

KOMGIS

AI System Inventory

*Controlled register and governance requirements for AI system ownership,
intended use, models, data, risk and operational status*

Core inventory commitment

Every production AI system operated by KOMGIS or for a client must be identifiable, owned, purpose-bound and traceable through a current AI System Inventory record. The inventory is a deployment gate and a lifecycle control: it records what the system is, why it exists, which models and data it uses, what risks and approvals apply, and whether it is authorized to operate.

Document owner: AI Governance / Technical Leadership

Version: 1.0

Effective date: 8 July 2026

Classification: Internal Governance Record Standard

Document Control

Field	Value
Document title	KOMGIS AI System Inventory
Document owner	AI Governance / Technical Leadership
Version	1.0
Effective date	8 July 2026
Review frequency	At least annually and after defined lifecycle, risk, provider, data or incident trigger events
Approved by	[Executive approver / role]
Classification	Internal Governance Record Standard
Applies to	All KOMGIS AI systems, client AI implementations, internal AI tools and AI-enabled production workflows
Record authority	AI Governance / Technical Leadership or delegated inventory administrator

Status and interpretation note

This document defines KOMGIS's controlled AI System Inventory requirements and record structure. It implements the inventory and intended-purpose requirements established by the KOMGIS Responsible AI and AI Management Policy. It is an internal governance control, not an ISO certification, conformity assessment or standalone legal classification. Regulatory role and classification must be assessed for each system's actual intended purpose, deployment context and jurisdiction.

Inventory Control Statement

The AI System Inventory is KOMGIS's authoritative portfolio record for AI-enabled systems. It is not a marketing list, architecture diagram or informal spreadsheet of experiments. A production AI system must have a unique inventory record that identifies accountable owners, intended purpose, technical and data dependencies, internal risk classification, operational status, required approvals and linked governance evidence.

An inventory record shall be created early enough to influence design and risk treatment. It shall be reviewed before production deployment, updated when material changes occur, and retained after retirement according to KOMGIS's governance and retention requirements.

Mandatory deployment rule

No production AI system shall be enabled for KOMGIS or a client when the inventory record is missing, has no named system owner or technical owner, lacks an approved intended purpose, or shows a lifecycle status that does not authorize production operation.

Contents

1. Purpose
2. Scope
3. Relationship to the KOMGIS AI Governance Framework
4. Definitions
5. Inventory Control Principles
6. AI System Identification and Unique Inventory IDs
7. System Ownership and Accountability
8. Intended Purpose and Approved Use Boundaries
9. Expected Users, Affected Parties and Deployment Context
10. KOMGIS Role and Regulatory Classification Assessment
11. Internal AI Risk Classification and Risk Linkage
12. System Architecture and Deployment Environment
13. Models, Model Providers and Model Configuration
14. Prompts, Workflows, Agents and Tool Capabilities
15. Data Categories and Data Processing
16. RAG Sources, Knowledge Stores and Vector Data
17. Personal, Confidential and Regulated Data
18. Integrations, Vendors and Subprocessors
19. Human Oversight and Approval Requirements
20. Evaluation, Testing and Release Evidence
21. Operational Status and Production Authorization
22. Monitoring, Alerts and Operational Health
23. Incident, Nonconformity and Corrective-Action Linkage
24. Change Control, Versioning and Material Change Triggers
25. Retention, Deletion, Backup and Data-Lifecycle Linkage
26. Periodic Review and Inventory Recertification
27. Inventory Access, Record Integrity and Auditability
28. Missing Information, Exceptions and Temporary Records
29. Portfolio Reporting and Management Review
30. Retirement, Archiving and Record Closure
31. Roles, Enforcement and Escalation
32. Document Review and Continual Improvement
Appendix A. Mandatory AI System Inventory Data Dictionary
Appendix B. AI System Inventory Record Template
Appendix C. Model and Model Provider Subregister Template
Appendix D. Data, RAG Source and Vector Store Register Template
Appendix E. Agent Tool and Integration Register Template
Appendix F. Operational Status Matrix and Transition Gates

Appendix G. Risk-Based Review and Evidence Matrix

Appendix H. AI Portfolio Summary and Management Dashboard Fields

Appendix I. Illustrative Enterprise Document Intelligence Inventory Record

Appendix J. Inventory Review Checklist

Appendix K. Material Change Trigger Matrix

Appendix L. Alignment and Reference Documents

1. Purpose

This document defines how KOMGIS creates, maintains, reviews and closes records in the AI System Inventory. The inventory provides a single controlled view of the AI systems KOMGIS develops, configures, integrates, deploys or operates.

The inventory is intended to make six questions answerable for every AI system:

- Who is accountable for the system and its operation?
- What specific business purpose is the system approved to perform?
- Which models, providers, prompts, agents, tools and integrations form part of the system?
- Which data categories, source systems, RAG repositories and derived AI data are processed?
- What internal risk level, regulatory assessment, human oversight and governance evidence apply?
- What is the system's current operational status, production authorization and lifecycle state?

The inventory also supports change control, incident response, internal audit, client due diligence, portfolio review and retirement by linking each system to its risk assessments, evaluation evidence, data-processing records, provider approvals and operational monitoring.

2. Scope

This inventory standard applies to AI systems developed, configured, integrated, deployed or used by KOMGIS where the system is used for company work, client delivery or production business processes. It includes standalone AI products and AI capabilities embedded inside larger software systems.

- AI assistants, chatbots and conversational interfaces;
- retrieval-augmented generation (RAG), enterprise search and document intelligence platforms;
- document summarization, classification, extraction and structured-output systems;
- AI agents, tool-using systems and controlled workflow automation;
- voice interfaces, transcription, conversational voice systems and AI-enabled avatars;
- decision-support, recommendation and prioritization systems;
- AI-generated reports, drafts, messages and structured records;
- embeddings, vector retrieval services and model gateways when they are part of an AI system;
- client-specific AI implementations and internal AI tools;
- material prototypes or pilots when they use real client data, affect real users or are connected to production systems.

Ordinary non-AI software libraries and purely deterministic rules are not separately inventoried as AI systems. They shall be recorded as components of an AI system when they materially enforce authorization, validation, approval, tool access or other AI control boundaries.

System boundary rule

Inventory the controlled business capability, not every model API call as a separate system. A model, embedding service or vector database is normally a component of an AI system unless KOMGIS intentionally operates it as a shared platform with distinct ownership, risk and operational controls.

3. Relationship to the KOMGIS AI Governance Framework

The AI System Inventory is a supporting governance record required by the KOMGIS Responsible AI and AI Management Policy. The inventory does not replace system-specific policies, risk assessments or evidence. It acts as the index that identifies which governance records apply and where they are maintained.

Governance record	Inventory linkage
-------------------	-------------------

Governance record	Inventory linkage
Responsible AI and AI Management Policy	Defines the requirement to inventory production AI systems and document intended purpose, ownership, risk, models, data and status.
AI Security Policy	Provides security control requirements referenced by the system architecture, RAG, prompt injection, tool, secret and monitoring fields.
Data Privacy Policy	Provides data category, provider, retention, deletion and client-data handling requirements referenced by inventory records.
AI Incident Response Plan	Provides incident severity, containment and reactivation requirements linked from operational status and incident fields.
AI Risk / Impact Assessment	Provides the detailed risk analysis and residual-risk decision associated with the inventory risk classification.
Model Provider / Vendor records	Provide due-diligence and processing details for model, cloud and subprocessor dependencies recorded in the inventory.
Human Oversight Record	Provides evidence of review and approval controls for sensitive outputs or actions.
Evaluation and Testing Records	Provide evidence supporting release, ongoing quality and safety claims recorded in the inventory.

The inventory shall reference authoritative records rather than duplicating entire risk assessments, contracts or test reports. A short summary may be stored in the inventory, but detailed evidence shall remain in the controlled source record.

4. Definitions

Term	Inventory meaning
AI system	A machine-based system that infers from inputs to generate outputs such as content, predictions, recommendations or decisions that may influence physical or virtual environments.
Inventory record	The controlled record representing one AI system and its ownership, intended purpose, technical components, data, risk, governance and lifecycle status.
AI system owner	The accountable business owner for the system's intended purpose, risk acceptance, operation, oversight and retirement.
Technical owner	The person or team accountable for technical implementation, architecture, controls, testing, monitoring and operational integrity.
Intended purpose	The documented use for which the system is designed, approved and evaluated, including users, task, context and expected output or action.
Use boundary	A documented limit defining what the system is not approved to do, which users or data are excluded, or where mandatory human handling applies.
Model component	A generative, reasoning, embedding, classification, transcription, vision or other model used by the system.
RAG source	An authorized document, database, knowledge store or other source from which content may be retrieved and provided to a model.
AI agent	An AI-enabled system able to select or call approved tools, integrations or actions to advance an assigned task.
Sensitive action	An external, irreversible, high-impact or regulated action that requires defined human approval.

Term	Inventory meaning
Operational status	The controlled lifecycle state indicating whether a system is proposed, being assessed, in development, testing, authorized for production, restricted, suspended, deprecated or retired.
Material change	A change to purpose, model, provider, data, permissions, RAG sources, tools, autonomy, oversight or other characteristic that may materially alter risk or control effectiveness.
Inventory administrator	The authorized role responsible for record quality, inventory conventions, portfolio completeness and administrative control of the register.

5. Inventory Control Principles

5.1 Completeness

Every in-scope production AI system must have an inventory record. The inventory shall also include material pilots and prototypes where real client data, real users, production integrations or significant risk are involved.

5.2 Single accountable system record

Each AI system shall have one authoritative master record. Supporting component registers may be linked to the master record, but ownership and production authorization shall not be fragmented across unconnected records.

5.3 Purpose before technology

The inventory shall identify the business purpose before listing models or providers. A system shall not be approved merely because a model performs well technically. The intended use, affected workflow and consequences of failure determine the required controls.

5.4 Current status

The record shall reflect the system that is actually operating. Model, provider, data source, tool, permission and human-approval changes shall be reflected through change control rather than left only in engineering tickets or source code.

5.5 Evidence linkage

Claims such as “tenant isolation tested,” “human approval required,” or “provider approved” shall link to or identify the relevant evidence, configuration, test record or controlled governance record where risk requires evidence.

5.6 Proportionality

Low-risk systems may use concise records. Limited, high and critical systems require more detailed inventory data and formal evidence. The minimum fields identified as mandatory apply regardless of risk unless a field is explicitly marked not applicable with a reason.

Do not use the inventory as a substitute for controls

Recording that a system has role-based access control, approval gates or client isolation does not implement those controls. The inventory identifies the expected control and its evidence; application and infrastructure controls must enforce it.

6. AI System Identification and Unique Inventory IDs

Each system shall receive a stable inventory identifier when the record is created. The identifier remains associated with the system throughout its lifecycle and shall not be reused after retirement.

Identification field	Requirement
Inventory ID	Unique immutable identifier, for example AI-SYS-0001.
System name	Human-readable approved name used consistently in governance records.
Short name / code	Optional technical or portfolio code used in dashboards and logs.
System version	Current governed release or product version.
Record version	Version of the inventory record itself, separate from application release version.
Business unit / portfolio	KOMGIS team, product line or client portfolio responsible for the system.
Client / tenant scope	Internal KOMGIS, named client, multi-client service or other defined scope.
Related parent system	Platform or larger software product in which the AI capability is embedded.
Related child components	Material AI subsystems or shared AI services linked to this record.
Created / last reviewed	Record creation date and latest formal inventory review date.

A major product redesign does not automatically require a new Inventory ID. The system owner and AI Governance / Technical Leadership shall determine whether the changed capability remains the same governed system or is a new system based on intended purpose, affected users, system boundary and risk profile.

7. System Ownership and Accountability

No production record may have “team,” “vendor,” “model provider,” or an application name as the sole accountable owner. The inventory must identify named accountable roles and, where practical, named individuals or current role holders.

Ownership field	Minimum responsibility recorded
AI system owner	Owns intended purpose, business use, risk acceptance, human oversight, operational review and retirement.
Technical owner	Owns architecture, implementation, technical controls, release evidence, monitoring and technical incident support.
Security / privacy reviewer	Reviews data exposure, access control, tenant isolation, provider risk and privacy requirements as applicable.
Project / client owner	Maintains client requirements, deployment commitments and coordinated client communication.
Human oversight owner	Ensures reviewer roles, approval criteria, training and escalation are defined.
Monitoring / alert owner	Receives operational alerts and ensures triage and escalation.
Incident response linkage	Identifies the response route and responsible function for AI incidents.
Backup / continuity owner	Where applicable, owns recovery and service continuity dependencies.

Ownership changes are controlled inventory updates. A departing or reassigned owner shall be replaced promptly. High or critical systems shall not remain in normal production operation without an active system owner and technical owner.

Accountability rule

Responsibility for the system shall not be assigned solely to the model provider. KOMGIS and the authorized human owners of the business process remain accountable for the system, its intended use, its controls and its operational decisions.

8. Intended Purpose and Approved Use Boundaries

The intended purpose is the central inventory field. It shall be specific enough to support risk assessment, evaluation and change control. “AI assistant,” “chatbot,” “automation” or “document AI” alone are not adequate intended-purpose statements for systems that access client data or perform actions.

8.1 Required intended-purpose elements

- business process or workflow supported;
- primary task the AI performs;
- expected user group or service identity;
- input types and main data context;
- expected output, recommendation or action;
- whether the output is advisory, draft, reviewed or automatically acted upon;
- deployment context, such as internal, client-facing or embedded in another application;
- material success criteria and accuracy expectations;
- explicit exclusions and circumstances requiring manual handling.

8.2 Intended-purpose format

Recommended statement pattern

[System] is intended to [AI task] for [authorized users] within [business process / deployment context] using [main input / source types] to produce [output or action]. The output is [advisory / draft / reviewed / automated] and must not be used for [material exclusions].

8.3 Example

Adequate: “The Enterprise Document Intelligence Platform is intended to answer authorized employee questions from documents the employee is permitted to access within the client workspace. It retrieves permission-filtered document chunks, generates a source-grounded response and displays citations. The response supports employee information retrieval and is not approved to make legal, employment, credit, insurance or other consequential decisions.”

Inadequate: “General RAG chatbot for company documents.”

8.4 Approved and prohibited use boundaries

The inventory shall record reasonably foreseeable uses that are approved and material uses that are not approved. Restricted or prohibited use categories identified by the Responsible AI and AI Management Policy shall be escalated before development commitment or deployment.

9. Expected Users, Affected Parties and Deployment Context

Inventory records shall distinguish the person using the AI system from people who may be affected by its output or action. A system used by an employee may still affect a client, customer, applicant, patient, policyholder or other person.

Field	Examples / recording rule
-------	---------------------------

Field	Examples / recording rule
Primary users	Employees, client administrators, client employees, support staff, reviewers, developers or service accounts.
Secondary users	People who consume a report, draft, recommendation or other downstream output.
Affected parties	Individuals or organizations whose access, money, rights, employment, insurance, safety or other material interest could be influenced.
Vulnerable groups	Record whether minors, elderly persons or other potentially vulnerable populations are materially involved.
Interaction mode	Chat, API, batch processing, background workflow, voice, agent or embedded application feature.
User visibility of AI	Obvious AI interaction, disclosed AI assistance, internal-only AI or not directly visible to the affected person.
Deployment context	Internal KOMGIS, single client, client-managed tenant, multi-tenant service, on-premises or other context.
Scale	Approximate user, document, request, action or affected-person volume where risk depends on scale.

Where affected persons or important decisions are material, the inventory shall identify the linked impact assessment and human oversight requirements.

10. KOMGIS Role and Regulatory Classification Assessment

The inventory shall record KOMGIS's assessed role under applicable law where relevant, such as provider or deployer, and shall identify the status of any regulatory classification review. This is separate from KOMGIS's internal operational risk level.

Assessment field	Required record
KOMGIS assessed role	Provider, deployer, multiple roles, not yet determined or not applicable, with reviewer/date where relevant.
Jurisdiction / market	Countries or regulatory contexts materially relevant to the deployment.
Regulatory classification status	Not assessed, preliminary, reviewed, escalated, or approved.
Potential restricted / high-risk signal	Yes / no / uncertain, with short rationale and escalation reference.
Transparency obligation review	Whether user-facing AI disclosure, synthetic-content marking or other transparency analysis is required.
Legal / compliance reviewer	Reviewer or function and review date when legal interpretation is required.
Decision reference	Link or identifier for the classification analysis or legal/compliance record.

Separation rule

An KOMGIS internal risk classification of Low, Limited, High or Critical does not determine the system's legal classification. The inventory shall store both assessments separately and shall not treat one as a substitute for the other.

11. Internal AI Risk Classification and Risk Linkage

Every AI system shall have an KOMGIS internal operational risk classification before production use. The inventory stores the current classification, rationale summary, approver and linked risk assessment.

Risk level	Typical inventory expectations
Low	Internal assistance, non-sensitive data, no material external action and easily reversible errors. Concise inventory, owner, basic testing and monitoring.
Limited	Client-facing content, confidential data, RAG, structured extraction or limited integrations. Risk assessment, privacy/security review, documented tests, logs and defined human review.
High	Sensitive domain, important decisions, material external communication, write tools, significant personal data, high autonomy or potentially serious client impact. Formal risk/impact assessment, strong oversight, approval gates, audit logs and management risk acceptance.
Critical	Potential severe harm, large-scale cross-client exposure, dangerous autonomous action, safety impact or potential prohibited/high-risk regulatory category. No deployment until executive, technical, security and legal/compliance approval and enhanced monitoring.

The inventory shall record: current risk level; classification date; classifier; short rationale; top material risk themes; residual-risk status; risk acceptance owner; next risk review date; and the authoritative risk or impact assessment reference.

The classification shall be based on the most consequential reasonably foreseeable scenario, not the average expected use. Uncertainty may justify a higher classification until evidence supports reduction.

12. System Architecture and Deployment Environment

The inventory shall contain a concise architecture summary sufficient to understand the system boundary and major control dependencies. Detailed architecture diagrams may remain in separate technical documentation and shall be linked from the inventory.

- application or service boundary;
- frontend and user interaction layer;
- backend application or orchestration layer;
- model gateway or direct provider integrations;
- RAG, vector or hybrid retrieval layer;
- databases, file stores and caches holding client or AI data;
- agent orchestration, tools and external integrations;
- authentication, authorization and tenant-isolation enforcement points;
- logging, monitoring and alerting systems;
- deployment environment, cloud or hosting provider, region and environment type;
- rollback, disable or safe-stop mechanism.

Environment field	Inventory requirement
Environment type	Development, test, staging, production or client-managed environment.
Hosting / infrastructure	Approved cloud, on-premises or managed platform used by the system.
Primary processing region	Region or location relevant to client data processing.
Data residency constraints	Client, contractual or regulatory restrictions.
Authentication source	Identity provider or authentication method.
Authorization boundary	Backend layer enforcing role, tenant and object-level access.

Environment field	Inventory requirement
Tenant isolation mechanism	Database, object, file, retrieval and credential isolation summary.
Disable / rollback control	Feature flag, service disable, tool revocation, model fallback or other stop mechanism.

13. Models, Model Providers and Model Configuration

The inventory shall identify every material model component used by the production system. Shared model infrastructure may be referenced through a linked subregister, but the system record must still identify which model capability is active for the system.

Model field	Recording rule
Model purpose	Generation, reasoning, embedding, classification, vision, transcription, reranking or other defined use.
Provider	Approved model provider or self-hosted model operator.
Product / model family	Provider product and model family sufficient for governance and vendor review.
Exact model identifier	Production model or deployment identifier where available.
Model version / alias handling	How mutable aliases, snapshots or provider-controlled versions are managed.
Hosting mode	Provider API, managed cloud, dedicated deployment, self-hosted or local.
Processing region	Known region or configuration relevant to data residency.
Training / service-improvement setting	Approved provider setting or contractual position for submitted data.
Retention setting	Provider-side retention or zero/limited-retention configuration where applicable.
Fallback model	Approved fallback and conditions for use.
Evaluation baseline	Test record or benchmark associated with the active model configuration.
Approval reference	Model provider review, vendor record or technical approval.

A model change is not considered “only a vendor update” when it materially affects quality, context limits, tool behavior, data processing, safety controls or cost. Material model changes shall trigger inventory, risk and evaluation review before production release.

Model is not the system

The model identifier shall not be used as the system name unless the model itself is the governed KOMGIS service. Inventory records must describe the complete AI-enabled business capability, including application controls, retrieval, tools and human oversight.

14. Prompts, Workflows, Agents and Tool Capabilities

AI behavior may be materially determined by prompts, workflow logic, routing, tool selection and application-level policies. The inventory shall identify governed behavior components and their versioning approach.

Component	Minimum inventory information
-----------	-------------------------------

Component	Minimum inventory information
System prompt / policy layer	Version or repository reference and purpose. Do not store secret values in the inventory.
Prompt templates	Material template family, versioning approach and intended task.
Workflow / orchestration	Workflow engine or orchestration logic and governed workflow version.
Agent capability	Whether the system is agentic and the scope of autonomy.
Read tools	Approved tools that retrieve or inspect information without material external change.
Write tools	Approved tools capable of creating, updating, sending, deleting or otherwise changing external state.
Sensitive actions	Actions requiring mandatory human approval.
Approval gate	Server-side mechanism blocking the action until authorized approval.
Tool credentials	Credential owner and scope; record references only, never secret values.
Rate / export limits	Volume or abuse controls relevant to tool and data access.
Safe-stop mechanism	Ability to disable an agent, tool or credential without disabling unrelated systems.

The inventory shall explicitly state whether a tool is read-only, reversible write, external communication, destructive or otherwise sensitive. An AI agent shall not be recorded as having “general tools” or “system access” without individual tool scopes and control boundaries.

15. Data Categories and Data Processing

The inventory shall identify the data categories the AI system receives, retrieves, generates, stores or exposes to model providers. The record shall be sufficiently specific to support privacy, security, retention and provider decisions.

Data category	Examples
Account and identity data	User identifiers, organization, workspace, roles and authentication metadata.
Client business data	Documents, records, cases, tickets, contracts, product or workflow information.
Prompts and user inputs	Chat messages, instructions, form fields, voice input and uploaded files.
Retrieved context	RAG chunks, database records, web content or tool output selected for model context.
AI outputs	Responses, summaries, drafts, classifications, extractions and structured outputs.
Embeddings and vector metadata	Derived vector representations, chunk metadata and source identifiers.
Workflow and action data	Tool calls, action payloads, approval records and downstream status.
Audit and monitoring data	Model identifiers, prompt/workflow versions, source references, security events and operational metrics.
Support / incident data	Troubleshooting records, evidence, screenshots or incident artifacts.

For each material data category, the inventory or linked Data Processing Map shall identify purpose, source, destination, provider exposure, storage, sensitivity, retention and deletion behavior. Derived AI data shall be governed as client data when generated from client content.

Data minimization rule

The inventory must describe the data actually needed for the approved task. Entire document libraries, databases or mailboxes shall not be treated as necessary merely because the system can technically access them.

16. RAG Sources, Knowledge Stores and Vector Data

RAG and enterprise document intelligence systems shall have a source register that identifies what content may be retrieved, how it is authorized and how source lifecycle changes propagate to extracted text, chunks and embeddings.

RAG / source field	Required information
Source name and type	Document library, file store, database, knowledge base, website or other source.
Source owner	Business or client owner responsible for the source.
Client / tenant scope	Client or workspace to which the source belongs.
Authorization hierarchy	Project, field, section, document, department, role, object or other permission hierarchy.
Retrieval filter	Metadata and permission conditions applied before content enters the model prompt.
Ingestion method	Upload, API, scheduled synchronization, event-driven ingestion or manual process.
Chunking / extraction version	Material processing pipeline version or configuration reference.
Embedding model	Active embedding model and linked model register entry.
Vector / retrieval store	Vector database or hybrid search service and environment.
Source citation mechanism	Document, page, section, chunk or other identifiers used for traceability.
Deletion propagation	How deleted or disabled source data removes or disables text, chunks and embeddings.
Isolation test evidence	Reference to cross-client and permission-aware retrieval testing.

Mandatory RAG authorization rule

The system must retrieve only data the active user and client workspace are authorized to access. The inventory shall never describe “model filtering” or “prompt instructions not to reveal data” as the primary authorization control.

17. Personal, Confidential and Regulated Data

The inventory shall identify whether personal, confidential, regulated or otherwise sensitive data may be processed. “Client data” alone is not sufficient when the sensitivity of the data materially changes the risk, provider configuration or human-oversight requirements.

Sensitivity field	Inventory entry
Personal data	Yes / no / possible / unknown; categories or linked privacy assessment.
Sensitive or special-category data	Record applicable categories where relevant and approved.
Client confidential data	Type of confidential business information processed.

Sensitivity field	Inventory entry
Secrets / credentials expected	Normally no. Record prevention and incident handling if accidental exposure is possible.
Regulated-domain data	Health, insurance, financial, employment, education, legal or other regulated context.
Data subject / affected person groups	Employees, customers, applicants, policyholders or other groups.
Cross-border / cross-region processing	Known transfers or processing locations.
Data residency requirement	Contractual or client requirement and technical configuration reference.
Privacy review	Reviewer, date and linked Data Processing Map or privacy assessment.

Real production client data used in development or testing shall be separately documented with necessity, approval, restrictions and deletion requirements. Synthetic, dummy, anonymized or client-approved test data shall be preferred whenever possible.

18. Integrations, Vendors and Subprocessors

The inventory shall identify material external services and integrations that process client data, influence AI behavior or enable system actions. Each material provider shall link to an approved vendor or subprocessor record where required.

Dependency	Inventory requirement
Model provider	Provider, product, data sent, processing region and approval reference.
Cloud / hosting provider	Service and region supporting compute, storage or networking.
Vector / search provider	Service storing or retrieving embeddings, chunks or search metadata.
Observability provider	Logs, traces, metrics or AI monitoring data processed.
Document processing provider	OCR, parsing, extraction or file conversion service.
Communication integration	Email, messaging, voice or notification service used for AI-assisted actions.
Business system integration	CRM, ERP, ticketing, document management, HR, finance or client system.
Identity provider	Authentication or enterprise identity dependency.
Other subprocessor	Any third party processing client or personal data on KOMGIS's behalf.

Unknown providers, personal AI accounts and unapproved public AI tools shall not be listed as acceptable production dependencies. A provider change is a controlled change and may trigger updates to risk, privacy, retention, data residency and evaluation evidence.

19. Human Oversight and Approval Requirements

The inventory shall describe how humans supervise the AI system and which outputs or actions require review. “Human in the loop” is insufficient unless the reviewer role, trigger, evidence and authority are defined.

Oversight field	Required detail
Oversight model	Normal user judgment, defined output review, mandatory approval or other controlled model.
Reviewer role	Authorized role or group responsible for review.

Oversight field	Required detail
Review trigger	Every output, selected workflow state, confidence threshold, exception or sensitive action.
Evidence available	Sources, retrieved documents, extracted fields, model rationale where appropriate, validation results or comparison data.
Reviewer authority	Ability to approve, reject, edit, override, reverse, stop or escalate.
Approval gate	Technical mechanism blocking sensitive action until approval.
Escalation path	Role or function receiving uncertain, disputed or high-impact cases.
Competence / training	Required reviewer knowledge or training reference.
Oversight record	Location of approval, rejection, material edit and decision records.

Sensitive external communication, material record updates, payments, external file sharing, important deletions and other difficult-to-reverse actions shall be recorded as sensitive actions and shall require human approval unless a specific lawful automation use has been assessed, approved and documented.

20. Evaluation, Testing and Release Evidence

The inventory shall state whether the system has passed the evaluation and control tests required for its intended purpose and risk. It shall link to authoritative evaluation and testing records rather than replacing them.

Evidence field	Examples
Quality evaluation	Task accuracy, completeness, hallucination rate, extraction precision or classification performance.
Grounding / citation evaluation	Faithfulness to source, citation correctness and source coverage.
Authorization testing	Authentication, object access and tenant isolation.
RAG permission testing	Authorized-only retrieval, wrong-client isolation and source deletion behavior.
Prompt injection testing	Direct and indirect malicious instructions, hidden content and tool-manipulation cases.
Agent tool testing	Unauthorized tools, wrong scopes, approval bypass and safe-stop behavior.
Output validation testing	Schema, allowed fields, downstream API validation and failure handling.
Privacy / logging testing	Secret exclusion, log redaction and data-minimization checks.
Performance / reliability	Latency, availability, cost or fallback criteria.
Release approval	Release decision, blocking defects resolved, residual risk accepted and approval date.

The inventory shall record evaluation status as Not started, In progress, Passed, Passed with accepted limitations, Failed / blocked, or Not applicable with rationale. A failed tenant-isolation test, bypassed approval gate or other blocking control defect prohibits normal production authorization.

21. Operational Status and Production Authorization

Operational status is a controlled lifecycle field and shall state whether the system is authorized to operate. Status shall not be inferred from the existence of a production URL, deployment pipeline or active client account.

Status	Meaning
--------	---------

Status	Meaning
Proposed	Use case identified; system not approved for production use.
Assessment	Purpose, role, data and risk are being evaluated.
Development	System is being built in a non-production context.
Testing	System is undergoing controlled evaluation or acceptance testing.
Pilot / restricted production	Limited real use under defined users, data, volume and enhanced review conditions.
Approved for production	Required governance gates passed and deployment authorized; activation may still be pending.
Active production	Currently operating for approved users and intended purpose.
Restricted	Operating with temporary limitations, disabled capabilities or increased review.
Suspended / incident containment	Normal operation stopped because of incident, control failure or management decision.
Deprecated	Still operating for transition only; no new adoption or expansion.
Retired	AI capability disabled and no longer used for the intended process.
Archived record	Lifecycle closed; record retained for audit, incident or governance history.

21.1 Production authorization fields

- current operational status and effective date;
- production authorized: yes, no or conditional;
- approver and approval date;
- approved users, client scope and environment;
- conditions or restrictions attached to approval;
- scheduled next review date;
- system disable, rollback or feature-isolation mechanism;
- reactivation approval reference when returning from suspension.

Status control rule

A suspended or incident-containment system shall not be changed to Active production merely because the technical service is running again. Reactivation requires the approvals and retesting defined by the AI Incident Response Plan and the system risk level.

22. Monitoring, Alerts and Operational Health

Active systems shall identify the monitoring signals, alert owners and review cadence appropriate to risk. The inventory may summarize the monitoring plan and link to detailed dashboards or operating procedures.

Monitoring area	Possible inventory signal
Quality	Reviewer rejection/edit rate, unsupported claims, extraction failures or classification degradation.
RAG / citations	Missing citations, unexpected sources, source coverage or retrieval drift.
Security	Prompt injection attempts, unauthorized access, wrong-client references or unusual export patterns.

Monitoring area	Possible inventory signal
Agent tools	Unexpected tool calls, approval bypass attempts, action failures or retry loops.
Privacy	Sensitive data detected in outputs or logs, provider exposure or deletion failures.
Reliability	Availability, latency, queue backlog, model errors or provider outages.
Cost / usage	Abnormal token, API, compute or storage spikes.
Human oversight	Approval backlog, reviewer workload, repeated overrides or escalation rate.
Client feedback	Complaints, support patterns or repeated user-reported errors.

The inventory shall identify the monitoring owner, alert destination, review frequency and response route. High and critical systems shall have formal or enhanced monitoring appropriate to their risk and applicable obligations.

23. Incident, Nonconformity and Corrective-Action Linkage

The inventory shall provide the system identifier used in incident, monitoring and corrective-action records. Significant incidents and recurring nonconformities shall be linked to the inventory record so that the current risk, status and control posture can be understood.

Incident linkage field	Requirement
Incident reporting route	Approved channel or process for reporting suspicious or harmful AI behavior.
Incident response owner / function	Responsible response function for the system.
Latest material incident	Reference, severity, date and current status where applicable.
Open corrective actions	Material actions, owner and due date reference.
Recurring issue flag	Whether monitoring, complaints or incidents show a pattern.
Containment capability	Feature, model, tool or integration disable mechanism.
Reactivation status	Required approvals, tests and owner decision after suspension.
Risk update required	Whether incident evidence triggered risk or impact reassessment.

The inventory shall not contain unnecessary copies of sensitive incident evidence. Prompts, outputs, documents, credentials or personal data needed for investigation shall be preserved and protected in the incident record according to the AI Incident Response Plan.

24. Change Control, Versioning and Material Change Triggers

The inventory shall be updated before or as part of a material production change. Engineering deployment alone does not complete AI governance change control.

- new intended purpose or materially expanded use;
- new user population, affected population or client scope;
- new model provider or materially different model family;
- new model configuration that materially affects behavior or data processing;
- new client data category, RAG source, database or processing region;
- new write tool, external integration or sensitive action;
- increase in autonomy or removal of a human approval step;
- material prompt, workflow or routing behavior change;

- change to authorization hierarchy or retrieval permission filtering;
- new subprocessor or materially changed provider retention/training terms;
- significant performance degradation, recurring incident pattern or known vulnerability.

Change record field	Minimum content
Change ID / release	Engineering or governance change reference.
Change summary	What changed and why.
Affected inventory fields	Purpose, model, data, RAG, tools, risk, oversight, status or monitoring.
Materiality decision	Material / non-material and rationale.
Risk review	Whether classification or risk assessment changed.
Evaluation impact	Tests rerun or new evaluation required.
Privacy / provider impact	Data Processing Map, vendor or residency review.
Approval	Required reviewers and release decision.
Effective date	Date the change became active in production.

25. Retention, Deletion, Backup and Data-Lifecycle Linkage

Inventory records shall identify the retention and deletion rules that apply to source and derived AI data. Detailed schedules may be maintained in the Data Privacy Policy, Data Processing Map or system retention standard and referenced from the inventory.

Data / record type	Inventory expectation
Source files / records	Client- or service-defined retention and authoritative deletion route.
Extracted text / chunks	Normally linked to the source lifecycle.
Embeddings / vector records	Governed as derived client data and normally deleted or disabled with the source.
AI outputs / chat history	Workflow-defined retention proportionate to business and audit need.
Approval records	Retention sufficient for accountability and sensitive-action traceability.
Audit logs	Security and governance retention appropriate to system risk.
Debug / error logs	Short technical retention unless preserved for an active incident.
Backups	Backup schedule, protection and delayed-deletion behavior.
Inventory record	Retained after retirement for governance, audit and incident history according to record policy.

The inventory shall record the deletion owner, deletion mechanism and whether active vector data, caches or derived summaries may remain after source deletion. Any documented exception shall state the purpose, duration and approval.

26. Periodic Review and Inventory Recertification

Inventory records shall be reviewed periodically to confirm that the documented system still matches production operation. Review depth and frequency shall be proportionate to risk, change rate and operational evidence.

Risk / state	Minimum review expectation
--------------	----------------------------

Risk / state	Minimum review expectation
Low	At least annually and after material change or material incident.
Limited	At least annually; consider more frequent review for active client-facing systems, changing providers or rapidly changing RAG sources.
High	Formal periodic review at least every six months, plus change- and incident-triggered review.
Critical	Enhanced management-defined review cadence, no less frequent than high-risk review, with explicit status and control confirmation.
Pilot / restricted	Review at the end of the pilot period and before expansion of users, data, actions or client scope.
Suspended	Review before reactivation; normal periodic cadence does not authorize restart.
Deprecated	Review continued need, migration progress and retirement date.

26.1 Recertification review questions

- Does the intended purpose still match actual use?
- Are the named system and technical owners still current?
- Do active models, providers, regions and retention settings match the record?
- Have data categories, RAG sources, permissions or client scope changed?
- Are tool scopes, sensitive actions and human approval gates unchanged and effective?
- Does the current risk classification remain appropriate?
- Have evaluation results, incidents, complaints or monitoring signals changed the risk picture?
- Are required client, privacy, security and regulatory reviews still current?
- Is the operational status accurate and is continued production authorization justified?

27. Inventory Access, Record Integrity and Auditability

The AI System Inventory is an internal controlled governance record. Access shall be limited according to business need while allowing system owners, technical owners, governance reviewers, auditors and incident responders to obtain the information required for their responsibilities.

- use an approved repository or system of record;
- maintain authenticated access and appropriate edit permissions;
- record material record changes, reviewer or approver identity and effective dates;
- avoid storing API keys, passwords, tokens, private keys or other secret values;
- prefer references to controlled evidence instead of copying sensitive client data into the inventory;
- protect client names, architecture details and provider configurations according to classification;
- retain prior versions or change history sufficient to reconstruct material lifecycle decisions;
- support export or audit review of active systems and their required governance links.

Where the inventory is implemented in software, validation should prevent invalid status transitions, missing mandatory owners and production authorization when blocking fields are incomplete.

28. Missing Information, Exceptions and Temporary Records

A missing mandatory field shall not be silently left blank. The record shall show one of the following: complete value; not applicable with rationale; unknown with assigned owner and due date; or blocked pending review.

Field state	Required handling
Complete	Current authoritative value recorded.

Field state	Required handling
Not applicable	Reason explains why the field does not apply to the system.
Unknown / investigation required	Owner and target date assigned; production approval may be blocked according to risk.
Pending external evidence	Vendor, client, legal or technical dependency identified and tracked.
Exception requested	Documented risk, compensating controls, duration and authorized approver.
Blocked	System or change cannot proceed until the field or underlying control is resolved.

No “TBD forever” rule

Temporary placeholders are permitted during design and assessment, but they shall not become permanent substitutes for ownership, intended purpose, risk, model/provider identification, data classification or production authorization.

29. Portfolio Reporting and Management Review

AI Governance / Technical Leadership shall be able to use the inventory to understand KOMGIS's AI portfolio and identify systems requiring attention. Portfolio reports should use inventory data and avoid manual restatement where possible.

- number of AI systems by operational status and internal risk level;
- systems without current owner, review date or risk assessment;
- active model providers, model families, processing regions and critical dependencies;
- systems processing personal, confidential or regulated data;
- RAG systems and systems with write tools or sensitive actions;
- systems requiring mandatory human approval;
- open high-severity incidents or overdue corrective actions;
- systems due or overdue for periodic review;
- deprecated systems and planned retirement dates;
- material portfolio changes since the previous management review.

Management review may use inventory summaries to identify concentration risk, common provider dependencies, recurring control weaknesses, resource needs and opportunities for shared controls or platform standardization.

30. Retirement, Archiving and Record Closure

Retirement is a controlled lifecycle state. Removing a user interface or stopping sales does not by itself close the AI system record.

1. Confirm that the AI capability is no longer used for the approved business process or client deployment.
2. Disable production access, agents, tools, model routes and scheduled processing as applicable.
3. Revoke or rotate system-specific credentials that are no longer needed.
4. Execute source and derived AI data retention and deletion requirements.
5. Address embeddings, chunks, caches, temporary files and generated summaries linked to retired data.
6. Confirm backup and delayed-deletion treatment according to the backup process.
7. Close or transfer open incidents, corrective actions and client commitments.
8. Record retirement date, retirement owner, reason and evidence of shutdown.
9. Change operational status to Retired and, when record closure is complete, Archived record.
10. Retain the inventory history according to KOMGIS governance record requirements.

A retired Inventory ID shall not be reassigned to a new AI system. A replacement capability shall have its own record or an explicitly governed successor relationship.

31. Roles, Enforcement and Escalation

Role	Inventory responsibilities
Executive leadership	Review high or critical systems and portfolio risks; support corrective action and resource needs.
AI Governance / Technical Leadership	Own inventory standard, risk methodology, portfolio review and formal governance escalation.
Inventory administrator	Maintain conventions, record quality, completeness checks, lifecycle status integrity and reporting.
AI system owner	Maintain purpose, business accountability, risk acceptance, oversight and production authorization.
Technical owner	Maintain model, architecture, RAG, tool, test, monitoring and change-control information.
Security / privacy owner	Review client isolation, data sensitivity, provider exposure and privacy/security dependencies.
Project / client owner	Maintain client scope, client requirements, deployment context and client communication linkage.
Employees and contractors	Use approved systems and promptly report unrecorded AI use, suspicious behavior or material inventory inaccuracies.

A materially inaccurate inventory record, unrecorded production AI system or unauthorized status change is a governance nonconformity and shall be corrected or escalated according to risk. KOMGIS may suspend the affected feature, provider integration or AI tool until required records and controls are complete.

32. Document Review and Continual Improvement

This inventory standard shall be reviewed at least annually and additionally when KOMGIS changes its AI governance framework, introduces materially new AI capabilities, changes its risk methodology, adopts significant new model or agent architectures, or identifies inventory gaps through incident, audit or management review.

Inventory fields, status transitions and review frequencies shall be updated when operational evidence shows that the register does not adequately support ownership, traceability, risk management, incident response or portfolio oversight.

Questions about inventory interpretation shall be escalated to AI Governance / Technical Leadership and, where legal or regulatory interpretation is required, to qualified legal or compliance review.

Appendix A. Mandatory AI System Inventory Data Dictionary

The following data dictionary defines the minimum fields for KOMGIS inventory records. Fields may be implemented in a spreadsheet, database, governance platform or other controlled record system, provided the required meaning and lifecycle controls are preserved.

ID	Field	Group	Applicability	Definition
A01	Inventory ID	Identity	Required	Immutable unique AI system identifier.
A02	System name	Identity	Required	Approved human-readable system name.
A03	System version	Identity	Required	Current governed production or release version.

ID	Field	Group	Applicability	Definition
A04	Record version	Identity	Required	Version of the inventory record.
A05	Business unit / portfolio	Identity	Required	Owning KOMGIS team or product portfolio.
A06	Client / tenant scope	Identity	Required	Internal, single-client or multi-client scope.
A07	AI system owner	Ownership	Required	Accountable business owner.
A08	Technical owner	Ownership	Required	Accountable technical owner.
A09	Security / privacy reviewer	Ownership	As applicable	Reviewer for data and security risk.
A10	Monitoring owner	Ownership	Required in production	Owner receiving operational signals.
A11	Intended purpose	Purpose	Required	Specific approved use statement.
A12	Business process	Purpose	Required	Workflow or process supported.
A13	Primary users	Purpose	Required	Authorized expected users.
A14	Affected parties	Purpose	As applicable	Persons or organizations materially affected.
A15	Approved outputs / actions	Purpose	Required	What the system may produce or perform.
A16	Use boundaries / exclusions	Purpose	Required	Material uses not approved.
A17	Deployment context	Purpose	Required	Internal, client-facing, API, batch, agent or embedded.
A18	KOMGIS assessed legal role	Regulatory	Where relevant	Provider, deployer or other assessed role.
A19	Regulatory review status	Regulatory	Required	Assessment status and reference.
A20	Internal risk level	Risk	Required	Low, Limited, High or Critical.
A21	Risk rationale	Risk	Required	Short classification rationale.
A22	Risk assessment reference	Risk	Required by risk level	Authoritative risk/impact assessment.
A23	Residual-risk status	Risk	Required by risk level	Open, treated, accepted or blocked.
A24	Architecture summary	Technical	Required	System boundary and major components.
A25	Deployment environment / region	Technical	Required	Hosting context and processing location.
A26	Authentication source	Technical	Required in controlled systems	Identity mechanism.
A27	Authorization / isolation summary	Technical	Required with client data	Backend and tenant/object authorization controls.
A28	Model components	Models	Required	Active models and purposes.
A29	Model providers	Models	Required if third party used	Approved providers.
A30	Model / provider approval reference	Models	Required by risk	Provider or vendor approval evidence.
A31	Prompt / workflow version	Behavior	Required when material	Governed behavior version.
A32	Agentic capability	Behavior	Required	No agent / constrained agent / other scope.
A33	Read tools	Tools	As applicable	Approved read capabilities.
A34	Write tools	Tools	As applicable	Approved write capabilities.
A35	Sensitive actions	Tools	As applicable	Actions requiring human approval.
A36	Data categories processed	Data	Required	Source, input, output and derived data categories.

ID	Field	Group	Applicability	Definition
A37	Personal / confidential data	Data	Required	Sensitivity classification.
A38	Data Processing Map reference	Data	Required by scope	Authoritative processing record.
A39	RAG sources	RAG	As applicable	Authorized source families.
A40	Authorization hierarchy / retrieval filter	RAG	Required for RAG	Permission model enforced before prompt.
A41	Vector / retrieval store	RAG	As applicable	Vector or hybrid retrieval service.
A42	Citation / source traceability	RAG	As applicable	Source identifier mechanism.
A43	Integrations / subprocessors	Dependencies	As applicable	Material external services.
A44	Human oversight model	Oversight	Required	Review and approval design.
A45	Reviewer role / approval gate	Oversight	As applicable	Reviewer and server-side blocking mechanism.
A46	Evaluation status	Evidence	Required before production	Current pre-deployment or ongoing evaluation status.
A47	Evaluation / test references	Evidence	Required by risk	Authoritative evidence.
A48	Monitoring plan / owner	Operations	Required in production	Signals, cadence and owner.
A49	Incident response linkage	Operations	Required	Incident route and system identifier.
A50	Operational status	Operations	Required	Current controlled lifecycle state.
A51	Production authorization	Operations	Required	Yes, no or conditional, with approver.
A52	Restrictions / conditions	Operations	As applicable	Temporary or permanent operating conditions.
A53	Retention / deletion reference	Lifecycle	Required with governed data	Data lifecycle rules.
A54	Disable / rollback mechanism	Lifecycle	Required in production	Control used to stop or isolate AI capability.
A55	Last reviewed / next review	Lifecycle	Required	Inventory recertification dates.
A56	Material change / release reference	Lifecycle	As applicable	Latest significant change.
A57	Retirement date / closure evidence	Lifecycle	On retirement	Shutdown and record closure information.

Appendix B. AI System Inventory Record Template

Use the following structure for an individual AI system record. The template is intentionally detailed; fields may be represented as structured database fields when the inventory is implemented in software.

B.1 System identity and ownership

Field	Value
Inventory ID	_____
System name	_____
System version	_____
Record version	_____
Business unit / portfolio	_____

Field	Value
Client / tenant scope	_____
Parent / related system	_____
AI system owner	_____
Technical owner	_____
Security / privacy reviewer	_____
Monitoring owner	_____
Created date	_____
Last reviewed / next review	_____

B.2 Intended purpose and use context

Field	Value / description
Intended purpose	_____ —
Business process supported	_____ —
Primary users	_____ —
Secondary users / affected parties	_____ —
Input types	_____ —
Approved outputs / actions	_____ —
Advisory / draft / reviewed / automated	_____ —
Approved uses	_____ —
Use boundaries / exclusions	_____ —
Deployment context and scale	_____ —

B.3 Risk and regulatory assessment

Field	Value
KOMGIS assessed legal role	_____
Jurisdiction / market	_____
Regulatory review status	_____

Field	Value
Potential restricted / high-risk signal	_____
Internal risk level	Low / Limited / High / Critical
Risk rationale	_____ —
Risk / impact assessment reference	_____
Residual-risk status / acceptance owner	_____

B.4 Technical, model and behavior configuration

Field	Value / linked register
Architecture summary / diagram	_____ —
Deployment environment / hosting	_____ —
Processing region / residency controls	_____ —
Authentication source	_____ —
Authorization / tenant isolation	_____ —
Model components / provider register	_____ —
Prompt / workflow version	_____ —
Agentic capability / autonomy scope	_____ —
Read tools	_____ —
Write tools / sensitive actions	_____ —
Disable / rollback mechanism	_____ —

B.5 Data, RAG and providers

Field	Value / linked register
Data categories processed	_____ —
Personal / confidential / regulated data	_____ —
Data Processing Map reference	_____ —

Field	Value / linked register
RAG sources / authorization hierarchy	_____ —
Retrieval filter / isolation control	_____ —
Vector / retrieval store	_____ —
Citation / source traceability	_____ —
Integrations / subprocessors	_____ —
Retention / deletion reference	_____ —

B.6 Oversight, evidence and operational status

Field	Value / reference
Human oversight model	_____ —
Reviewer role / approval gate	_____ —
Evaluation status	Not started / In progress / Passed / Passed with limitations / Failed / N/A
Evaluation / testing references	_____ —
Monitoring plan / alert owner	_____ —
Incident response linkage	_____ —
Operational status	_____ —
Production authorization	No / Yes / Conditional
Approval owner / date	_____ —
Restrictions / operating conditions	_____ —
Latest material change / release	_____ —
Open incidents / corrective actions	_____ —

Appendix C. Model and Model Provider Subregister Template

Create one row for each material production model component. Where a shared model gateway is used, identify the gateway and the actual model or governed route used by the system.

Model ID	Purpose	Provider / product	Exact model / deployment	Hosting / region	Data / retention setting	Approval / eval ref	Status
MOD-___	Generation / reasoning / embedding / other	_____	_____	_____	_____	_____	Active / fallback / disabled
MOD-___	_____	_____	_____	_____	_____	_____	_____
MOD-___	_____	_____	_____	_____	_____	_____	_____

Additional model notes shall record alias/version handling, fallback logic, training or service-improvement terms, evaluation baseline and change-control trigger when the provider changes the model behind an alias.

Appendix D. Data, RAG Source and Vector Store Register Template

Use this subregister for material data categories and knowledge sources. A RAG source row shall identify permission enforcement before prompt construction.

Source / data ID	Category / source	Owner / tenant	Sensitivity	Purpose	Authorization / retrieval filter	Store / region	Retention / deletion	Evidence
DATA-___	_____	_____	_____	_____	_____	_____	_____	_____
RAG-___	_____	_____	_____	_____	_____	_____	_____	_____
VEC-___	_____	_____	_____	_____	_____	_____	_____	_____

For document intelligence platforms, record the application authorization hierarchy - for example Project -> Field -> Section -> Document or another client-defined hierarchy - and the metadata filters or backend checks that enforce the same scope during retrieval.

Appendix E. Agent Tool and Integration Register Template

Tool ID	Tool / integration	Purpose	Read / write	Data accessed	Credential / scope owner	Sensitive action?	Approval gate	Rate / export control	Disable method
TOOL-___	_____	_____	Read / write	_____	_____	Yes / no	_____	_____	_____
TOOL-___	_____	_____	Read / write	_____	_____	Yes / no	_____	_____	_____
TOOL-___	_____	_____	Read / write	_____	_____	Yes / no	_____	_____	_____

Tool register rule

Tools shall be individually identifiable and least-privilege scoped. The inventory must not use “all company tools,” “admin API” or “general system access” as acceptable tool descriptions for an agent.

Appendix F. Operational Status Matrix and Transition Gates

Status	Meaning	Minimum gate / record condition	Normal next state
Proposed	Use case identified	Inventory ID, provisional owner, purpose hypothesis	Assessment
Assessment	Purpose, role, data and risk under review	Intended purpose, users, preliminary architecture/data, risk screening	Development / blocked / closed

Status	Meaning	Minimum gate / record condition	Normal next state
Development	Controlled non-production build	Named owners, system boundary, initial risk and data records	Testing
Testing	Evaluation and control verification	Required tests, provider review, oversight design, blocking defects resolved	Pilot / Approved for production / Development
Pilot / restricted	Limited real operation under conditions	Defined client/users/data/volume, monitoring, rollback, enhanced review	Approved production / Restricted / Suspended / Retired
Approved for production	Governance gates passed; activation authorized	Release approval, residual risk acceptance, monitoring and incident route	Active production
Active production	Operating for approved purpose	Current inventory, monitoring and scheduled review	Restricted / Suspended / Deprecated
Restricted	Operating with temporary limitations	Restriction owner, reason, controls, review date	Active / Suspended / Deprecated
Suspended / incident containment	Normal use stopped	Containment, evidence preservation, incident owner	Restricted / Active after reactivation approval / Retired
Deprecated	Transition-only operation	Migration plan, no expansion, retirement owner/date	Retired
Retired	Capability disabled and use ended	Shutdown, credential, data and open-action closure	Archived record
Archived record	Lifecycle closed	Final record integrity and retention	Closed

Appendix G. Risk-Based Review and Evidence Matrix

Control / evidence	Low	Limited	High	Critical
AI System Inventory	Required	Required	Required	Required
Named system and technical owners	Required	Required	Required	Required
Intended purpose and boundaries	Required	Required	Formal	Formal
Risk classification	Required	Required	Required	Required
AI Risk Assessment	Basic / as needed	Required	Formal and approved	Formal and approved
AI Impact Assessment	Usually not required	Case-by-case	Required where people / important decisions materially affected	Required where applicable
Data Processing Map	If client / personal data	Required	Required	Required
Model / provider review	If provider used	Required	Formal	Formal / enhanced
RAG isolation evidence	If RAG used	Required	Formal	Formal / enhanced
Human oversight record	Not normally	Sensitive actions	Required	Required
Evaluation and testing record	Basic	Required	Formal	Formal / enhanced
Security review	Basic	Required	Formal	Formal / enhanced
Monitoring plan	Basic	Required	Formal	Enhanced
Management risk acceptance	Not normally	As needed	Required	Required
Periodic inventory review	At least annual	At least annual	At least six months	Management-defined enhanced cadence

Appendix H. AI Portfolio Summary and Management Dashboard Fields

The following fields may be used to generate a portfolio summary from the controlled inventory. Counts should be derived from current records rather than maintained as separate manual totals.

Dashboard area	Suggested measures / filters
Portfolio size	Total systems; active; proposed; testing; restricted; suspended; deprecated; retired.
Risk	Systems by Low / Limited / High / Critical; overdue risk reviews; unresolved residual-risk actions.
Ownership	Missing owners; owners with multiple high-risk systems; upcoming role transitions.
Models / providers	Systems by provider and model family; shared critical provider dependencies; fallback coverage.
Data	Systems processing personal, confidential or regulated data; cross-region processing; missing Data Processing Maps.
RAG	RAG systems; vector stores; permission hierarchy; overdue isolation tests; citation evaluation status.
Agents / tools	Agentic systems; systems with write tools; sensitive actions; mandatory approval gates.
Evidence	Evaluation passed / conditional / failed; security review status; overdue periodic reviews.
Operations	Active alerts; restricted systems; recent status changes; cost or reliability outliers.
Incidents	Open High / Critical incidents; systems in containment; overdue corrective actions; recurring issue flags.
Lifecycle	Deprecated systems; planned retirement dates; retired systems awaiting archival closure.

Appendix I. Illustrative Enterprise Document Intelligence Inventory Record

Illustrative record only

This example demonstrates the expected level of detail using KOMGIS's enterprise document intelligence / RAG platform concept. Model provider, exact model, hosting region, retention settings, approvals and production status are intentionally marked for confirmation where they have not been established in this document.

Field	Illustrative value
Inventory ID	AI-SYS-EXAMPLE-001
System name	KOMGIS Enterprise Document Intelligence Platform
System owner	[Named product / business owner - to be assigned]
Technical owner	[Named technical owner - to be assigned]
Intended purpose	Allow authorized employees to ask questions about enterprise documents they are permitted to access and receive source-grounded answers with inline citations.
Business process	Internal enterprise information retrieval and document-assisted knowledge work.

Field	Illustrative value
Primary users	Authenticated client employees and authorized client administrators.
Use boundaries	Not approved to make legal, employment, credit, insurance, health or other consequential decisions; not approved to access documents outside the authenticated user's permissions.
Deployment context	Client-facing enterprise application; multi-tenant capability with client and department-aware access control.
Internal risk	Limited - illustrative preliminary classification because the system is client-facing, processes confidential client documents and uses RAG. Formal classification must be confirmed for each deployment and expanded capability.
Architecture summary	Authenticated application -> backend authorization -> permission-filtered retrieval -> selected document chunks -> model generation -> response validation / citations -> user interface.
Authorization hierarchy	Project -> Field -> Section -> Document, with client and department-aware access control; actual hierarchy may be client-defined.
RAG control	Tenant, user and document permission filtering must occur before retrieved content is added to the model context.
Citations	Inline source references back to authorized documents and relevant source locations.
Models	[Generation model and embedding model - exact provider/model to be confirmed in Model Subregister]
Data categories	Account/workspace data, client documents, extracted text, chunks, prompts, retrieved context, outputs, embeddings/vector metadata, audit metadata and support records.
Personal/confidential data	Confidential client data expected; personal data possible depending on client document content. Data Processing Map required.
Agent / tools	Document retrieval and read-oriented information assistance. Any future write tools or autonomous actions require a material-change review.
Human oversight	Users verify answers against displayed citations. Sensitive downstream decisions remain with authorized human process owners.
Evaluation	Required: retrieval permission tests, tenant isolation, citation correctness, faithfulness / hallucination evaluation, prompt injection and malicious-document tests.
Monitoring	Wrong-client references, unexpected retrieval sources, citation failures, reviewer/user rejection signals, prompt injection attempts, latency and provider errors.
Operational status	Illustrative / not a production authorization record.
Production authorization	No - this appendix is an example only.
Required linked records	Risk Assessment, Data Processing Map, Model Provider / Vendor records, RAG security evidence, Evaluation and Testing Record, Monitoring Plan and Incident Response linkage.

Appendix J. Inventory Review Checklist

#	Review item	Complete / Evidence
1	The system has a unique Inventory ID and current system name.	☐ _____
2	A named AI system owner is assigned and active.	☐ _____
3	A named technical owner is assigned and active.	☐ _____
4	The intended purpose describes task, users, process, inputs and expected output/action.	☐ _____
5	Approved use boundaries and material exclusions are documented.	☐ _____
6	Expected users and materially affected parties are identified.	☐ _____

#	Review item	Complete / Evidence
7	Deployment context and client / tenant scope are accurate.	☐ _____
8	KOMGIS's assessed legal role is recorded where relevant.	☐ _____
9	Regulatory classification review status and escalation references are current.	☐ _____
10	The internal risk classification is approved and the rationale is current.	☐ _____
11	The linked risk / impact assessment matches the current system.	☐ _____
12	Architecture summary and system boundary match production.	☐ _____
13	Hosting environment and processing region are current.	☐ _____
14	Authentication and backend authorization controls are identified.	☐ _____
15	Tenant and client isolation mechanisms are described and tested as required.	☐ _____
16	All material model components are listed.	☐ _____
17	Model providers and approval references are current.	☐ _____
18	Exact model / deployment identifiers are identifiable where available.	☐ _____
19	Prompt / workflow versions are identifiable for material behavior.	☐ _____
20	Agent autonomy and tool scope are accurately recorded.	☐ _____
21	Read and write tools are individually listed.	☐ _____
22	Sensitive actions and human approval gates are identified.	☐ _____
23	Data categories processed are accurate and sufficiently specific.	☐ _____
24	Personal, confidential and regulated data exposure is recorded.	☐ _____
25	The Data Processing Map is linked where required.	☐ _____
26	RAG sources and authorization hierarchy are current.	☐ _____
27	Retrieval permissions are enforced before prompt construction.	☐ _____
28	Vector store, embedding model and deletion propagation are recorded.	☐ _____
29	Citation / source traceability is documented for document-grounded answers.	☐ _____
30	Material integrations, vendors and subprocessors are listed.	☐ _____
31	Human oversight roles, evidence and reviewer authority are defined.	☐ _____
32	Evaluation and testing status is current and linked to evidence.	☐ _____
33	Blocking security or isolation defects are resolved before production.	☐ _____
34	Monitoring signals, alert owner and review cadence are defined.	☐ _____
35	Incident response linkage and disable / rollback controls are ready.	☐ _____
36	Operational status accurately reflects real use.	☐ _____
37	Production authorization, approver and conditions are current.	☐ _____
38	Retention and deletion rules cover source and derived AI data.	☐ _____
39	Material changes since the previous review are recorded.	☐ _____
40	Open incidents, nonconformities and corrective actions are linked.	☐ _____
41	The next inventory review date is assigned.	☐ _____

#	Review item	Complete / Evidence
42	Deprecated or retired systems have a transition or closure plan.	☐ _____

Appendix K. Material Change Trigger Matrix

Change trigger	Inventory fields to review	Common linked reviews
New intended purpose	Purpose, users, outputs, boundaries, status	Risk / impact, regulatory classification, evaluation, client approval
New user or affected population	Users, affected parties, scale, oversight	Impact, transparency, training, privacy
New model provider / family	Models, provider, region, retention, status	Vendor, privacy, security, evaluation, continuity
New data category	Data, sensitivity, provider exposure, retention	Data Processing Map, privacy, risk, client requirements
New RAG source	Source register, permissions, vector store, citations	RAG security, isolation tests, deletion tests, evaluation
Authorization hierarchy change	Architecture, tenant/object controls, retrieval filters	Security review, tenant-isolation tests
New write tool / external action	Tool register, autonomy, sensitive action, approval	Risk, security, human oversight, agent testing
Human approval removed or reduced	Oversight model, status, risk	Formal risk/impact review, management approval
Processing region change	Hosting / region, residency, providers	Privacy, contract, vendor, client review
Prompt / workflow behavior change	Prompt/workflow version, intended output, tools	Evaluation, injection tests, change approval
Significant performance degradation	Evaluation, monitoring, status, restrictions	Risk update, incident / nonconformity review
High or Critical incident	Status, incidents, risk, controls, reactivation	Incident response, corrective action, retesting, management review

Appendix L. Alignment and Reference Documents

This document is designed as the detailed inventory and intended-purpose companion to the KOMGIS Responsible AI and AI Management Policy. The alignment table is a governance design overview and is not a certification or legal-compliance statement.

Inventory area	KOMGIS governance purpose	Management-system / regulatory theme
System identity and ownership	Named accountability and controlled system boundary	Roles, authorities, documented information and quality-management accountability
Intended purpose and use boundaries	Purpose limitation and evaluation context	Intended purpose, scope, risk management and technical documentation
Models and providers	Model traceability and supply-chain governance	Provider / supplier governance, records and change control
Data and RAG sources	Data minimization, client isolation and source traceability	Data governance, privacy, cybersecurity and traceability
Risk and regulatory assessment	Separate internal operational risk from legal classification	Risk-based governance and applicability analysis

Inventory area	KOMGIS governance purpose	Management-system / regulatory theme
Human oversight	Define reviewer role, authority and approval gates	Human oversight, competence and accountability
Evaluation and testing	Evidence that the system meets intended-purpose and control criteria	Performance evaluation, accuracy, robustness and cybersecurity
Operational status	Prevent unauthorized production use and control reactivation	Operational control, post-deployment monitoring and incident handling
Change and retirement	Maintain current records throughout lifecycle	Documented change control, continual improvement and lifecycle management

Reference Documents

- KOMGIS Responsible AI and AI Management Policy - company-wide governance policy requiring inventory, intended-purpose, ownership, risk and lifecycle records.
- KOMGIS AI Security Policy - access control, prompt injection, RAG, agent tool, secret, output and secure-development controls.
- KOMGIS Data Privacy Policy - client data, AI inputs and outputs, embeddings, providers, retention, deletion and data-request requirements.
- KOMGIS AI Incident Response Plan - AI incident severity, containment, investigation, communication, corrective action and reactivation.
- KOMGIS AI Risk Assessment / Impact Assessment - system-specific known and foreseeable risks, affected parties, controls and residual risk.
- KOMGIS Model Provider Disclosure / Vendor and Subprocessor List - approved AI, cloud and processing dependencies.
- KOMGIS Human Oversight Record - review and approval of sensitive AI outputs or actions.
- KOMGIS Evaluation and Testing Records - pre-deployment and ongoing quality, security and safety evidence.
- ISO/IEC 42001:2023 - Information technology - Artificial intelligence - Management system.
- Regulation (EU) 2024/1689 of the European Parliament and of the Council - Artificial Intelligence Act.