



FRONTIER PUBLICATION / GOVERNANCE & ASSURANCE

Governance and Responsible Intelligence Framework

The public framework governing evidence, human authority, responsible systems, client boundaries and commercial claims.

FIG-PUB-GOV-01

Edition 1.1

Effective 20 October 2026

Public document

SECTION 00

Framework purpose

This is the public expression of how Frontier intends responsible commercial intelligence to be directed, challenged and held accountable.

The framework applies to research, monitoring, analysis, client delivery, public publishing and the use of specialist systems. It establishes the principles that should be visible in the design of work and the records created during delivery.

Frontier is human-directed. Systems can increase reach and consistency; people retain authority for purpose, judgement, approval, client representation and consequence.

DOCUMENT	POSITION
Reference	FIG-PUB-GOV-01
Status	Public · controlled publication
Edition	1.1
Effective date	20 October 2026
Owner	Frontier governance
Review	At least annually, and sooner after a material change in law, regulation, technology, risk, service design or public claims.

Framework map

01	Accountability Who owns the purpose, decision and consequence.
02	Responsible intelligence How evidence becomes a bounded commercial conclusion.
03	Privacy and information How personal, client and confidential information is governed.
04	Security and resilience How risk is considered across the information lifecycle.
05	Human-directed systems Where systems support work and where people must decide.
06	Publication and claims How public authority is supported without overstating evidence.
07	Review and improvement How issues, change and learning alter the control environment.

SECTION 01

Accountability and authority

Every material programme should have an accountable owner, a defined purpose and a clear route for challenge.

Governance begins before tools or data are selected. Frontier defines the business question, the people authorised to decide, the information boundary and the consequence of getting the work wrong. Responsibility is not transferred to a workflow, model, supplier or source.

Accountability model

ROLE	ACCOUNTABILITY
Company governance	Sets the public standards, legal position, risk boundaries and escalation expectations.
Programme owner	Owns the commissioned purpose, service design, resources, client relationship and material exceptions.
Evidence reviewer	Challenges provenance, currency, contradiction, confidence and the limits of the conclusion.
Decision owner	Approves priority, client-facing conclusions and any material external action.
Publication reviewer	Checks accuracy, fairness, sourcing, legal risk, clarity and claim boundaries before release.

Segregation of duties

Not every activity requires a different person, particularly in a smaller operating environment. The control objective is that consequential work receives a second view, an explicit approval or a recorded challenge proportionate to the risk. The person or system producing an output should not silently grant it authority.

Escalation

A material privacy, security, legal, client, evidence or reputation concern is escalated to the owner able to decide the response. Where the available authority or evidence is insufficient, work is paused or narrowed rather than allowed to progress by default.

SECTION 02

Responsible commercial intelligence

The objective is not to produce more signals. It is to give a client a better basis for deciding where to focus, where to wait and where not to act.

Frontier’s evidence discipline separates observation, interpretation, assumption and unanswered question. Relevance is tested against client context. Timing is investigated through connected commercial, operational, financial, access and supplier factors. A conclusion remains proportionate to the evidence available.

The decision path

STAGE	CONTROL QUESTION
Observe	What has changed, and what is the original source?
Connect	Which other facts, pressures or dependencies alter the meaning?
Test	What evidence contradicts the first interpretation?
Qualify	Does this matter to the client’s fit, timing, access and capacity?
Decide	What action, pause, monitoring position or rejection is justified?
Learn	What happened next, and what should change in the method?

Refusal is a feature

Responsible intelligence must be able to conclude that evidence is too weak, timing is wrong, access is absent, fit is poor or the client should stop. A system that only manufactures reasons to proceed is not a decision system.

A page view is not procurement intent. A leadership change is not a budget. A funding announcement is not a funded project. Each may justify investigation; none justifies an unsupported conclusion.

SECTION 03

Privacy, confidentiality and information governance

Useful intelligence must remain compatible with the rights of individuals and the obligations owed to clients, sources and professional partners.

Frontier applies purpose limitation, data minimisation, accuracy, storage limitation, security and accountability to personal information. Public availability does not automatically remove the duty to use information fairly or explain relevant processing. Personal information is handled under an identified lawful basis and with safeguards proportionate to the context.

Information classes

CLASS	GOVERNANCE POSITION
Public evidence	Source, licence or permitted use, date, provenance and relevant access restrictions remain reviewable.
Professional contact information	Used for defined business purposes with transparency, relevance checks and an effective objection or opt-out route.
Client information	Used within the commissioned boundary, with agreed access, delivery, retention and exit arrangements.
Confidential information	Restricted to authorised purposes and protected from unauthorised disclosure during and after the relationship.
Sensitive or high-risk information	Avoided unless necessary, lawful, proportionate and supported by additional controls.

Data rights

Requests and objections can be directed to privacy@frontierinsightgroup.co.uk. Frontier verifies identity where appropriate, records the request and responds within the legal timeframe. Rights are not absolute in every circumstance; any restriction or refusal will be explained with the available complaint route.

Professional transparency

Where Frontier uses professional information obtained from public or third-party sources, it provides clear information about its identity, purposes, categories, source types, lawful basis, sharing, retention and rights. Direct marketing is governed separately from research and client delivery, with suppression and objection controls applied as required.

SECTION 04

Information security and resilience

Security is treated as a lifecycle discipline: understand the information, reduce exposure, control access, detect problems and recover responsibly.

Frontier’s approach is proportionate to the information, the service and the likely impact of loss, alteration, unavailability or unauthorised disclosure. No public statement is intended to imply a certification or guarantee that risk has been eliminated.

Lifecycle controls

LIFECYCLE	CONTROL INTENT
Collect	Use necessary information from appropriate sources for a defined purpose.
Store	Apply suitable protection, separation and access restrictions.
Use	Limit processing to authorised people, services and purposes.
Share	Use approved routes, appropriate recipients and the minimum necessary content.
Monitor	Review material access, change, exception and service risk.
Respond	Contain, assess, record, notify and remediate an incident in proportion to its impact.
Retain or dispose	Keep information only while necessary and dispose of it through an appropriate controlled route.

Resilience and continuity

A programme identifies critical services, information, people and handovers. Source failure, service interruption and personnel absence are considered in the design. Recovery prioritises protection of information, restoration of the most important client function and an accurate record of what changed.

Incidents

Suspected incidents are recorded and assessed. The response considers containment, evidence preservation, affected people and clients, legal or contractual notification, correction and lessons. Public disclosure is managed lawfully and does not compromise affected parties or the security response.

SECTION 05

Human-directed systems

Frontier uses specialist systems to reduce avoidable effort and improve consistency while keeping authority with accountable people.

Systems may support discovery, extraction, comparison, structuring, monitoring, drafting and quality checks. Their role is bounded by the purpose, the information allowed, the consequence of error and the level of human review required.

Control model

SYSTEMS MAY	SYSTEMS MAY NOT
Collect and organise relevant evidence within an approved scope.	Invent a source, conceal uncertainty or turn an inference into a fact.
Compare records and surface contradiction or missing information.	Approve their own output for consequential client or external use.
Prepare a draft classification or explanation for review.	Represent an organisation, person or buyer intention without authority.
Monitor defined changes and notify an accountable owner.	Expand the purpose or information boundary without approval.
Create an auditable record of the work performed.	Replace legal, commercial or professional judgement where that judgement is required.

Model and service change

A material change in a supporting service, model, data source or access route is reviewed for effect on accuracy, privacy, security, continuity and contractual commitments. Where the change could alter a material output, the affected workflow is tested or restricted before normal use resumes.

Client transparency

Frontier explains the role of specialist systems at the level needed to understand the service and its risks. It does not expose the operating stack as a substitute for explaining outcomes, nor publish protective detail that would weaken security.

SECTION 06

Publication, authority and commercial claims

Publishing should help a reader understand a problem and its commercial consequence, without disguising promotion as evidence.

Substantive Frontier publications identify their scope, evidence basis, limitations, publication date and revision position. Sources are selected for relevance and authority; primary and official material is preferred where it can answer the question. Facts, interpretation and Frontier's judgement remain distinguishable.

Publication review

- Is the central claim supported by the cited evidence?
- Are material dates, entities, definitions and comparisons correct?
- Are conflicting facts and reasonable limitations visible?
- Does the headline match the evidence rather than amplify it?
- Could the publication unfairly identify, misrepresent or harm a person or organisation?
- Does any client, confidential, licensed or personal information require authority, restriction or removal?
- Is the commercial implication clear without presenting speculation as certainty?

Claims about Frontier

A case study, outcome statement, certification, client name, audience measure or service claim is published only at the level supported by evidence and authority. Illustrative work is labelled as illustrative. Associated movement is not presented as caused by Frontier. Where independent assurance is absent, it is not implied through visual language or ambiguous wording.

SECTION 07

Review, challenge and continuous improvement

The framework is maintained through operating evidence, not treated as a statement that becomes true merely because it is published.

Issues, near misses, objections, client feedback, corrections, service changes and outcome evidence are inputs to improvement. Material lessons alter the relevant instructions, review gates, training, service design or public wording. A change should identify its owner and the records or outputs that may be affected.

Review triggers

TRIGGER	EXPECTED RESPONSE
Legal or regulatory change	Assess affected processing, terms, publications and operating instructions.
New service or material workflow	Define purpose, information, authority, risk and assurance before launch.
Material incident or control failure	Contain, investigate, correct, notify where required and record lessons.
Significant supplier or source change	Reassess reliability, access, privacy, security, continuity and claim impact.
Client or individual challenge	Review the specific record and the wider control where the issue may recur.
Evidence of a better method	Test the change and update the controlled standard if it improves the outcome.

Corrections and revisions

A material public error is corrected transparently. The current version, effective date and the nature of a substantive revision should be identifiable. A silent edit is not used where it would conceal a material change in meaning or accountability.

The test is practical: can a reasonable client see who decided, what evidence supported the decision, what remained uncertain and what changed after the result?

SECTION FINAL

Accountability and contact

Questions should reach the person responsible for the subject, not disappear into a general inbox.

Privacy and individual rights

Write to privacy@frontierinsightgroup.co.uk for privacy questions, data-rights requests, objections and complaints.

Client assurance and due diligence

Write to assurance@frontierinsightgroup.co.uk for assurance enquiries, security questionnaires, control evidence and procurement review.

Legal and contractual notices

Write to legal@frontierinsightgroup.co.uk for formal legal and contractual correspondence. Notices may also be sent to the registered office where appropriate.

CORPORATE PARTICULAR	INFORMATION
Registered company name	FRONTIER INSIGHT GROUP LIMITED
Company number	17529472
ICO registration	ZC279086
Place of registration	England and Wales
Registered office	71–75 Shelton Street, Covent Garden, London, WC2H 9JQ, United Kingdom
Website	frontierinsightgroup.co.uk

A public document explains the control position. It does not expose credentials, client-confidential material, security architecture or internal playbooks. Supporting evidence may be reviewed through an appropriate due-diligence process and, where necessary, under confidentiality.

Current versions

The current public suite is maintained at <https://frontierinsightgroup.co.uk/governance/>. A printed or downloaded copy should be checked against that page before it is relied upon.