CORPORATE WHITE PAPER

Designed for Australian Accountability

How Australian legislation informs Songlines—and what that means for enterprise and government

APPROVED AUTHORITY.
CONFIGURED CONTROL.
REVIEWABLE EVIDENCE.

Cetus AI | Version 1.0
2 November 2026

cetusai.com.au | hello@cetusai.com.au

For boards, executive teams, government accountable officials, technology, privacy, legal, risk and Finance leaders.

General information and implementation guidance. Not legal advice, a compliance determination, regulator endorsement or independent assurance.

Contents

The legislative rationale, the operating design and the customer outcomes.

01 Why Australian obligations shaped Songlines....3
02 An Australian company's design rationale....4
03 Laws, policies and customer-specific applicability....5
04 How obligations become operational design....6
05 Privacy by operational design....8
06 Corporate governance and defensible oversight....10
07 Consumer protection and trustworthy representations....11
08 Public resources, authority and value for money....12
09 Records, transparency and investigation readiness....13
10 Government AI policy and agentic control....14
11 The connected Songlines architecture....15
12 Value Control and the discipline of benefit validation....17
13 Two illustrative customer workflows....18
14 Deployment, validation and customer benefits....19
References and contact....20

Australian legislative obligations informed the design choices. They are not a universal executable rulebook: applicability, legal interpretation, policy approval and operating accountability remain with the customer.

01 / LEGISLATION TO OPERATIONS

Why Australian obligations shaped Songlines

Cetus AI developed Songlines around a practical Australian accountability problem: organisations can adopt AI quickly, while the duties governing the resulting activity remain attached to people and institutions. A model may draft advice, an employee may upload information, or an agent may call a tool. The organisation still needs to establish the purpose, applicable authority, information-handling conditions, oversight and record of what occurred.

Australia already has laws addressing personal information, corporate conduct, consumer representations, public resources and Commonwealth records. These obligations do not become irrelevant because the activity is AI-enabled. Their precise application depends on the entity, transaction, information and facts. Government AI policies and technical guidance add operating expectations, but must be distinguished from legislation. [1] [6] [11] [14] [18] [21] [22]

Cetus AI's design response is to make those accountability questions part of the operating pathway. Songlines connects known AI uses and owners with approved policy, configured decisions, customer enforcement evidence, human review and later value assessment. Its design is additive: existing identity, business, integration, security and Finance systems retain their roles. [27]

This is what it means to say Songlines was developed around Australian legislative obligations. The obligations informed the questions the product must help customers answer, the separation of decision rights, the structure of evidence and the need to maintain a reviewable record. It does not mean the platform interprets every Act, exercises statutory discretion, certifies a customer or makes every action lawful.

The distinction matters commercially. A generic dashboard may show activity without establishing accountability. A policy document may express an intention without showing whether a configured control operated. A token-cost report may show expenditure without demonstrating a useful outcome. Songlines connects these views so the customer can make a better-supported decision about a selected workflow. [27] [29]

> **The design objective is not to automate legal judgement. It is to make approved authority, configured controls, source evidence and accountable decisions connected and reviewable.**

The benefits are relevant to both sectors. A corporation can use the approach to support oversight, customer protection and investment discipline. A government entity can use it to support delegated-authority controls, public-resource decisions and records of administrative activity. Neither use transfers the organisation's responsibilities to Cetus AI.

02 / LEGISLATION TO OPERATIONS

An Australian company's design rationale

Cetus AI is an Australian-owned and operated company based in Queensland. Its product, Songlines, was developed for organisations whose AI activity is distributed across an existing technology estate. The company's approach starts with the customer's operating obligations rather than assuming that every workload must move into a new central platform.

The rationale has three parts. First, organisations need to know what AI is used for and who owns that use. Second, they need to apply approved restrictions to selected actions. Third, they need to connect the evidence supporting those actions with business and public-service outcomes. Songlines brings those requirements together through Teams, Control, the shared Evidence Fabric capability and the integrated Value Control module. [27] [29]

Accountability before automation

A useful AI governance record starts with a defined purpose and an accountable owner. The product's operating model therefore associates a use case with business, technical, data, governance and review roles. A user identity or agent credential is not treated as a substitute for approved authority. The relevant question is what that identity is permitted to do for this purpose under the current conditions.

This reflects the wider Australian accountability setting. Directors and officers have their own statutory duties. Commonwealth accountable authorities have duties concerning governance and public resources. Privacy obligations attach to in-scope entities and their information-handling activities. A technology provider can support these responsibilities, but cannot assume them merely by supplying software. [1] [6] [14]

Control at the point of action

An approved AI policy is useful only if the selected workflow can apply it. Songlines' Policy Decision Point evaluates customer-approved metadata against configured, versioned policy and returns an outcome with reasons and conditions. The customer's application, gateway or orchestrator remains responsible for enforcing that outcome. This separation is central to the architecture. [27] [28]

It enables organisations to add AI-specific control without replacing mature integration and security infrastructure. It also makes the acceptance test explicit: the customer must demonstrate that the returned decision actually results in the required downstream behaviour.

Evidence as a design requirement

Evidence is not an afterthought appended to a dashboard. The selected workflow needs source identifiers, timestamps, policy versions, conditions, review outcomes and action receipts that can be linked. Missing records must remain visible. A correlation result is not silently elevated into legal proof, a security guarantee or a complete account of every event. [28]

The connected-pathway idea is also reflected in the Songlines name: purpose, authority, action, evidence and value should be understandable as related parts of an operating system, not isolated artefacts. This paper discusses the technical design rationale, not a claim of cultural authority or endorsement.

The resulting product is legislation-informed and customer-configured. Its differentiation is the connected operating method, not an assertion that legislation has been permanently encoded into a fixed library of universal answers.

03 / LEGISLATION TO OPERATIONS

Laws, policies and customer-specific applicability

The first design decision is to determine which obligations apply. Australian legislation is not one uniform regime covering every organisation and every AI use in the same way. A private company, a non-corporate Commonwealth entity and a state health service may use similar technology while having different legal and administrative settings.

The legislative foundations

The Privacy Act 1988 contains the Australian Privacy Principles and the Notifiable Data Breaches scheme for entities and activities within its scope. The Corporations Act 2001 includes duties relevant to directors and officers. The Australian Consumer Law, in Schedule 2 to the Competition and Consumer Act 2010, addresses matters including misleading conduct, specified representations and consumer guarantees where applicable. [1] [6] [11]

The Public Governance, Performance and Accountability Act 2013 governs defined Commonwealth institutions and public-resource responsibilities. The Archives Act 1983 and Freedom of Information Act 1982 provide Commonwealth recordkeeping and information-access frameworks. These Commonwealth-specific instruments should not be assumed to apply automatically to state, territory, local-government or private customers. [14] [18] [21]

The same caution applies within corporate markets. Consumer guarantees have statutory scope tests, and financial services can fall under different arrangements. An organisation’s industry, legal status, transaction and data use must be considered before assigning a control to an obligation. [11] [13]

Policy and guidance are different instruments

The Australian Government’s responsible-AI policy, its agentic technical addendum, the Protective Security Policy Framework and the Information Security Manual have different purposes and applicability. They are not interchangeable with Acts. A policy requirement may be mandatory for a covered government entity; technical guidance may describe recommended practice; a framework may guide risk and security control selection. [22] [23] [25] [26]

For example, the responsible-AI policy is mandatory for non-corporate Commonwealth entities within its stated scope, with identified carve-outs. Other entities should assess its relevance rather than being described as automatically subject to every requirement. Corporate customers can adopt useful practices without implying they are covered agencies. [22]

The customer’s applicability record

A customer implementation should record the entity and jurisdiction, the relevant function, the information involved, the applicable instrument and version, and the person responsible for interpretation. It should also identify the selected control and the evidence needed to review its operation.

This is a proposed implementation method, not a claim that Songlines supplies an automatically maintained legal register. Legal and governance owners approve the mapping. Product configuration follows that approved interpretation; it does not create it.

A similar technical control can support different obligations. The customer must establish the legal basis, scope and evidence standard for its own environment.

04 / LEGISLATION TO OPERATIONS

How obligations become operational design

Cetus AI's approach translates legislative-informed questions into an operating sequence: establish applicability, approve the organisational policy, configure the selected path, preserve source evidence and hold an accountable review. Each transition has an owner. The purpose is to connect work already undertaken by legal, governance, architecture, security, records and Finance teams. [27]

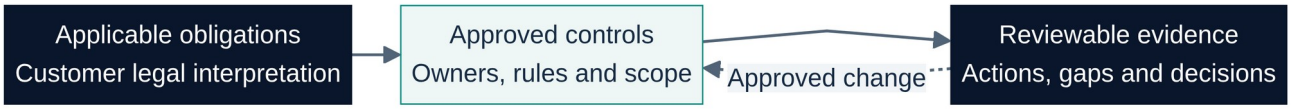


Figure 1. Legislative-informed design pattern: customer interpretation connects applicable obligations to approved controls and reviewable evidence.

Define the obligation and the policy owner

An obligation does not necessarily prescribe a single technical rule. Privacy requirements concerning use and disclosure, for example, depend on purpose, information and permitted pathways. The customer's privacy and legal owners establish that basis before a system can evaluate a configured route. A corporate or public-resource duty likewise requires human judgement about the decision, evidence and circumstances. [1] [6] [14]

The policy owner then approves an operational statement: which identities may use the workflow, what data classes are allowed, which destinations are permitted, when review is required and what happens when a required condition cannot be established.

Specify the attributes and the action boundary

A deterministic decision needs reliable inputs. Typical approved attributes include workflow ID, user or service identity, agent owner, purpose, data classification, requested destination, environment, policy version and review status. The source and quality of each field matter; a value supplied by an untrusted component cannot be treated as authoritative merely because it appears in a request.

The customer defines the point at which an action can create a consequence. It may be the release of an external communication, disclosure to a provider, amendment of a business record or submission of a transaction. Songlines returns the configured policy decision; the customer controls that release point. [27]

Require evidence of the actual outcome

A policy decision, an enforcement action and a business outcome are different records. A returned deny does not independently prove that the action was prevented. A returned allow does not prove that the action succeeded. The selected acceptance test must examine the customer's downstream system, alternative routes and recorded outcome.

Evidence Fabric links the approved records and their identifiers. It can make missing or unmatched evidence visible; it does not invent a receipt when one is absent. This protects the customer from confusing an intended control with an observed result. [28]

Maintain change and exception discipline

Policy versions, data routes, agent permissions and business conditions can change. The implementation should identify which changes require renewed approval, retesting or suspension. A historical approval should not become an indefinite authority to continue under materially different conditions.

Exceptions require an authorised owner, a rationale, conditions, an expiry or review date and evidence of the released action. Some circumstances will not be suitable for an exception. That is a customer policy and legal decision, not an automatic software judgement.

The benefit is a repeatable engineering and operating method. The organisation can review what was approved, what was tested, what actually happened and what must change, without claiming that this record settles every legal question.

05 / LEGISLATION TO OPERATIONS

Privacy by operational design

The Privacy Act is a strong example of why governance must connect organisational practice with technical controls. For an APP entity, APP 1 addresses reasonable practices, procedures and systems and an up-to-date privacy policy. APPs 3 and 5 address collection and notice. APP 6 concerns use and disclosure, APP 8 overseas disclosure, APP 10 information quality and APP 11 protection and lifecycle treatment. Each has its own scope and conditions. [1] [4] [5]

Purpose, information and destination

For a selected AI use, the customer should establish what personal information is necessary, why it is used, who receives it and whether the proposed use is within the approved purpose or another lawful pathway. Customer-approved classification and route metadata can then contribute to a configured policy decision.

Songlines can support a rule requiring a particular destination, restricting a selected data class or holding an action for review. It cannot make collection necessary, obtain consent, create an exception to a statutory restriction or decide the legal basis for an overseas disclosure. Those matters require the customer's approved process and professional judgement.

Data minimisation without false anonymity

The architecture allows metadata-only decisions where the selected use permits. Prompt content need not be transmitted for every policy evaluation. This can reduce unnecessary replication, but metadata may still identify a person. Identity references, timestamps and linked source IDs need their own privacy, access and retention treatment. [27]

Australian hosting also does not settle the full data-flow question. Model providers, support services, subprocessors, logs and remote access may affect the assessment. APP 8 applicability and the relevant safeguards must be examined for the actual arrangement. [4]

Quality, lifecycle and correction

An AI-generated statement may be inaccurate even if a policy check passed. The customer should establish source quality, review and correction requirements appropriate to the intended use. Evidence of those steps can be linked to the final record.

APP 11 protection includes organisational as well as technical measures. Its destruction or de-identification requirements must be assessed with applicable exceptions and other legal retention duties. A universal instruction to keep all AI evidence forever, or to delete every prompt immediately, is not a sound design assumption. [1] [5]

Incident assessment, not automatic breach classification

The Notifiable Data Breaches scheme involves statutory tests concerning unauthorised access, disclosure or qualifying loss and likely serious harm. Reasonable suspicion triggers an expeditious assessment, with all reasonable steps to complete it within 30 days. That timeframe is not a default waiting period. Notification duties depend on the applicable threshold and circumstances. [1] [3]

A scoped incident record can preserve awareness time, source evidence, affected information, remediation and the accountable assessment. An AI-use indicator is not itself proof of a disclosure or eligible data breach. The customer determines the legal assessment and notifications.

Preparing for 10 December 2026

As at 2 November 2026, the additional APP 1.7–1.9 provisions are enacted but not yet operative. They commence on 10 December 2026. Where the statutory tests are met, an APP entity's privacy policy must include specified information about personal-information use and kinds of computer-program decisions and substantially and directly related acts that may significantly affect individuals' rights or interests. [2]

A maintained use-case register and decision-context record can support preparation. They do not automatically produce an adequate privacy policy or create a general right to an explanation of every individual outcome. Legal and privacy owners must determine the required disclosures.

06 / LEGISLATION TO OPERATIONS

Corporate governance and defensible oversight

Sections 180 and 181 of the Corporations Act address care and diligence, good faith and proper purpose for directors and officers. These duties are relevant to the quality of corporate decision-making, but do not make every AI error an automatic contravention. The statutory setting and facts matter. [6]

Songlines supports a practical oversight objective: give accountable leaders a connected view of the AI use, approved policy, material exceptions, evidence gaps, cost basis and proposed action. The product does not substitute a score for board deliberation or determine whether a director has fulfilled a duty.

From tool counts to material decisions

A board may be told how many staff use AI or how much token usage has increased. Those measures do not establish whether material uses have approved owners, suitable data boundaries and adequate review. Teams' known-use and ownership approach helps identify the selected estate and unresolved governance work.

Control and Evidence Fabric add the policy and source context for covered workflows. A board or management report can then distinguish configured coverage from exclusions, intended controls from observed outcomes, and resolved exceptions from outstanding evidence. [27] [28]

The resulting management view should not imply that absence of an alert proves absence of risk. Scope and source completeness must remain visible.

The lesson from ASIC's AI review

ASIC's Report 798 examined governance arrangements in a selected group of Australian financial services and credit licensees. It was a bounded, non-representative review, not a rulebook or a finding about every Australian company. Its relevance here is the need to consider governance arrangements alongside the development and use of AI. [7]

Cetus AI's response is an operating architecture that connects ownership, policy, source evidence and review. A current AI register can support oversight, but it is not enough unless material actions and exceptions can also be examined.

Investment decisions remain human decisions

Value Control connects a selected initiative's baseline, full cost, observed outcome, attribution and Finance review before an accountable portfolio decision. This can improve the basis of management papers and board discussions. It does not supply investment advice, prove causation or determine accounting recognition. [29]

Directors and management still decide what evidence is sufficient, what risks are acceptable and whether the initiative should continue. Reliance and delegation are governed by their own legal and organisational conditions.

Preparing for regulatory enquiries

ASIC can use compulsory information-gathering powers within its remit. The particular notice governs scope, timing and production requirements. Source-linked records and tested retrieval may assist the customer's response, but a governance export is not automatically a compliant production bundle. Legal professional privilege requires separate assessment. [8] [9] [10]

The benefit is more coherent oversight and retrieval, not guaranteed legal defensibility or immunity from an adverse finding.

07 / LEGISLATION TO OPERATIONS

Consumer protection and trustworthy representations

AI can affect the organisation's external conduct through marketing, customer communications, service recommendations, policy explanations and complaints handling. The organisation must consider the applicable consumer-law setting, not just whether the model generated a fluent answer.

Australian Consumer Law section 18 addresses misleading or deceptive conduct in trade or commerce. Section 29 addresses specified false or misleading representations. Section 60 provides a due-care-and-skill guarantee for services where the statutory conditions apply. Financial services and particular transactions may involve different arrangements or exceptions. [11] [13]

Approval must consider the overall impression

A statement can mislead through omissions, qualifications or the overall impression, not only through a plainly false sentence. ACCC guidance emphasises accurate claims and a sound basis for representations. [12]

For a selected customer-communication workflow, the customer may require approved sources, restrictions on unsupported claims and human review before release. Songlines can return the configured hold or condition and link the approval with the released version. It does not independently judge the truth of every claim or the legal effect of a message.

A practical claims-evidence pattern would retain the approved statement, intended audience, evidence source, material assumptions, reviewer, release record and later correction. This is a customer-specific configuration and source-mapping approach, not a preconfigured consumer-law compliance module.

Service quality and remedies

AI assistance does not remove the need for the customer's quality controls. A useful workflow records whether the output was accepted, corrected, rejected or escalated. Where a complaint occurs, the organisation should preserve the complaint, review basis, decision, remedy and closure evidence through its service-management process.

Evidence Fabric can link authorised references from those processes. The customer still owns complaint handling and the legal assessment of rights and remedies. A human approval record does not itself prove the service met every consumer guarantee.

Accurate claims about AI value

The same discipline applies to internal and external statements about an AI investment. Forecast savings, simulated performance and adoption metrics should not be presented as realised customer benefits. Value Control separates those evidence states so that authorised Business and Finance owners can review the basis before a claim is made. [29]

For investigations, ACCC section 155 powers sit in the Competition and Consumer Act itself. They are distinct from ACL substantiation notices under section 219. A customer's response must follow the actual statutory request rather than assuming that one standard export satisfies every enquiry. [11]

The commercial benefit is clearer evidence behind selected representations and service decisions. It is not a guarantee that all AI-generated content is accurate, lawful or free from complaints.

08 / LEGISLATION TO OPERATIONS

Public resources, authority and value for money

Government AI adoption must be examined through the customer's institutional and statutory setting. For Commonwealth entities, the PGPA Act defines proper use and management of public resources in terms of efficiency, effectiveness, economy and ethics. Sections 15 and 16 place governance and risk/internal-control duties with the accountable authority. [14]

This creates a natural connection between AI governance and evidence of purpose, authority, cost, risk and outcome. An AI initiative should not be assessed only by technical capability or the number of licences deployed.

Software permissions are not statutory authority

An agent may possess a token allowing it to call a procurement, finance or administrative API. That technical capability does not establish that a lawful commitment or administrative decision can be made.

The customer must determine the responsible official, governing authority and applicable delegation. Section 23 authority is specifically framed for non-corporate Commonwealth entities, and section 110 delegation has statutory conditions; the general duties in sections 15 and 16 are non-delegable. These provisions should not be generalised to every government organisation. [14]

Songlines can associate configured permissions and action conditions with approved customer authority records. It cannot grant statutory authority to software or determine that a delegation is legally valid. Consequential release points remain subject to the customer's authorised process.

Value for money is more than price

Finance guidance identifies value for money as the core Commonwealth Procurement Rules rule, with reasonable enquiries and financial and non-financial assessment. The applicable procurement record should capture the requirement, evaluation basis, approvals, supplier agreement and decision rationale in proportion to the procurement's scale, scope and risk. [15] [16]

A scoped Songlines evidence pattern can link references to those authoritative records with policy and operational events. Procurement and records systems remain the source of the official decision. The product does not replace the evaluation or certify the result.

Benefits need an accepted comparison basis

A public-service outcome may involve improved timeliness, quality, accessibility or administrative efficiency. A favourable operational measure is not automatically a cash saving. The relevant owners must approve the baseline, measure, attribution, cost treatment and decision basis.

Value Control preserves those distinctions and the current validation state. It can help a programme identify when expansion is supported, when optimisation is required or when evidence is insufficient. It does not determine the customer's public-value priorities or prove a causal benefit. [29]

Outcome-based commercial terms also require a clearly agreed measurement and attribution basis. They do not remove procurement obligations or establish value for money by themselves. Documented due diligence and customer approvals remain necessary. [15] [17]

The intended benefit is more disciplined stewardship of a selected AI programme: a connection between authorised purpose, resources consumed, evidence of outcomes and the decision to continue or change.

09 / LEGISLATION TO OPERATIONS

Records, transparency and investigation readiness

A material AI decision is not fully explained by its final output. The relevant record may also require the approved purpose, information sources, policy version, human judgement, released action and later correction. What must be retained depends on the record's function and legal setting.

For Commonwealth records, section 24 of the Archives Act controls disposal, alteration and certain transfers, subject to the statutory exceptions and authorities. National Archives guidance addresses how AI-created records and supporting context should be managed. It does not require blanket retention of every prompt, output or routine log. [18] [19] [20]

Retain the right record, not every possible payload

The customer should determine which outputs and supporting inputs are needed for business, legal, evidentiary or accountability purposes. Its records authority and approved procedures inform retention and disposal. Evidence Fabric can link the authoritative material and relevant metadata without assuming that all source content should be duplicated into the governance platform.

A metadata-minimised design therefore needs a deliberate records hand-off. If the substantive record must be retained, the customer's recordkeeping system must capture it appropriately. A governance reference that points to material subsequently deleted without authority is not a sufficient substitute.

Preserve correction and source lineage

AI outputs can be corrected, decisions can be reconsidered and source information can change. A reviewable record should distinguish the original from the correction, record the responsible person and preserve the relationship where required.

Configured tamper-evident records can support integrity checks. They do not prove that the original information was true, establish legal admissibility or replace authorised administration, retention and correction controls. [27] [28]

Retrieval and disclosure are different decisions

The FOI Act provides a request-based access framework with exemptions and conditional exemptions. Being able to retrieve an AI-related record does not mean it must be disclosed without assessment. Scope, exemptions, public-interest questions and any edited release remain customer decisions under the applicable framework. [21]

Similarly, legal professional privilege is not created by a confidential label or the presence of a lawyer in an email thread. The customer and its legal advisers assess it separately when responding to a relevant investigation or request. [10]

Make gaps visible before they become urgent

A useful evidence review asks whether the selected event can be reconstructed from the approved sources and whether the material can be retrieved with its context. Missing request IDs, absent review outcomes or inaccessible action receipts should be tracked as issues, not concealed by a clean-looking report.

This is the practical meaning of investigation readiness: knowing what can be retrieved, what remains uncertain and who must resolve the gaps. It is not a guarantee that an investigation will be avoided, that a regulator will accept the record or that the underlying conduct was permissible.

10 / LEGISLATION TO OPERATIONS

Government AI policy and agentic control

Legislation provides part of the accountability setting. Government policy and technical guidance provide additional operating expectations for the entities and activities within their scope.

The responsible-AI policy version 2.0 took effect on 15 December 2025; version 2.1 included minor updates published on 21 October 2026. For covered non-corporate Commonwealth entities, it addresses accountable officials, transparency, strategic and operational arrangements, use-case ownership, registers, training and assessment. These are agency responsibilities, not product certifications. [22]

A maintained register and ownership process

Teams' known-use and ownership approach can support a customer-maintained use-case register. The operating value lies in scope, participation, accountable owners, current review status and unresolved work—not in claiming to discover every AI tool automatically.

Coverage depends on authorised sources and participating populations. Personal devices, accounts or networks cannot be treated as universally visible. A declaration, an observed indicator, a correlated use case and a reviewed status must remain distinct.

Bound authority before introducing more autonomy

The government agentic addendum and ASD guidance describe risk-informed approaches to agentic systems. They support attention to bounded access, least privilege, monitoring, human control and continuing review. They are technical guidance, not a replacement for legal duties or system-specific security design. [23] [24]

A selected Songlines workflow can represent the agent's identity and owner, requested action, permitted purpose, data boundary, review requirement and current policy. The customer validates the source attributes, authorisation and enforcement. If authority or material conditions change, the design should require reevaluation rather than relying indefinitely on yesterday's approval.

More human approvals are not always stronger control. Excessive standing permissions cannot be corrected merely by asking a person to approve every step. The implementation should constrain the permitted action and use human judgement where required by the consequence and policy.

Security and governance must work together

The PSPF and ISM have distinct protective-security and cyber-security roles. The applicable controls, classification, risk treatment and acceptance remain customer-specific. [25] [26]

Songlines does not replace security testing, isolation, identity administration, network controls or incident response. It adds the policy and evidence connection for covered paths. An agent must not be able to bypass that path through direct credentials, alternate endpoints or uncontrolled retries.

> **A configured policy decision is useful only when the customer validates the enforcement boundary, failure behaviour and alternative paths.**

The intended benefit is a governable expansion of selected AI capability, with explicit authority and reviewable evidence. It is not unrestricted autonomy or a promise that all agent behaviour will be safe.

11 / LEGISLATION TO OPERATIONS

The connected Songlines architecture

Cetus AI is the company and enterprise AI governance platform provider. Songlines is the product. Teams and Control are components, Evidence Fabric is a shared evidence capability, and Value Control is an integrated module—not a separate platform. Together they create a connected record across the selected operating boundary. [27] [29]



Figure 2. The connected operating model: product components support an accountable customer decision without taking over that decision.

Teams: establish known use and accountable ownership

Teams helps structure the selected use-case estate, purpose, data context, technical and governance ownership, lifecycle status and unresolved evidence. This creates the starting point for privacy mapping, agency registers, executive reporting and review prioritisation.

Its boundary is equally important. A known-use register is not proof that every use has been found. An observed indicator does not independently establish misconduct or disclosure.

Control: apply approved policy to selected paths

Control evaluates approved attributes against configured policy and returns an outcome, reason and conditions. It does not make policy ownership disappear or interpret legislation on behalf of the customer.

In the metadata-only sidecar pattern, the customer keeps the workload and payload. Its application or integration layer applies the returned deny, hold, route, redact or release behaviour. The specific transformation and release mechanisms must be designed and tested in that environment. [27] [28]

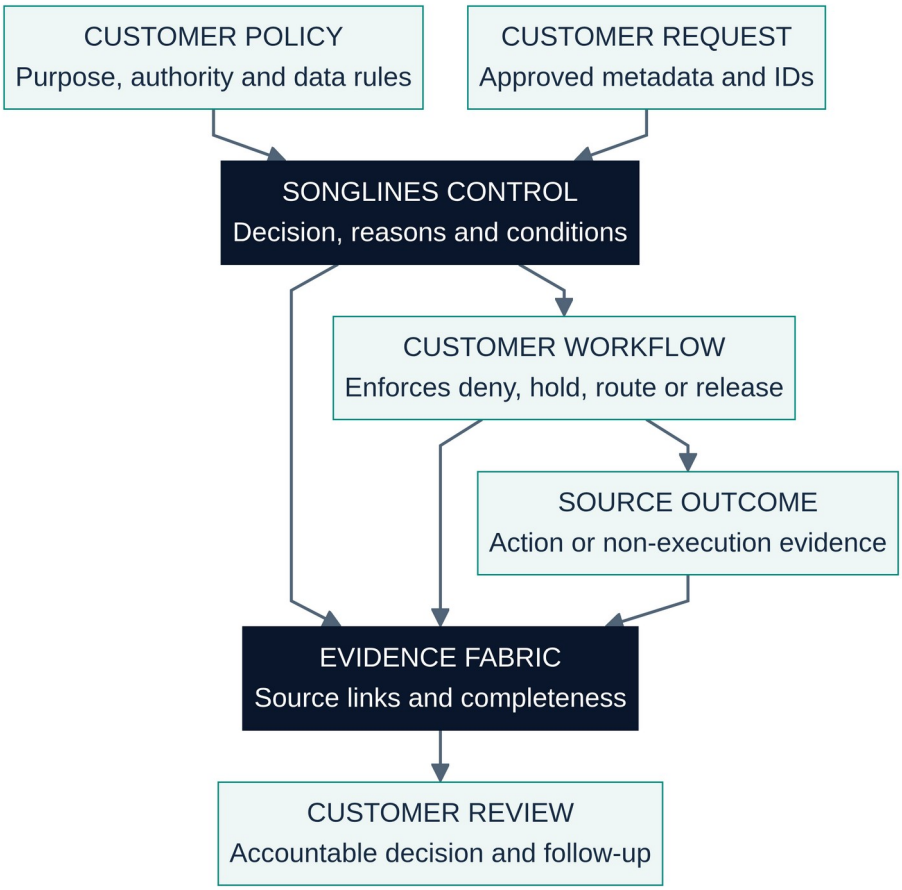


Figure 3. Policy-decision and enforcement boundary: Songlines supplies the decision and evidence linkage; the customer controls execution and validates the source outcome.

Evidence Fabric: connect records and show uncertainty

Evidence Fabric links authorised governance, identity, workflow, model, policy and source references. The evidence contract defines the required fields, identifiers, quality and completeness conditions for the selected review objective. Missing, unmatched or stale records remain visible. [28]

A configured output may include a known-use register, AI Decision Record, policy-decision trace, human-review record or evidence-completeness view. The customer agrees the output's scope, sources and acceptance basis. These are not a regulator-prescribed universal production format.

Value Control: connect evidence with portfolio action

Value Control uses the same ownership and evidence foundations to preserve the baseline, full cost, observed outcome, attribution, Finance review and risk treatment. Its purpose is an accountable Scale, Optimise, Review or Retire decision. [29]

This architecture explains why the legislative-informed design benefits the whole product. Privacy needs purpose and data context; corporate oversight needs ownership and review; public-resource stewardship needs authority and value; recordkeeping needs lineage and retrieval. These are connected requirements, not separate compliance slogans.

12 / LEGISLATION TO OPERATIONS

Value Control and the discipline of benefit validation

AI investment creates an evidence problem as well as a cost problem. Organisations may incur licence, model, implementation, integration, change, human-review and rework costs before they have agreed how success will be measured. An increase in activity can be mistaken for an increase in value.

Value Control preserves five progressive states. Each requires an agreed evidence basis and an accountable review; a calculation does not automatically become a recognised benefit because more data is available. [29]



Figure 4. Progressive value states: advancement requires the customer's defined evidence and approval gates; it is not automatic benefit recognition.

From hypothesis to qualified decision evidence

Forecast records the intended benefit, target, assumptions and owner. **Observed** records a measured operational change against the approved baseline. **Attributed** records an approved contribution method that considers dependencies and alternative causes. **Finance validated** records the authorised Finance review of benefit definition, cost treatment and calculation basis. **Risk adjusted** records the approved uncertainty, correction and governance-risk treatment for the portfolio decision.

These states support different executive questions. Is the business case still plausible? Has the process measure changed? How much of that change can reasonably be attributed to the initiative? Has Finance accepted the internal comparison basis? Does the risk-adjusted evidence support expansion?

Corporate and government applications

For a corporation, the method can strengthen the management record supporting an AI investment decision. For a government programme, it can help connect resource use to approved service outcomes and the evidence informing continuation or change. The business owner determines which outcomes matter; Finance determines the appropriate financial treatment; accountable governance owners determine the action.

A reduction in measured task time is not automatically a reduction in expenditure. A service-quality improvement may have public value without being a cash saving. A cost allocation from FinOps is an input to the review, not evidence that the initiative caused the outcome.

Sources and decisions remain distinct

The architecture can use customer-approved source exports or scoped mappings from existing cost and Finance systems. Named tools or providers are potential sources, not proof of certified native integration. Access, allocation, identifiers, reconciliation and acceptance must be validated for the implementation. [27] [29]

The final decision is recorded by authorised people. Scale expands scope where evidence supports it. Optimise changes the cost, model, workflow or conditions. Review holds the question open while evidence or risk is unresolved. Retire stops or replaces the initiative when the approved basis supports that action.

Value Control does not provide accounting, audit, legal, investment or assurance advice. Its Finance-validation state is an internal governance checkpoint, not an audit opinion, a statutory accounting determination or proof of causation.

13 / LEGISLATION TO OPERATIONS

Two illustrative customer workflows

The following scenarios show how the design can be applied. They are fictional implementation examples, not customer deployments, clinical validation results, quantified savings or evidence of regulatory compliance.

Corporate example: AI-assisted customer communication

A corporate service team proposes using AI to draft responses from approved customer and product information. The organisation first determines the applicable privacy and consumer-law setting, the permitted information use and which statements require review. It assigns a business owner, privacy owner, technical owner and authorised reviewer. [1] [11]

Teams records the use, scope and ownership. The customer configures the application to supply approved workflow, data-class and destination metadata. Control evaluates that request against the approved policy. A restricted data route is denied; a permitted draft can be held until the required reviewer approves its release.

The customer application enforces the outcome. Evidence Fabric links the policy decision, review, released version and source-system receipt. If the release record is absent, the event remains incomplete. If a complaint later concerns the content, the service system holds the substantive complaint and remedy record, with authorised references linked for review.

Value Control then assesses the selected operational measures against an approved baseline. Faster drafting is examined alongside review effort, corrections, quality and full cost. Business and Finance owners determine attribution and the appropriate value state before deciding to scale, optimise, review or retire.

The practical benefit is a connected record of purpose, control, communication and outcome. It does not establish that every generated statement was accurate or that a consumer-law obligation was necessarily met.

Government example: AI-assisted procurement analysis

A fictional Commonwealth team uses AI to summarise authorised procurement material and prepare an evaluation working paper. The use is assistive: the AI does not select the successful supplier, exercise a statutory delegation or enter a commitment.

The agency identifies its applicable procurement and records requirements, official roles, evaluation method and data boundary. Teams records the purpose and owner. Control evaluates whether the configured workflow may use the proposed source and route, and whether the next action requires an authorised official’s review. [14] [15] [16]

The customer system prevents release of a consequential action through this path without the approved review. Evidence Fabric links the source references, policy decision, reviewer rationale and authoritative action receipt. Procurement and recordkeeping systems retain the formal evaluation and approval. Access or disclosure requests are handled under the applicable process, not automatically by the governance record.

Value Control can support an internal assessment of evaluation effort, rework, quality and cost. It does not determine the procurement’s value-for-money conclusion or attribute every improvement to AI.

The intended benefit is an assistive workflow with clearer authority, evidence and resource review. It is not a substitute for the official evaluation or a claim that software has assumed the agency’s statutory accountability.

14 / LEGISLATION TO OPERATIONS

Deployment, validation and customer benefits

Legislative-informed architecture becomes useful through implementation. The starting point should be one material workflow and one defined governance, evidence or value question—not a claim of instant coverage across the whole organisation.

Agree scope and responsibility

The customer identifies the relevant entity and legal setting, purpose, owner, sources, data flows and action boundary. Legal and governance teams approve the obligation-to-control mapping. Architecture and security teams define the metadata, credentials, routing, enforcement, failure behaviour and operational support.

Cetus AI supplies the agreed product configuration and evidence structures. Customer and third-party owners remain responsible for their source systems and authorised access. Consultant support may assist policy translation, operating design, adoption and review, but does not transfer accountability to the platform.

Validate before relying on the record

Acceptance should test the required policy outcomes, untrusted or missing attributes, changed authority, human-review conditions and actual enforcement. It should also test direct-provider bypass, alternative routes, timeout, retry and cache behaviour for the selected scope.

Evidence tests should establish whether the required source IDs and timestamps are present, corrections remain distinguishable, missing receipts are reported and the review record can be retrieved. Privacy, retention, privileged administration and records hand-offs require explicit acceptance. Value tests require an approved baseline and a defined Finance-review basis.

A demonstration is not customer acceptance. Delivery scope must reflect the public capability register's available, implementation-pattern, controlled-pilot and roadmap distinctions. Value Control progressive states are publicly listed for controlled evaluation; customer-specific integrations require validation. [28]

Intended corporate benefits

Corporate customers can gain clearer ownership, selected runtime controls and evidence for management decisions, reducing ambiguity across technology, privacy, legal, service and Finance teams. Actual efficiency and commercial benefits require measurement.

The value is not simply more reporting. It is the ability to connect a material question to its source evidence, identify the missing part and assign the next action.

Intended government benefits

Government customers can support defined authority, public-resource review and appropriate AI records. Provider-neutral evidence can preserve a common governance method across approved suppliers, without guaranteeing interchangeability or eliminating integration costs.

For state and territory customers, the legal and administrative mapping must be rebuilt around their applicable instruments rather than copied from the Commonwealth examples. Sector-specific requirements, including clinical accountability where relevant, remain additional design inputs.

Australian obligations informed Songlines' design. Customer-approved policy gives that design operational meaning. Tested enforcement, source evidence and accountable review determine what the customer can rely on. Start with one approved evidence contract; expand only after testing.

References and contact

Sources reviewed 2 November 2026. Recheck the current instrument and commencement provisions before relying on a legal or policy mapping. Cetus product pages describe provider-authored capability, not independent customer-outcome evidence.

[1] Privacy Act 1988 current compilation
Read source

[2] Privacy and Other Legislation Amendment Act 2024
Read source

[3] OAIC Part 4 Notifiable Data Breach scheme
Read source

[4] OAIC Chapter 8 APP 8 Cross-border disclosure of personal information
Read source

[5] OAIC Chapter 11 APP 11 Security of personal information
Read source

[6] Corporations Act 2001 current compilation
Read source

[7] REP 798 Beware the gap Governance arrangements in the face of AI innovation
Read source

[8] ASIC compulsory information-gathering powers
Read source

[9] ASIC document production guidelines
Read source

[10] Claims of legal professional privilege
Read source

[11] Competition and Consumer Act 2010 Compilation No. 167
Read source

[12] False or misleading claims
Read source

[13] Consumer rights and guarantees
Read source

[14] Public Governance, Performance and Accountability Act 2013
Read source

[15] Department of Finance value for money guidance
Read source

[16] Department of Finance accountability and transparency guidance
Read source

[17] Department of Finance Due Diligence in Procurement
Read source

[18] Archives Act 1983 No. 79 current compilation
Read source

[19] Disposal of Commonwealth records in the absence of an agency-specific records authority
Read source

[20] Information management for records created using artificial intelligence technologies
Read source

[21] Freedom of Information Act 1982 current compilation
Read source

[22] Policy for the responsible use of AI in government version 2.1 Implementation
Read source

[23] Agentic AI addendum to the AI technical standard for Australian Government
Read source

[24] Careful adoption of agentic AI services
Read source

[25] PSPF Annual Release
Read source

[26] Information security manual
Read source

[27] Cetus AI — Enterprise architecture and customer enforcement boundaries
Read source

[28] Cetus AI — Public capability status and implementation dependencies
Read source

[29] Cetus AI — Value Control method, progressive states and decision rights
Read source

Discuss one material AI workflow, its applicable obligations and the evidence required for an accountable decision.
cetusai.com.au | hello@cetusai.com.au