AUDIT - TRAIN
EDUCATE

Operational AI Governance Framework (OAGF)

POSITIVE CYBER SOLUTIONS LTD

Emma

AUDIT – TRAIN
—EDUCATE—

Operational AI Governance Framework (OAGF)

Published by Positive Cyber Solutions

Version	Date	Author	Change Summary	Approved by
1.0	10 Mar. 26	Emma Derbi	Initial release	Director
1.1	19 Mar. 26	Emma Derbi	Changes to Tier system and added template to Annex D	Director

Introduction: The Operational AI Governance Framework (OAGF) defines requirements for the safe and controlled use of third-party AI tools and AI-enabled SaaS features ("AI consumption"). It is intended for organisations of any size. This document contains the **normative requirements** for OAGF conformity. Examples include, rollout advice, staff awareness materials, and worked scenarios are provided separately in annexes.

Foreword

0. Overview

This clause summarises the purpose, structure, and normative language conventions of the OAGF.

Normative language: In this document, **shall** indicates a mandatory requirement; **shall not** indicates a prohibition; **should** indicates a recommended, optional practice; and **may** indicates permission.

Document conventions: Clauses 1–8 contain the requirements for conformity and are normative unless a clause is explicitly stated to be informative. Annexes provide supporting material; Annex A contains definitions used by this framework, and Annexes B–D provide guidance and examples that do not create additional requirements.

You are welcome to adopt, customise, and integrate this framework into your internal governance program. To support implementation, organisations often maintain additional artefacts such as policy documents, templates, registers, and assessment forms aligned to the OAGF evidence requirements (Clause 8) and the control catalogue (Clause 7). These can be created internally or obtained as companion implementation materials.

0.1 SME quick start (informative)

This quick start is designed for small and medium-sized organisations that want a practical minimum viable rollout. It is guidance only and does not add requirements beyond Clauses 1–8.

In week 1–2, aim to do the following:

- Assign the minimum roles (Clause 4): one person as AI Governance Owner and one person as Risk Review Authority/Tool Approval Authority (these may be the same person in a small company).
- Create a simple AI Tool Register (AI-02) and list what is already being used (include built-in "copilot" features and any public tools).
- Publish one-page staff rules using Annex B.2 as a starting point (AI-04), including your data red lines (AI-03) and how to report issues (AI-10).
- Pick one common use case (e.g., drafting internal documents) and classify it using 6.2; record the tier decision and rationale in the register.

Within 30 days, aim to have:

- All in-scope tools and use cases recorded in the register with owner, tier, allowed/prohibited data, and required review steps (AI-02, Clause 6).
- Basic supplier checks completed for any external AI tools used for work (Clause 8.2, AI-06).
- A simple approval note for each use case (AI-12) and a re-approval trigger list (AI-09) recorded in the register.
- An incident route and log (AI-10) and a basic shadow AI check (AI-15), even if it is only a quarterly staff attestation.

AUDIT – TRAIN
—EDUCATE—

Table of Contents

AUDIT – TRAIN
—EDUCATE—

1. Scope

This document specifies requirements for establishing, implementing, maintaining, and continually improving governance for the **use** of third-party AI tools and AI-enabled features ("AI consumption") within an organisation.

Framework type: The OAGF is a governance control framework for the safe use of third-party AI tools and AI-enabled SaaS features (AI consumption). It is **not** a full AI management system standard in the sense of ISO/IEC 42001. Organisations may implement the OAGF as a standalone governance framework or integrate it into an existing management system (e.g., AI, information security, or privacy governance), provided the requirements in this document are met.

- **Organisational scope:** This framework shall apply to all organisational units, staff, and third parties acting on behalf of the organisation who select, procure, configure, access, or use AI tools for organisational purposes.
- **Technology scope:** This framework shall apply to (a) standalone third-party AI services (including GenAI), (b) AI-enabled features embedded within SaaS and other business software, and (c) integrations, connectors, plugins, and extensions that enable AI processing of organisational data.
- **Exclusions:** This framework does not specify requirements for developing or training AI models in-house, unless the organisation explicitly extends its scope to cover AI development.

2. References

The following documents provide useful guidance and context for organisations implementing the OAGF. They are **informative** references and are not required for OAGF conformity:

- ISO/IEC 42001 (Artificial Intelligence — Management system)
- ISO/IEC 27001 (Information Security Management Systems)
- NIST AI Risk Management Framework (AI RMF)

If an organisation chooses to align its implementation to these references, it shall ensure that doing so does not override, reduce, or weaken any OAGF requirements in Clauses 1–8.

3. Terms and definitions

For the purposes of this document, the terms and definitions given in **Annex A: Terms and definitions** apply.

AUDIT – TRAIN
—EDUCATE—

4. Governance principles and structure

4.1 Governance principles

- The organisation shall assign accountability for AI tool use within scope, including approval authority and escalation routes.
- The organisation shall maintain transparency of AI tool use by maintaining an up-to-date AI Tool Register (AI-02 in Clause 7).
- The organisation shall apply proportionate, risk-based governance to AI tool use cases (Clause 6) and shall not deploy use cases without the required evidence (Clause 8).
- The organisation shall protect organisational and personal data by defining and enforcing data input, retention, and transfer controls (AI-03 in Clause 7).
- The organisation shall implement human oversight for AI outputs where required (AI-05 in Clause 7), particularly for external communications and consequential decisions.
- The organisation shall ensure supplier responsibility and assurance through due diligence and contractual safeguards prior to approval (AI-06 in Clause 7).
- The organisation shall monitor, learn from, and respond to incidents and near-misses involving AI tool use (AI-08 and AI-10 in Clause 7), and shall continually improve controls over time.

4.2 Governance structure

The organisation shall establish, document, and maintain a governance structure for AI tool use that defines accountability, approval authority, and escalation routes. Where roles are combined, the organisation shall ensure responsibilities remain assigned and auditable.

SME note (informative): In a small organisation, the AI Governance Owner, Risk Review Authority, and Tool Approval Authority may be the same person, provided decisions are recorded and conflicts of interest are managed (e.g., obtaining a second-person review for higher-risk approvals). The “Tool Administrator” role may be your IT provider or the person who manages Microsoft 365/Google Workspace/admin consoles.

Role	Minimum responsibilities (Normative)
AI Governance Owner	• Shall approve the AI governance policy and any material changes. • Shall define and approve the organisation’s risk appetite for AI tool use (including prohibited uses and data red lines). • Shall act as escalation authority for high-risk approvals and significant incidents.

Risk Review Authority	• Shall ensure each AI tool use case is risk classified (Clause 6) and that required controls and evidence are defined. • Shall maintain the AI Tool Register (AI-02) or assign an accountable owner to do so. • Shall ensure incidents are recorded, investigated, and reported (AI-10).
Tool Approval Authority	• Shall approve (or reject) tools and use cases for go-live based on the required evidence set (Clause 8). • Shall ensure supplier due diligence is completed for tools prior to approval (AI-06). • Shall ensure configuration, access control, and monitoring requirements are defined as approval conditions where applicable (AI-07, AI-09).
Use Case Owner	• Shall define the approved purpose, boundaries, and required human oversight for the use case (AI-05). • Shall ensure data rules are applied in practice and re-approval is requested when conditions change (AI-03, AI-09).
Tool Administrator (where applicable)	• Shall configure and operate the tool in line with approved settings, including access control and logging where available (AI-07). • Shall support investigations by enabling and retaining logs where feasible (AI-10).

5. AI tool lifecycle requirements

The organisation shall govern each AI tool use case through a documented lifecycle consisting of: (a) discovery and scoping, (b) risk assessment, (c) data handling controls, (d) supplier due diligence, (e) configuration and access control, (f) approval and deployment, (g) monitoring and change control, and (h) retirement/offboarding. The organisation shall not deploy an AI tool use case to production use until the applicable lifecycle stages are completed and evidence is recorded (Clause 8). For Tier 2 and higher use cases, the organisation shall complete an AI Use Impact Assessment (AUIA) prior to approval and deployment (see AI-13 in Clause 7). For Tier 1–2 use cases, the organisation may capture lifecycle evidence in the AI Tool Register (AI-02) and a simple approval record (AI-12), consistent with the SME baseline in Clause 8.2.

6. Risk classification model

The organisation shall classify each AI tool use case using documented criteria that consider, as a minimum: (a) data sensitivity, (b) automation level, (c) decision impact, and (d) regulatory and contractual exposure. The organisation shall record the classification decision and rationale in the AI Tool Register (see AI-02 in Clause 7) and/or in another documented assessment record retained in accordance with AI-12 (in Clause 7) and the evidence requirements in Clause 8.

Criterion	Minimum requirement
Data sensitivity	The organisation shall determine whether prompts, uploads, logs, and outputs contain public, internal, personal, confidential, or restricted data, and apply corresponding controls.
Automation level	The organisation shall determine whether AI outputs are (a) advisory/draft only, (b) used with mandatory human review, or (c) used to trigger actions automatically.
Decision impact	The organisation shall determine whether outputs influence decisions that have material effect on customers, staff, or the public, and define human oversight and contestability controls accordingly.
Regulatory & contractual exposure	The organisation shall identify applicable laws, sector rules, and client contract obligations (including cross-border transfer conditions) and incorporate them into the approval and monitoring requirements.

6.1 Tier-to-control mapping

6.2 How to determine the tier

The tier is determined by applying the criteria in Clause 6 to the specific AI tool use case (not the tool in general). The organisation shall document the tier decision and rationale as part of the approval record (AI-12) and/or in the AI Tool Register (AI-02).

1. **Confirm the use case boundaries.** Define the purpose, intended users, target audience (internal vs external), and whether outputs will be used to make or influence decisions.
2. **Assess data sensitivity.** Identify the highest data category that could be entered, uploaded, retained, or produced (including prompts, attachments, logs, and outputs). If personal, confidential, or restricted data is involved, the organisation shall consider at least Tier 2 (and Tier 3 where impact is material).
3. **Assess automation level and decision impact.** Determine whether outputs are (a) draft/advisory only, (b) used with mandatory human review, or (c) used to trigger actions automatically. Where outputs are customer-facing, safety/security-significant, or used for consequential decisions, the organisation shall consider Tier 3.

4. **Assess regulatory and contractual exposure.** Identify whether the use case is regulated (or contractually controlled), includes cross-border transfer constraints, or creates notification/audit obligations. If the EU AI Act high-risk categories apply (or equivalent contractual requirements exist), Tier 4 overlay obligations shall be applied in addition to the base tier.
5. **Select the highest applicable tier.** If multiple criteria point to different tiers, the organisation shall adopt the highest tier indicated. Where the organisation is uncertain between two tiers, it should classify up and reduce later if evidence supports it.

Quick guide (informative): Tier 1 is typically internal productivity support using public/internal data with no material impact. Tier 2 typically includes personal data and/or outputs that influence work beyond simple drafting. Tier 3 typically includes customer/individual material impact, regulated contexts, or reliance on outputs for consequential decisions. Tier 4 is applied when EU AI Act high-risk (or equivalent contractual) obligations apply.

The organisation shall apply additional controls and evidence requirements as the risk tier increases. As a minimum, Tier 1 use cases shall meet the Tier 1 requirements below; Tier 2 use cases shall meet Tier 1 and Tier 2 requirements; and Tier 3 use cases shall meet Tier 1, Tier 2, and Tier 3 requirements. Tier 4 is an overlay that shall be applied in addition to Tier 3 where applicable (see Annex C) and shall not reduce any Tier 1–3 requirements.

Tier	Mandatory controls (Clause 7)	Minimum additional requirements
Tier 1 (Low)	AI-01, AI-02, AI-03, AI-04, AI-12, AI-15	• The use case shall be recorded in the AI Tool Register with owner, purpose, and data rules. • Outputs shall be treated as draft and shall not be published externally without review, where applicable.
Tier 2 (Medium)	Tier 1 + AI-05, AI-06, AI-07, AI-08, AI-09, AI-10, AI-13, AI-15, AI-16	• The organisation shall complete and approve an AI Use Impact Assessment **(AUIA)** for the use case prior to approval and deployment (AI-13). • Human review shall be implemented for outputs used externally or that influence decisions. • The organisation shall define re-approval triggers and an incident route for the use case.

Tier 3 (High)	Tier 2 + AI-14	• A documented monitoring plan shall be defined and followed (see AI-08), including frequency, measures, and review owner. • Human review shall be mandatory prior to external use and for any consequential decision outputs. • Approval shall be granted by the Tool Approval Authority, with escalation to the AI Governance Owner where the risk appetite boundary is exceeded.
Tier 4 (Overlay)	Tier 3 + additional EU/contractual obligations	• The organisation shall identify and document applicable high-risk overlay obligations and implement additional evidence and monitoring as required. • The organisation shall retain evidence sufficient to demonstrate conformity with Tier 3 and overlay requirements (Clause 8).

The organisation shall retain evidence demonstrating implementation of the applicable tier requirements in accordance with Clause 8, including maintaining an auditable record of approvals, monitoring, incidents, and changes (see AI-08, AI-09, AI-10, and AI-12 in Clause 7).

7. Control catalogue

The organisation shall implement the controls in this clause. Controls are written to be auditable. Controls are grouped into domains to support implementation and audit planning. Where a control is not applicable due to the organisation's defined scope, the organisation shall document the justification.

7.1 Control domains and objectives

Domain	**Control objective**
Governance	Establish accountability, policy, decision rights, and a single source of truth for approved AI tools and use cases.
Data	Ensure organisational and personal data is handled safely when entered into AI tools, including retention and transfer considerations.

Supplier	Select and manage third-party AI suppliers with appropriate due diligence, contractual safeguards, and assurance evidence proportionate to risk.
Operational	Operate AI tools safely through configuration, access controls, change control, approved use enforcement, and detection of shadow AI.
Assurance	Provide confidence that controls are implemented and effective through monitoring, incident management, competence, record keeping, and periodic review.

7.2 Governance controls

AI-01 AI governance policy

Control statement	The organisation shall establish, approve, communicate, and maintain an AI governance policy applicable to AI tool use within the defined scope.
Purpose	To define organisational boundaries, responsibilities, and minimum rules for safe AI tool use.
Minimum implementation expectations	• The policy shall define scope, roles, prohibited uses, data rules, human oversight expectations, and incident reporting routes. • The policy shall be reviewed at least annually and after significant incidents or material change.
Example evidence	Approved AI policy document; review logs; communications record.

AI-02 AI Tool Register

Control statement	The organisation shall maintain a central AI Tool Register of approved AI tools and AI tool use cases within scope.
Purpose	To provide a single source of truth for what AI is approved, who owns it, what data is permitted, and what evidence exists.
Minimum implementation expectations	• The register shall include: tool/supplier, use case(s), owners, risk classification, allowed/prohibited data, approval status, key configuration conditions, review cadence, and links to evidence. • The register shall be updated prior to go-live and upon material change.
Example evidence	AI Tool Register (spreadsheet, GRC tool, or ticketing system extract).

7.3 Data controls

AI-03 Data input, retention, and transfer controls

Control statement	The organisation shall define and enforce rules for what data may be entered, uploaded, retained, and transferred when using AI tools, including prompts, attachments, logs, and outputs.
Purpose	To prevent leakage or inappropriate processing of personal, confidential, or restricted data via AI tools.
Minimum implementation expectations	• Allowed/prohibited data types shall be defined per use case and recorded in the AI Tool Register. • The organisation shall define retention expectations for prompts and outputs (where the tool retains them) and ensure they align with records management and privacy requirements. • The organisation shall identify and control cross-border transfers of personal or confidential data via AI tools, including ensuring appropriate transfer mechanisms where required.
Example evidence	Data input rules; retention decision; transfer assessment note; AI Tool Register fields completed.

7.4 Operational controls

AI-04 Acceptable and prohibited use

Control statement	The organisation shall define acceptable use and prohibited use of AI tools and shall ensure users comply with these rules.
Purpose	To set clear behavioural boundaries and reduce shadow AI and misuse.
Minimum implementation expectations	• Users shall use approved tools only for organisational work. • Users shall not upload restricted data into unapproved/public AI services. • AI-generated outputs used externally or for consequential decisions shall be subject to human review as defined for the use case.
Example evidence	Acceptable use policy; prohibited use list; user acknowledgement record.

AI-05 Human oversight and review

Control statement	The organisation shall define and implement human oversight controls for AI tool outputs, proportionate to the risk classification and decision impact.
Purpose	To ensure AI outputs are not relied upon inappropriately and that humans retain meaningful control.
Minimum implementation expectations	• The organisation shall specify which outputs require review, who can approve them, and escalation criteria. • For consequential decisions or regulated contexts, AI outputs shall not be the sole basis for decisions unless explicitly approved and controlled.
Example evidence	Defined review workflow; approval thresholds; escalation criteria; sample-check records (where used) (AI-16).

7.5 Supplier controls

AI-06 Supplier due diligence and contractual safeguards

Control statement	The organisation shall complete proportionate supplier due diligence prior to approving an AI tool and shall ensure contractual safeguards are in place for data use, confidentiality, security, and incident notification.
Purpose	To ensure third-party tools meet organisational security, privacy, and operational requirements and that risk is contractually managed.
Minimum implementation expectations	• The organisation shall assess supplier data handling, including whether prompts/outputs are used for model training, retention periods, data location, and sub-processors. • The organisation shall ensure contract terms cover confidentiality, permitted data use, incident notification timeframes, and exit/portability where applicable. • Where applicable and where assurance evidence is available, the organisation shall obtain appropriate assurance evidence (e.g., ISO 27001 and/or SOC 2) and shall define audit rights or equivalent assurance mechanisms. • The organisation shall define expectations for liability and responsibility allocation appropriate to the use case risk. • For Tier 1–2 use cases (and for smaller organisations), supplier due diligence may be satisfied through a documented set of basic supplier checks (as defined in

	Clause 8.2), provided the organisation's data rules and risk appetite are met.
Example evidence	Supplier due diligence record; contract clause checklist; security assurance report; sub-processor list.

AI-07 Configuration and access control

Control statement	The organisation shall configure AI tools to enforce approved use cases, including access control, integration restrictions, and security settings aligned to the risk classification.
Purpose	To reduce the likelihood of policy breaches and data exfiltration through misconfiguration.
Minimum implementation expectations	• The organisation shall implement role-based access control and least privilege for users and administrators where supported. • The organisation shall restrict plugins, connectors, or integrations to approved ones where supported. • The organisation shall document key configuration settings for each approved use case.
Example evidence	Configuration record; access group list; integration allow-list.

7.6 Assurance controls

Domain mapping (informative): Governance (AI-01, AI-02); Data (AI-03, AI-13); Supplier (AI-06); Operational (AI-04, AI-05, AI-07, AI-09, AI-15); Assurance (AI-08, AI-10, AI-11, AI-12, AI-14, AI-16).

AI-08 Logging, monitoring, and traceability

Control statement	The organisation shall monitor AI tool use cases and maintain appropriate logging and traceability to support assurance and incident investigation, proportionate to risk and tool capabilities.
Purpose	To detect misuse, manage drift and supplier change, and maintain an audit trail.
Minimum implementation expectations	• For each use case, the organisation shall define monitoring frequency, measures, and re-approval triggers. • Where the tool provides logs, the organisation shall enable and retain them for a defined period consistent with incident and compliance needs. • Where relevant, the organisation shall define what traceability is required for outputs (e.g., prompt templates, version/feature changes, and approval conditions).

Example evidence	Monitoring plan; log retention setting; periodic review record; change alerts captured.

AI-09 Change control and re-approval

Control statement	The organisation shall control changes to approved AI tools and use cases and shall require re-approval when changes could materially affect risk.
Purpose	To ensure new features, integrations, data types, or usage expansion do not bypass governance.
Minimum implementation expectations	• Re-approval shall be required before introducing new use cases, new data categories, customer-facing automation, or new integrations/connectors. • The organisation shall monitor supplier changes (features/terms/data locations) and assess whether re-approval is required.
Example evidence	Change log; re-approval record; updated register entry; supplier change notice.

AI-10 Incident reporting and investigation

Control statement	The organisation shall define and operate an incident process for AI tool misuse, data leakage, unsafe outputs, and other AI-related events, including investigation and corrective actions.
Purpose	To ensure timely containment, learning, and compliance with notification duties.
Minimum implementation expectations	• Incidents shall be recorded in an Incident Log with date/time, description, potential data affected, and actions taken. • The organisation shall define escalation routes for significant incidents and shall consider regulatory/client notification obligations. • Corrective actions shall be tracked to completion and shall feed continual improvement.
Example evidence	Incident Log; investigation notes; corrective action tracker.

AI-11 Competence and awareness

Control statement	The organisation shall ensure personnel using or overseeing AI tools are competent for their role and aware of the organisation's AI use rules, including data handling and escalation routes.
Purpose	To reduce human error and shadow AI by ensuring users understand rules and limits.

Minimum implementation expectations	• The organisation shall communicate acceptable use and data rules to relevant personnel. • The organisation shall ensure relevant roles understand incident reporting requirements.
Example evidence	Training/briefing record; policy acknowledgement; role onboarding checklist.

AI-12 Documented information and auditability

Control statement	The organisation shall maintain documented information necessary to demonstrate that the OAGF controls are implemented and effective within the defined scope.
Purpose	To enable assurance, audits, and consistent governance decisions.
Minimum implementation expectations	• The organisation shall maintain evidence required for tool approvals, monitoring, incidents, and change control. • Documented information shall be retained, protected from unauthorised change, and retrievable.
Example evidence	Evidence set defined in Clause 8; version control records; audit trail of approvals.

AI-13 AI Use Impact Assessment

Control statement	The organisation shall complete and document an AI Use Impact Assessment for each AI tool use case classified as Tier 2 or higher prior to approval and deployment.
Purpose	To ensure risks relating to data use, automation, decision impact, and regulatory exposure are identified and controlled before operational deployment.
Minimum implementation expectations	The assessment shall consider at minimum: • Data categories processed • Automation level • Decision impact • Affected individuals or customers • Supplier data handling • Required human oversight • Monitoring requirements • Regulatory obligations

	The assessment shall be approved by the Risk Review Authority prior to deployment.
Example evidence	Completed AUIA form; approval record; linked entry in the AI Tool Register.

AI-14 Periodic governance review

Control statement	The organisation shall perform periodic governance reviews of AI tool use within scope to confirm continued suitability, effectiveness of controls, and completion of required corrective actions.
Purpose	To ensure governance remains current as tools, suppliers, data, and usage patterns change.
Minimum implementation expectations	• The organisation shall define a review cadence (at least annually; more frequent for Tier 3) and a review owner. • The review shall cover: register accuracy (AI-02), incidents/near-misses (AI-10), monitoring results (AI-08), supplier changes (AI-06/AI-09), and completion/quality of required assessments and records (including AI Use Impact Assessments (AI-13) where applicable). • Actions from the review shall be recorded and tracked to completion.
Example evidence	Governance review minutes/record; action log; updated AI Tool Register; management reporting pack (where used).

AI-15 Shadow AI detection and response

Control statement	The organisation shall implement proportionate measures to detect and address unapproved AI tool use (“shadow AI”) within scope.
Purpose	To reduce uncontrolled data exposure and ensure AI use is governed and recorded.
Minimum implementation expectations	• The organisation shall define what constitutes unapproved AI tool use and the escalation route (AI-04, AI-10). • As a minimum, the organisation shall perform periodic checks to identify shadow AI (e.g., staff attestation/survey, review of browser extensions/plugins where managed, and/or procurement/expense review). • Where technical controls are available, the organisation should consider implementing monitoring or blocking controls (e.g., DLP, web filtering, CASB) proportionate to risk.

	• Identified shadow AI instances shall be recorded, assessed for data exposure, and either approved through the lifecycle (Clause 5) or prohibited and remediated.
Example evidence	Shadow AI check record (survey/attestation results); list of identified tools; remediation actions; approvals or prohibitions recorded in the AI Tool Register.

AI-16 Output validation and quality assurance

Control statement	The organisation shall implement proportionate validation and quality assurance of AI outputs before they are used, relied upon, or communicated, in line with the use case risk tier and intended audience.
Purpose	To reduce the likelihood of incorrect, misleading, unsafe, or non-compliant AI outputs being acted on or shared externally.
Minimum implementation expectations	• For Tier 1 use cases, users shall treat outputs as draft and perform basic sense-checking before use. • For Tier 2–3 use cases, the organisation shall define required validation steps for the use case (e.g., fact checking, data reconciliation, policy/compliance review, and/or second-person review) and ensure they are performed prior to external use or consequential decisions. • Where outputs contain numbers, factual claims, legal/contractual statements, or customer-specific commitments, validation shall include checking against authoritative sources. • Validation requirements and responsibilities shall be recorded in the AI Tool Register entry or associated use case documentation. • Where systematic errors are detected, the organisation shall update prompts/templates, user guidance, or approval conditions, and consider re-approval triggers (AI-09).
Example evidence	Validation checklist or guidance; sample-check log; peer review/approval record; documented prompt templates; QA sign-off for customer-facing content.

8. Conformity and evidence requirements

An organisation may claim conformity with this framework only if it can demonstrate that all applicable requirements in Clauses 1–7 are implemented within the defined scope and that the evidence in this clause is maintained and retrievable.

8.1 Minimum conformity criteria

- A documented scope (Clause 1) and governance model with accountable roles (Clause 4).
- A maintained AI Tool Register (AI-02) covering all in-scope approved tools and use cases.
- Documented risk classification for each use case, including rationale (Clause 6).
- Implemented data input/retention/transfer rules for each use case (AI-03) and acceptable/prohibited use rules (AI-04).
- Completed supplier due diligence prior to approval (AI-06) and documented key contractual safeguards.
- Defined and implemented human oversight for outputs where required (AI-05).
- Defined monitoring and change control (AI-08, AI-09) and an incident process with an incident log (AI-10). Where AI outputs are used externally or relied upon for consequential decisions, proportionate output validation and quality assurance shall be implemented (AI-16).

8.2 SME baseline (minimum viable controls)

Where the organisation is small and roles are combined, the organisation shall, as a minimum, implement AI-02, AI-03, AI-04, AI-05, AI-06 (basic supplier checks), AI-10, and AI-15 (basic shadow AI checks), and shall document role assignment for the governance model (Clause 4). For SMEs operating Tier 1–2 use cases, the organisation shall be permitted to meet lifecycle evidence requirements by capturing the required information directly in the AI Tool Register and a simple approval record, rather than producing separate documents for each stage.

- **Basic supplier checks (minimum):** the organisation shall confirm (a) whether prompts/outputs are used for training, (b) default retention period and how to delete data where applicable, (c) data location/cross-border transfer position for personal/confidential data, (d) account/admin controls available (e.g., SSO/MFA/roles), and (e) how incidents are notified and supported.
- **Minimum lifecycle documentation (Tier 1–2):** the organisation shall record purpose, owner, tier, allowed/prohibited data, approval decision, required human review, and re-approval triggers in the AI Tool Register (AI-02) and retain a basic approval note (AI-12).
- **When separate documentation is required:** if the organisation operates Tier 3 use cases, it shall maintain a monitoring plan (AI-08) and periodic governance review records (AI-14) as separate evidence where appropriate.

8.3 Assurance readiness (optional best practice)

Optional (recommendation): The OAGF does not define a formal certification scheme, audit criteria, or audit scope. However, organisations seeking internal assurance, client assurance,

or third-party assessment preparedness should be able to provide, on request, an evidence pack for a sample of use cases across risk tiers. As a minimum, this pack should include approvals, risk classification rationale, supplier due diligence, configuration record, monitoring results, and incident records.

AUDIT – TRAIN
—EDUCATE—

Annex A: Terms and definitions

A. Terms and definitions

This glossary defines key terms used in this framework. Definitions are written for business users and are intended to support consistent understanding and implementation.

Term	Definition
AI (Artificial Intelligence)	A broad term for computer systems that perform tasks that normally require human judgement, such as generating text, summarising information, recognising patterns, or making recommendations.
AI tool	Any software, service, or feature that uses AI to generate, analyse, transform, or recommend content and may process organisational data (including GenAI assistants, transcription, summarisation, and “copilot” features).
AI tool use case	A defined way an AI tool is used in the organisation (who uses it, for what purpose, with what data, and with what controls). The same tool can have multiple use cases with different risk levels.
AI Tool Profile	A short description of an AI tool and its approved configuration and limits, including supplier, key settings, data handling expectations, intended use, known limitations, and required controls.
AI Tool Register	A central list of approved AI tools and AI tool use cases, including owners, risk tier, data rules, approvals, and links to required records.
AI Tool Use Request	A simple request that explains why an AI tool will be used, what success looks like, who will use it, what data is involved, and what boundaries apply. It is the starting point for approval and governance.
AI Use Impact Assessment (AUIA)	A proportionate assessment of risks, potential harms, and required controls for an AI tool use case. It typically covers who may be affected, what data is used, what could go wrong, required human review/oversight, and the monitoring plan.
AI-enabled feature	An AI capability built into an existing product (e.g., email, document, CRM, or website tools) rather than a standalone AI product. It may still process organisational data and therefore must be governed.
Audit trail	Records that show what decisions were made, by whom, and why (e.g., approvals, risk assessments, changes, incidents, and monitoring results). An audit trail supports accountability and investigations.
Confidential data	Information the organisation treats as sensitive and not for public disclosure (e.g., contracts, pricing, internal strategy, client

	information). The exact definition should align to the organisation's data classification scheme.
Data at rest	Data stored somewhere (e.g., within the AI tool, logs, the supplier's systems, or the organisation's storage locations).
Data being processed	Data actively used by a system to produce an output (e.g., the AI tool analysing text provided by the user to generate a response).
Data classification	A method for labelling data by sensitivity (e.g., public, internal, confidential, restricted) to determine how it can be stored, shared, and processed.
Data in transit	Data being transmitted from one system to another (e.g., when a user sends a prompt or uploads a document to an AI tool).
Data loss prevention (DLP)	Controls that detect or prevent sensitive data from being shared or transferred inappropriately (e.g., blocking certain data types from being pasted into tools or warning users before sending).
DPIA (Data Protection Impact Assessment)	A structured assessment used under UK GDPR when processing is likely to result in high risk to individuals. In this framework it is used as a trigger-based control for higher-risk AI tool use involving personal data.
EU AI Act high-risk overlay	Additional requirements applied when the EU AI Act is in scope and the relevant use is considered high risk (or where an organisation agrees equivalent requirements contractually). This overlay adds extra documentation, monitoring, and role clarity as needed.
Generative AI (GenAI)	AI that generates new content such as text, images, code, audio, or summaries. GenAI can produce confident sounding but incorrect content ("hallucinations"), so review and controls are important.
Governance & Risk Committee (AI Use Oversight)	The senior group that sets risk appetite, approves policy, and acts as an escalation route for higher-risk AI tool decisions and incidents.
Human oversight	Ongoing supervision to ensure an AI tool is used safely (e.g., setting rules, monitoring outcomes, auditing usage, and making changes when risks emerge). Oversight is an operating model responsibility, not a one-off check.
Human review	A person checking an AI output before it is used, relied upon, or shared (especially externally). Human review is commonly required for higher-risk communications or decisions.
Incident	An event where AI tool use causes or could cause harm, policy breach, data leakage, security issues, or significant errors. Incidents shall be logged and managed in accordance with AI-10 (in Clause 7) and retained as evidence per Clause 8.

Information Security Lead	The role responsible for security reviews and ensuring AI tool use is protected from misuse and data leakage, including incident response linkage.
IT Service Owner / System Administrator	The role responsible for configuring and operating approved AI tools safely (e.g., access control, logging/retention settings, integrations, and technical safeguards where available).
LLM (Large Language Model)	A type of model often used in Generative AI that can generate text and respond to prompts based on patterns learned from large amounts of data. LLM outputs can be incorrect or misleading, so organisations commonly implement verification and review controls for relevant use cases.
Near-miss	An event that could have caused harm or a breach but was prevented in time (e.g., sensitive data was about to be pasted into an unapproved tool but was stopped). Near-misses should still be recorded to improve controls.
Personal data	Information relating to an identified or identifiable individual (e.g., names, contact details, ID numbers, customer references linked to a person). Definitions and handling requirements come from UK GDPR.
Privacy Assessment	A proportionate check of privacy implications for an AI tool use case (e.g., what personal data is involved, what notices are needed, retention, access controls). It may trigger a DPIA where required.
Prohibited use	Clear “red lines” for staff, describing what must not be done with AI tools (e.g., uploading restricted data to public tools, impersonation/deception, bypassing controls). See AI-04 (in Clause 7) and supporting staff guidance in Annex B.
Re-approval trigger	A condition that requires the organisation to revisit approval and controls (e.g., new use case, new data type, major supplier change, repeated incidents, moving to external/customer-facing use).
Restricted data	The most sensitive category of organisational data (e.g., credentials, special category data, security keys, regulated data, or information that would cause serious harm if disclosed). The exact definition should align to the organisation’s data classification scheme.
Risk & Compliance Lead	The role coordinating day-to-day governance for AI tool use, including the AI Tool Register, approvals workflow, completion of required records, and reporting on KPIs/incidents.
Risk tier (Tier 1–4)	A simple categorisation of how risky an AI tool use case is, used to decide what controls and records are required. Tier 4 indicates an EU AI Act high-risk overlay may apply.

Service Owner / Process Owner	The business owner accountable for how a specific AI tool use case is used within a service, process, or team, including boundaries, training, review steps, and corrective actions.
Shadow AI	Use of AI tools or AI-enabled features that have not been approved, assessed, or configured under this framework (including personal accounts, public tools, unapproved extensions, or unapproved SaaS AI features). Shadow AI increases the risk of data leakage, loss of audit trail, and non-compliance.
Special category data	A sensitive category of personal data under UK GDPR (e.g., health information, biometric data used for identification, religious beliefs). Special category data requires extra protections and is typically restricted from most AI tool use cases.
Supplier due diligence	Checks performed before approving an AI tool supplier, including licensing/terms, data handling, security assurance, admin controls, incident notification, and exit/portability.
Tool retirement/offboarding	The controlled process of switching off a tool or use case, removing access, handling data retention/deletion, archiving required records, and updating the AI Tool Register. See lifecycle requirements in Clause 5 and change/records controls AI-09 and AI-12 (in Clause 7).
UK GDPR	The UK General Data Protection Regulation, which sets requirements for processing personal data in the UK (including transparency, security, minimisation, and rights of individuals).
Data Protection Officer / Privacy Lead	The role responsible for privacy compliance and determining when privacy assessments or DPIAs are required for AI tool use cases involving personal data.

Annex B: Implementation guidance and examples

Annex B.0 Background and context

Artificial Intelligence (AI) presents both transformative opportunities and meaningful risks. Organisations benefit from clear and practical governance to reduce the likelihood of data leakage, misuse, over-reliance on outputs, and regulatory or contractual breaches.

This framework is UK-focused by default (e.g., UK GDPR, Data Protection Act 2018, and UK regulatory expectations such as ICO guidance). Where organisations operate in, or provide services into, the EU, additional obligations may apply (including under the EU AI Act). Organisations may therefore adopt a “UK baseline + EU overlay” approach: implement strong UK governance as the baseline and apply additional EU-related controls when in scope.

The OAGF has been developed by Positive Cyber Solutions to help organisations of all sizes implement AI governance without unnecessary complexity.

- Client-ready and adaptable — organisations may replace “the organisation” with their own entity name.
- Practical and operational — designed for real-world AI tool use governance.
- Aligned to global standards — intended to complement recognised standards and frameworks.
- Lifecycle-driven — supports governance across selection, approval, use, monitoring, and offboarding.

This annex provides non-normative guidance to support implementation. It includes rollout approaches, staff awareness materials, worked examples, KPI examples, and optional mappings to external standards. Guidance in this annex does not create additional mandatory requirements beyond Clauses 1–8.

Annex B.1 Rollout guidance (30/60/90-day example)

Days 1–30 (establish control)	**Days 31–60 (standardise)**	**Days 61–90 (run & improve)**
• Appoint owners (governance, privacy, security) and agree risk appetite for Tier 1–3. • Create the AI Tool Register; log what is already used (including shadow AI discovery via staff survey). • Publish staff do/don’t rules and launch a simple request/approval route. • Pick 1–2 priority use cases and run through the lifecycle stages as a pilot.	• Complete **AUIAs** for Tier 2–3 use cases in flight (AI-13), along with any required Privacy/Security reviews where applicable. • Implement configuration controls (access groups, logging, retention, connector restrictions) for approved tools. • Create repeatable templates: Use Request, AUIA, Tool Profile, Deployment & Approval Record. • Train staff on safe prompting and required human review steps.	• Start KPI reporting (see AI-08 in Clause 7) and maintain a consistent incident/near miss log (see AI-10 in Clause 7 and evidence expectations in Clause 8). • Review supplier changes/terms and set re-approval triggers. • Expand to additional use cases and refresh acceptable-use guidance based on issues observed. • Schedule annual review and internal audit-style spot checks.

Annex B.2 Staff quick rules (one page example)

DO	DON'T
• Use approved AI tools only (check the AI Tool Register if unsure). • Treat AI output as draft and verify facts, numbers, and claims before using them (see AI-16 Output validation and quality assurance). • Apply human review before sending/publishing customer-facing content or making consequential decisions. • Use minimum necessary data and prefer placeholders (e.g., "<customer name>"). • Report suspected issues: unsafe outputs, data leakage, or policy breaches (treat as an incident). • For regulated advice (legal/medical/financial) or decisions affecting people, follow your organisation's existing approval routes and do not rely on AI outputs without explicit approval and documented controls.	• Don't paste/upload restricted or confidential data into public/unapproved AI tools (including consumer/free accounts). • Don't enter credentials (passwords, API keys), payment card data, or special category data unless the use case explicitly permits it. • Don't send AI-generated outputs externally without review, even if they "sound right". • Don't use AI to impersonate people, fabricate approvals, or mislead customers. • Don't bypass controls (logging, retention, DLP warnings, blocked connectors/extensions).

When to escalate: If you are unsure whether data is allowed, if an output could affect a customer/person materially, or if the tool behaves unexpectedly (unsafe content, incorrect confident claims, suspected leakage), stop and escalate to your Service Owner / Process Owner or the Risk & Compliance Lead.

Annex B.3 Worked example (customer email and website copy)

This worked example demonstrates how an organisation might apply the OAGF lifecycle stages to a common GenAI use case: drafting customer emails and website copy. It is provided for illustration only and does not add requirements beyond the normative clauses.

Example stages (maps to Clause 5 lifecycle)

1. **Discovery & scoping:** define purpose (drafting), channels (email/website), users, and boundaries (no restricted data; human review before sending/publishing). Evidence: Use Request; Register entry.

2. **Risk assessment (AUIA):** classify as Tier 2 if personal data is used (even limited), or Tier 1 if strictly public content only; define review controls. Evidence: AUIA (AI-13); DPIA decision (if needed).
3. **Data handling controls:** enforce placeholders; prohibit client confidential details; define retention expectations and allowed outputs. Evidence: Tool Profile; data rules in Register.
4. **Supplier due diligence:** confirm training-on-data position, retention, sub-processors, assurance, incident notification. Evidence: due diligence record; contract clause checklist.
5. **Configuration & access:** restrict access to marketing/customer service; block risky connectors; enable logging where available. Evidence: configuration record; access groups.
6. **Pilot & quality checks:** sample-check outputs for accuracy, tone, and policy compliance; test failure modes (hallucinations, unsafe content). Evidence: pilot notes; sample-check log (AI-16).
7. **Deployment & approval:** record approval conditions (mandatory human review, prohibited data); publish user guidance. Evidence: approval record; updated Register.
8. **Monitoring:** track complaints, rework rates, policy breaches, and supplier changes; set re-approval triggers. Evidence: monitoring plan; KPI log; incident log.
9. **Retirement:** remove access; confirm deletion/retention; archive evidence. Evidence: retirement log; updated Register.

Annex B.4 Optional mappings (placeholders)

Organisations may create a mapping table between OAGF clauses/controls and external frameworks such as ISO/IEC 42001 and the NIST AI Risk Management Framework. Any mapping is informative and shall not override the requirements in Clauses 1–8.

Annex B.5 Worked Tier examples

These examples show how the tier criteria (Clause 6.2) translate into a practical decision and what a "minimum viable" evidence set can look like for an SME (Clause 8.2). They are illustrative and do not add requirements.

Example 1: Tier 1 (internal drafting with no personal data)

Use case	Staff use an approved GenAI assistant to draft internal policies, meeting notes, and marketing ideas, using **public or internal non-sensitive** information only.
Tier decision (why)	• Data: no personal/confidential/restricted data. • Automation/impact: draft/advisory only; internal use. • Regulatory exposure: none specific. → **Tier 1**

Minimum viable evidence (SME)	• AI Tool Register entry (AI-02): owner, purpose, Tier 1 rationale, allowed/prohibited data, and "outputs treated as draft". • Staff quick rules communicated (AI-04) including escalation route (AI-10). • Basic data red lines recorded (AI-03).

Example 2: Tier 2 (customer email drafting using limited personal data)

Use case	Customer support uses an approved AI tool to draft response emails. Prompts may include **customer name** and **order reference** but must not include payment data or sensitive categories. All emails are reviewed by a human before sending.
Tier decision (why)	• Data: personal data is processed (customer identifiers). • Impact: external communication; risk if incorrect/misleading. • Oversight: mandatory human review before sending. → **Tier 2**
Minimum viable evidence (SME)	• AI Tool Register entry (AI-02) including allowed personal data fields and prohibited data (AI-03), plus who can use the tool and required review step (AI-05/AI-16). • Completed AUIA (AI-13) proportionate to the use case (may be short-form for SMEs), approved prior to go-live. • Basic supplier checks recorded (Clause 8.2 / AI-06), including training-on-data position, retention, and incident notification route. • Approval note (AI-12) and re-approval triggers recorded (AI-09).

Annex C: Risk classification matrix

C. Risk Classification Matrix (4 tiers + EU AI Act overlay)

The tiers in this appendix are a simple OAGF-defined risk classification to help organisations apply proportionate controls (they are not a legal or regulatory tiering scheme). Classify each AI tool use case (not just the tool) into the most appropriate tier below. Where your organisation already has an enterprise risk rating method, you may map these tiers to your existing scheme, provided the minimum conformity and evidence requirements in Clause 8 are still met (and recorded in accordance with AI-12 in Clause 7).

- **Use-case based:** the same AI tool can have multiple use cases with different tiers.
- **Use the highest applicable tier:** if a use case meets Tier 3 criteria, treat it as Tier 3 even if it also meets Tier 2 criteria.
- **When unsure, classify up:** if you are between tiers, pick the higher tier and reduce later if evidence supports it.
- **Record the reason:** store a short rationale in the AI Tool Register (see AI-02 in Clause 7) and document the classification decision consistent with Clause 6.

Note on Tier 4: Tier 4 is an overlay (additional requirements) used when the EU AI Act applies, and the relevant use is considered high-risk (or when an organisation chooses to meet equivalent controls contractually). In practice, a Tier 4 use case will usually be treated as Tier 3 + additional Tier 4 obligations, not as a separate "base" risk level.

- Tier 1 (Low): internal productivity support; no personal data; no customer/individual impact.
- Tier 2 (Medium): uses personal data and/or influences internal decisions; limited external impact (e.g., drafts that are reviewed before being sent externally).
- Tier 3 (High): material impact on customers/individuals; regulated or safety/security-significant context; or high potential for harm if wrong (including reliance on outputs for decisions).
- Tier 4 (EU AI Act High-risk Overlay): apply in addition to Tier 3 when the EU AI Act is in scope and the system is high-risk (or when contractually required to meet equivalent EU-aligned controls).

Annex D: Example documentation templates

D. AI Tool Register Template

This appendix provides an example AI Tool Register format. Organisations may adapt it to suit their systems and tools.

Ref	AI Tool / Feature	Supplier	Business Function	Description of Use	Data Involved (High-level)	Human Oversight (Yes/No)
A1	Microsoft Copilot	Microsoft	Administration	Drafting internal emails and first drafts of internal documents (always reviewed before sending)	Internal business data (no client or personal data)	Yes