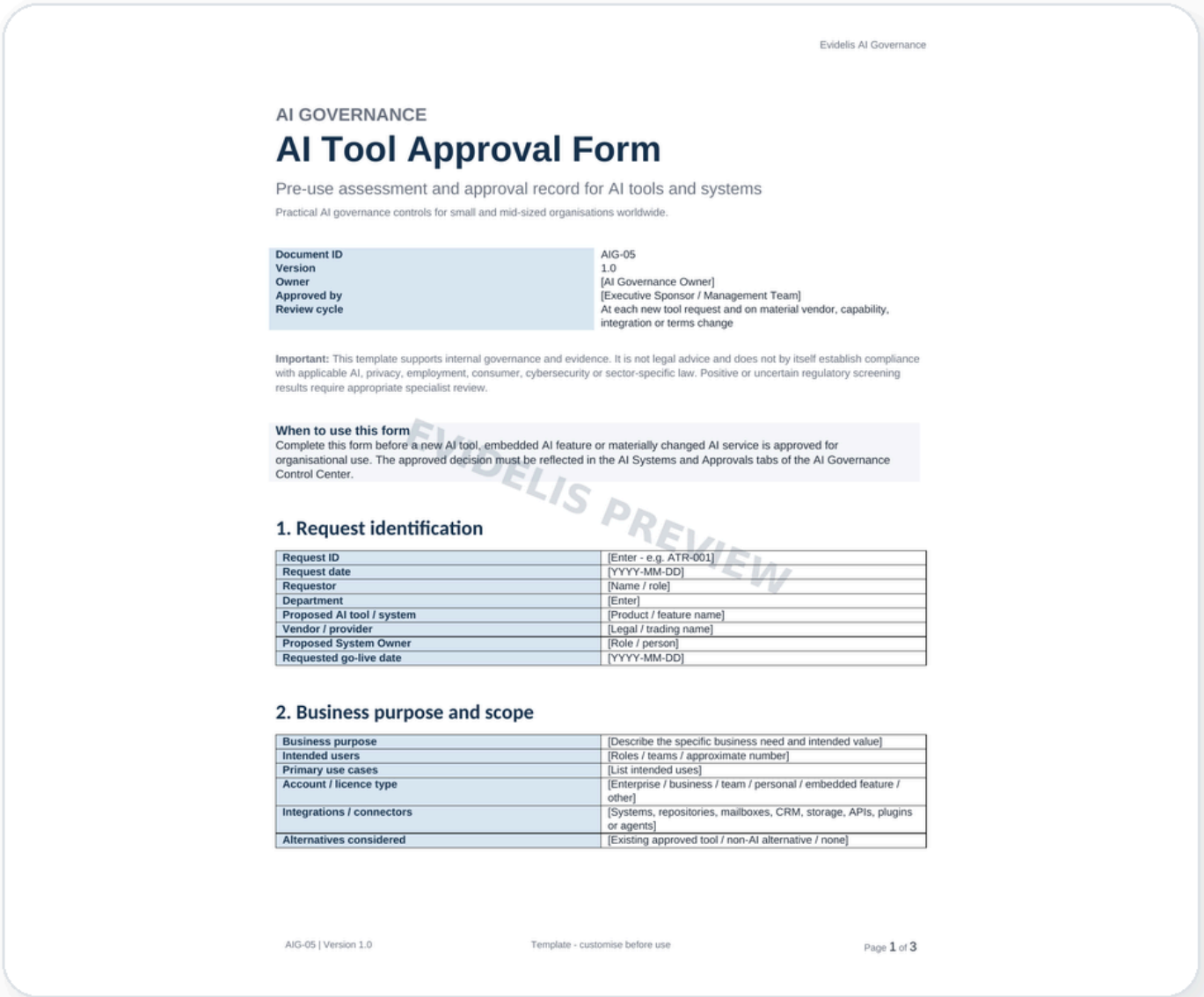
PRE-USE CONTROL

AI Tool Approval Form

- Capture business purpose, users, integrations, vendor details and requested go-live date.
- Create a repeatable approval record before a new AI tool or embedded feature enters organisational use.
- Designed to link decisions back into the Control Center.

WHY THIS MATTERS

Makes tool approval evidence consistent instead of relying on email threads or informal sign-off.



Evidelis AI Governance

AI GOVERNANCE

AI Tool Approval Form

Pre-use assessment and approval record for AI tools and systems

Practical AI governance controls for small and mid-sized organisations worldwide.

Document ID	AIG-05
Version	1.0
Owner	[AI Governance Owner]
Approved by	[Executive Sponsor / Management Team]
Review cycle	At each new tool request and on material vendor, capability, integration or terms change

Important: This template supports internal governance and evidence. It is not legal advice and does not by itself establish compliance with applicable AI, privacy, employment, consumer, cybersecurity or sector-specific law. Positive or uncertain regulatory screening results require appropriate specialist review.

When to use this form
Complete this form before a new AI tool, embedded AI feature or materially changed AI service is approved for organisational use. The approved decision must be reflected in the AI Systems and Approvals tabs of the AI Governance Control Center.

EVIDELIS PREVIEW

1. Request identification

Request ID	[Enter - e.g. ATR-001]
Request date	[YYYY-MM-DD]
Requestor	[Name / role]
Department	[Enter]
Proposed AI tool / system	[Product / feature name]
Vendor / provider	[Legal / trading name]
Proposed System Owner	[Role / person]
Requested go-live date	[YYYY-MM-DD]

2. Business purpose and scope

Business purpose	[Describe the specific business need and intended value]
Intended users	[Roles / teams / approximate number]
Primary use cases	[List intended uses]
Account / licence type	[Enterprise / business / team / personal / embedded feature / other]
Integrations / connectors	[Systems, repositories, mailboxes, CRM, storage, APIs, plugins or agents]
Alternatives considered	[Existing approved tool / non-AI alternative / none]

AIG-05 | Version 1.0 Template - customise before use Page 1 of 3

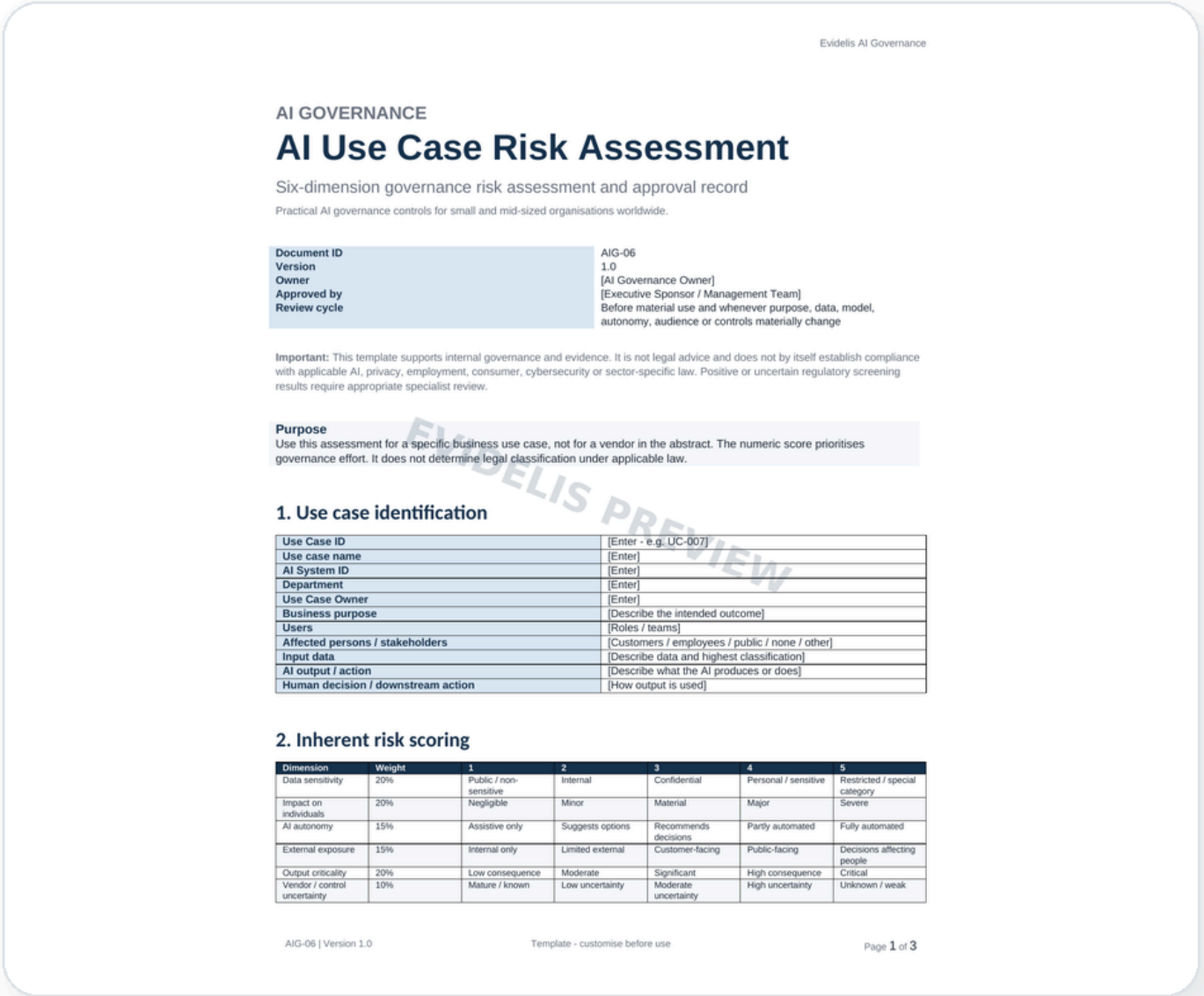
RISK DECISION

AI Use Case Risk Assessment

- Assess six governance dimensions including data sensitivity, impact, autonomy and output criticality.
- Prioritise governance effort without pretending an internal score is a legal classification.
- Connect risk outcome, controls, approval and review evidence.

WHY THIS MATTERS

Provides a repeatable decision method that can be adapted to the organisation’s own risk appetite.



AI GOVERNANCE

AI Use Case Risk Assessment

Six-dimension governance risk assessment and approval record

Practical AI governance controls for small and mid-sized organisations worldwide.

Document ID	AIG-06
Version	1.0
Owner	[AI Governance Owner]
Approved by	[Executive Sponsor / Management Team]
Review cycle	Before material use and whenever purpose, data, model, autonomy, audience or controls materially change

Important: This template supports internal governance and evidence. It is not legal advice and does not by itself establish compliance with applicable AI, privacy, employment, consumer, cybersecurity or sector-specific law. Positive or uncertain regulatory screening results require appropriate specialist review.

Purpose
Use this assessment for a specific business use case, not for a vendor in the abstract. The numeric score prioritises governance effort. It does not determine legal classification under applicable law.

EVIDELIS PREVIEW

1. Use case identification

Use Case ID	[Enter - e.g. UC-007]
Use case name	[Enter]
AI System ID	[Enter]
Department	[Enter]
Use Case Owner	[Enter]
Business purpose	[Describe the intended outcome]
Users	[Roles / teams]
Affected persons / stakeholders	[Customers / employees / public / none / other]
Input data	[Describe data and highest classification]
AI output / action	[Describe what the AI produces or does]
Human decision / downstream action	[How output is used]

2. Inherent risk scoring

Dimension	Weight	1	2	3	4	5
Data sensitivity	20%	Public / non-sensitive	Internal	Confidential	Personal / sensitive	Restricted / special category
Impact on individuals	20%	Negligible	Minor	Material	Major	Severe
AI autonomy	15%	Assistive only	Suggests options	Recommends decisions	Partly automated	Fully automated
External exposure	15%	Internal only	Limited external	Customer-facing	Public-facing	Decisions affecting people
Output criticality	20%	Low consequence	Moderate	Significant	High consequence	Critical
Vendor / control uncertainty	10%	Mature / known	Low uncertainty	Moderate uncertainty	High uncertainty	Unknown / weak

IMPLEMENTATION

30-Day Implementation Guide

- A day-by-day route from ownership and inventory to controls, training, incidents and management review.
- Defines tangible outputs and minimum go-live evidence.
- Built for organisations that need a governance baseline without a long transformation programme.

WHY THIS MATTERS

Converts governance from policy drafting into a practical implementation sequence.

Day	Theme	Primary action	Output / evidence
12	Design controls	Define required data, oversight and output-verification controls.	Control requirements.
13	Decisions	Approve, conditionally approve, pilot or reject assessed cases.	Decision log.
14	Control Center	Reconcile systems, use cases, vendors, approvals and review dates.	Current system of record.
15	Employee guidance	Issue Employee Quick Guide and approved-tool route.	Employee communication.
16	Manager guidance	Brief managers on approval, oversight and escalation.	Manager communication.
17	Literacy profiles	Adapt L0-L3 internal profiles to actual roles/exposure.	Role Matrix adapted.
18	Literacy plan	Assign initial modules and evidence method.	Implementation Tracker.
19	Incident route	Confirm incident intake and escalation channels.	Incident process live.
20	Tabletop	Run a short AI incident scenario with owner, IT/privacy and manager.	Lessons / actions.
21	Shadow AI check	Ask managers and key users for unregistered AI use.	Inventory gap list.
22	Material changes	Define what triggers reassessment: model, vendor, data, purpose, integration or autonomy.	Change triggers communicated.
23	Review cadence	Populate review calendar for systems, use cases, vendors and literacy.	Review Calendar current.
24	Evidence check	Confirm each approval has owner, date, conditions, evidence and next review.	Evidence gaps closed.
25	KPI baseline	Record initial dashboard metrics.	Baseline management metrics.
26	Open actions	Prioritise unresolved specialist reviews, vendor gaps and overdue literacy.	Action plan.
27	Management pre-read	Prepare dashboard, high-risk/escalated items, incidents and decisions needed.	Review pack.
28	Governance review	Conduct first management AI governance review.	AIG-16 approved record.
29	Remediate	Implement actions from management review and update registers.	Actions assigned.
30	Go-live checkpoint	Confirm minimum evidence, publish final rules and move to quarterly cadence.	Operating governance system.

EVIDELIS PREVIEW

3. Minimum go-live evidence

Control	Minimum evidence by Day 30	Owner
Accountability	Executive sponsor and AI Governance Owner named.	Management
Inventory	Known AI systems and material use cases registered.	AI Governance Owner

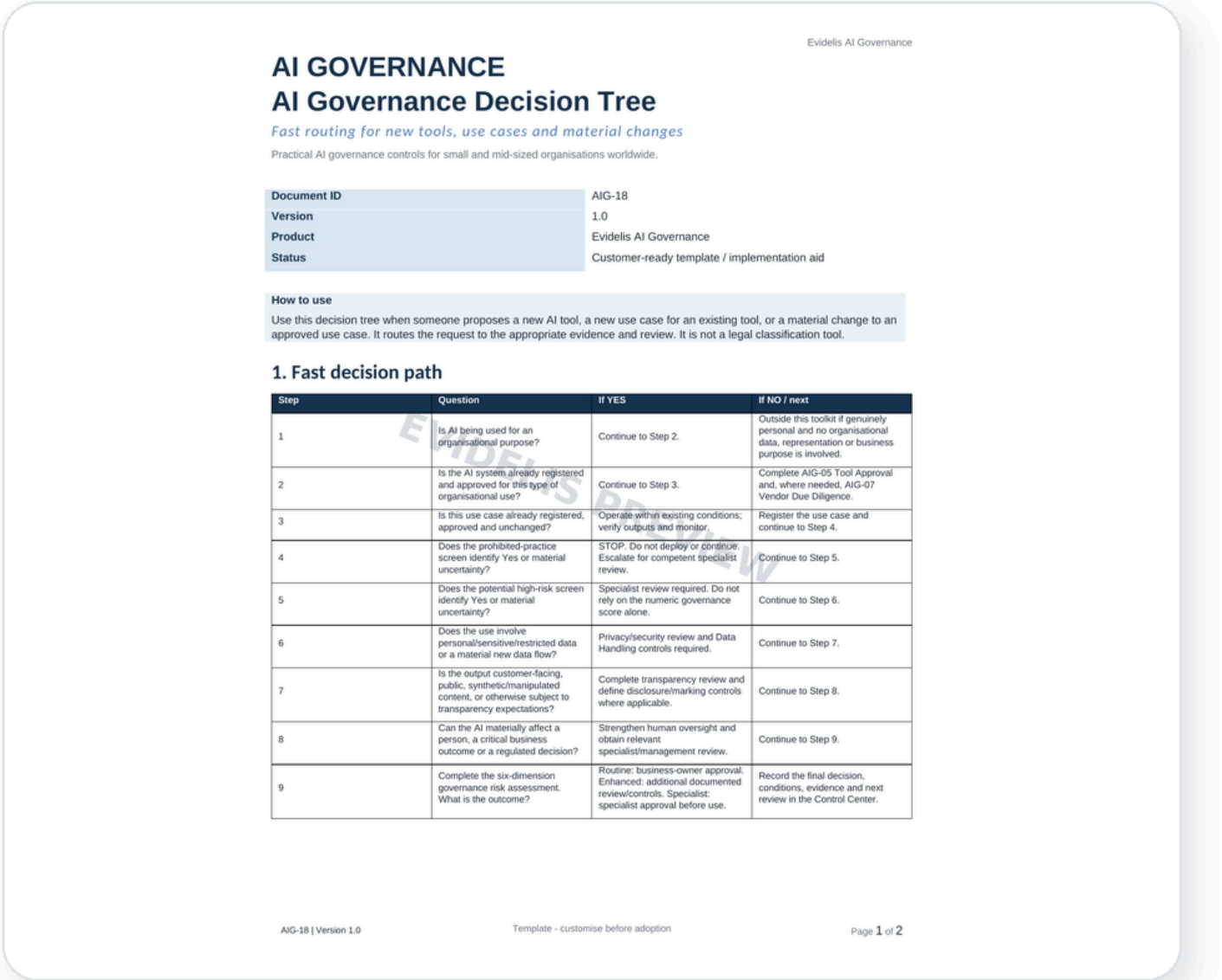
FAST ROUTING

AI Governance Decision Tree

- Route new AI tools, use cases and material changes to the right review path.
- Escalate data, transparency, high-impact and prohibited-practice signals.
- Keep business owners moving without bypassing specialist review where it is needed.

WHY THIS MATTERS

Gives managers a consistent first-line route for deciding what evidence and review a proposed AI use needs.



AI GOVERNANCE
AI Governance Decision Tree

Fast routing for new tools, use cases and material changes

Practical AI governance controls for small and mid-sized organisations worldwide.

Document ID	AIG-18
Version	1.0
Product	Evidelis AI Governance
Status	Customer-ready template / implementation aid

How to use

Use this decision tree when someone proposes a new AI tool, a new use case for an existing tool, or a material change to an approved use case. It routes the request to the appropriate evidence and review. It is not a legal classification tool.

1. Fast decision path

Step	Question	If YES	If NO / next
1	Is AI being used for an organisational purpose?	Continue to Step 2.	Outside this toolkit if genuinely personal and no organisational data, representation or business purpose is involved.
2	Is the AI system already registered and approved for this type of organisational use?	Continue to Step 3.	Complete AIG-05 Tool Approval and, where needed, AIG-07 Vendor Due Diligence.
3	Is this use case already registered, approved and unchanged?	Operate within existing conditions; verify outputs and monitor.	Register the use case and continue to Step 4.
4	Does the prohibited-practice screen identify Yes or material uncertainty?	STOP. Do not deploy or continue. Escalate for competent specialist review.	Continue to Step 5.
5	Does the potential high-risk screen identify Yes or material uncertainty?	Specialist review required. Do not rely on the numeric governance score alone.	Continue to Step 6.
6	Does the use involve personal/sensitive/restricted data or a material new data flow?	Privacy/security review and Data Handling controls required.	Continue to Step 7.
7	Is the output customer-facing, public, synthetic/manipulated content, or otherwise subject to transparency expectations?	Complete transparency review and define disclosure/marking controls where applicable.	Continue to Step 8.
8	Can the AI materially affect a person, a critical business outcome or a regulated decision?	Strengthen human oversight and obtain relevant specialist/management review.	Continue to Step 9.
9	Complete the six-dimension governance risk assessment. What is the outcome?	Routine: business-owner approval. Enhanced: additional documented review/controls. Specialist: specialist approval before use.	Record the final decision, conditions, evidence and next review in the Control Center.

EVIDELIS PREVIEW

PROOF IN USE

Northstar Worked Example

- A fictional 75-person consulting company with populated systems, use cases, decisions and controls.
- Shows routine, enhanced, specialist and STOP outcomes side by side.
- Lets buyers see how the same templates look when they are actually used.

WHY THIS MATTERS

The worked example reduces adoption friction by showing completed records and decision logic.



ID	System	Status	Approval	Primary data	Next review
SYS-003	Canva Magic Studio	Active	Conditionally Approved	Internal	2027-01-10
SYS-004	Example public meeting bot	Suspended	Not Approved	Personal / sensitive	2026-10-01
SYS-005	GitHub Copilot Business	Pilot	Conditionally Approved	Confidential	2026-11-20

4. Use-case portfolio

ID	Use case	Residual risk	Screening	Outcome	Decision
UC-001	Draft internal marketing copy	22	No special trigger	Routine Governance	Approved
UC-002	Summarise client project documents	29	Data / confidentiality controls	Routine Governance	Conditionally Approved
UC-003	Create customer-facing visual assets	34	Transparency trigger	Routine Governance	Conditionally Approved
UC-004	Rank job applicants	80	Potential high-risk indicator	Specialist Review	Not Approved
UC-005	Internal code completion	36	Security / IP controls	Routine Governance	Pilot
UC-006	Employee emotion scoring	100	Prohibited-practice screen = Yes	STOP / Specialist Review	Not Approved
UC-007	Draft client proposals with confidential bid data	50	External output + confidential data	Enhanced Review	Conditionally Approved

5. Walk-through A - routine governance

UC-001 uses an approved organisational account to create first drafts of non-sensitive marketing text. The business owner rates data sensitivity, individual impact and autonomy low. Human review occurs before use. The residual score is 22 and regulatory screening is negative. The Marketing Director approves the use with standard output-verification controls and annual review.

Control question	Northstar answer
Approved tool?	Yes - SYS-001.
Personal/restricted data?	No.
Customer/public output?	Campaign output may be external, but a human approves final material.
Human oversight	HO-1 / routine human review.
Evidence	Use-case record, approval, owner, review date.

6. Walk-through B - enhanced review

UC-007 prepares first drafts of client proposals using confidential bid information. The use remains assistive, but the output can influence a material commercial commitment and goes to an external client. Its residual governance score is 50. Northstar conditionally approves the use only for business accounts, requires a confidentiality check before prompting, prohibits restricted data, requires source verification and mandates manager review before release.

Control	Condition
Data	Confidential allowed only where contract and approved tool conditions permit; Restricted data excluded.

EVIDELIS PREVIEW