RESEARCH PARTNERSHIP DISCUSSION PACK

Universal Readiness Engine State-of-the-Art Review

Public landscape review of standards, workflow orchestration, assurance, provenance and document intelligence

One engine. Domain-specific readiness applications. Evidence first. Human judgement retained.

PREPARED BY	Axiom Systems Pty Ltd
PLATFORM	**Universal Readiness Engine**
ISSUE DATE	19 August 2026
STATUS	NON-CONFIDENTIAL OVERVIEW

Purpose. This document is a non-confidential discussion aid for prospective research, industry and commercialisation partners. It does not constitute a product certification, regulatory opinion, funding commitment or offer of legal terms.

© 2026 Axiom Systems Pty Ltd. All rights reserved.

Document map

Note: Open in Microsoft Word and use References → Table of Contents if an automatically paginated table of contents is required. This discussion version uses a concise document map to remain portable.

Section	Scope
1	Purpose, questions and method
2	The readiness problem as a system category
3	Standards and management-system frameworks
4	Process orchestration and durable workflow
5	GRC, controls and compliance-management platforms
6	Document intelligence and AI-assisted extraction
7	Provenance and structured assurance arguments
8	Maturity and readiness models
9	Vertical information-management systems
10	Comparative synthesis and opportunity space
11	Research hypotheses and validation design
12	Conclusions, limitations and references

© 2026 Axiom Systems Pty Ltd. All rights reserved.

1. Purpose, questions and method

This review examines publicly documented methods, standards and software categories relevant to a configurable Universal Readiness Engine. It is not a patentability, freedom-to-operate or exhaustive market-clearance opinion. Its purpose is to identify established capabilities, avoid overclaiming novelty, and define researchable integration gaps.

1.1 Research questions

1. How do current standards define governance, risk, compliance, quality, AI and information-management expectations?
2. How do workflow platforms represent and execute long-running processes?
3. How do GRC and compliance platforms connect controls, evidence, issues and remediation?
4. How do document-intelligence services extract structured information from unstructured artefacts?
5. How do provenance and assurance-case standards represent claims, evidence and reasoning?
6. How do maturity and readiness models support progression decisions?
7. What synthesis opportunity remains for a reusable, domain-configurable, human-reviewed evidence-to-readiness layer?

1.2 Method

- Desk review of official standards-body, government, vendor and product documentation available publicly as at the issue date.
- Functional comparison rather than feature-count scoring; products and standards are evaluated against the specific readiness workflow described in the Platform Specification.
- Primary sources used where practical. Controlled standards text is not reproduced; public overview pages are summarised.
- No claim that a listed product is the only or best implementation in its category.
- The opportunity statement is explicitly a synthesis and research hypothesis, not proof that no comparable system exists.

> **Interpretive discipline**
>
> The market already contains substantial overlap: requirements management, GRC, BPM, document extraction, assurance cases, project controls and vertical workflow systems. The relevant question is not whether each component exists. It is whether a configurable product can combine these components into a practical, evidence-led, human-gated readiness workflow with sufficient usability, traceability and domain adaptability.

2. The readiness problem as a system category

The proposed system category sits between information collection and an authorised decision. It is concerned with whether a defined target state is sufficiently evidenced and reviewed to progress, not merely whether a process step has executed or a document exists.

Dimension	Why it matters
Target-state definition	A bounded milestone or decision whose readiness can be assessed.
Context sensitivity	Requirements and evidence expectations vary by project, risk, jurisdiction, asset, user and stage.

© 2026 Axiom Systems Pty Ltd. All rights reserved.

Dimension	Why it matters
Evidence sufficiency	Presence is not enough; evidence can be stale, partial, conflicting, unauthorised or outside scope.
Provenance	The decision record must retain where evidence came from, when and how it was created, and who reviewed it.
Human authority	Professional or regulatory judgement cannot be safely delegated to extraction or generative models.
Action closure	Readiness improves when gaps become owned, monitored actions rather than static findings.
Versioned outcome	The readiness status changes over time and should be reproducible against accepted evidence and configuration.
Cross-system orchestration	The relevant evidence often remains in specialist systems that should not be replaced.

3. Standards and management-system frameworks

Standards establish governance expectations, terminology and control structures. They are critical inputs to a readiness configuration, but they generally do not prescribe a complete case-level software interaction model for gathering heterogeneous evidence, resolving gaps and recording a human-gated readiness decision.

Framework	Primary focus	What it contributes	Relation to URE
ISO/IEC 42001	AI management system	Organisation-level policies, objectives, processes and continual improvement for AI systems.	Provides governance and control expectations; a URE configuration could operationalise evidence and lifecycle gates but would not itself confer certification. [S1]
NIST AI RMF	AI risk management	Voluntary functions and outcomes for governing, mapping, measuring and managing AI risks.	Useful as a requirement taxonomy and evaluation lens; implementation evidence and approval workflow remain organisation-specific. [S7]
ISO 37301	Compliance management	Requirements and guidance for a compliance-management system.	Supports obligation, role, monitoring and improvement concepts; case-level evidence orchestration requires implementation design. [S2]
ISO 31000	Risk management	Principles, framework and process for managing risk.	Provides risk-management concepts but not a domain-specific evidence application. [S3]
ISO 9001	Quality management	Process, customer, evidence and continual-improvement orientation.	Can inform manufacturing and service-readiness packs; quality-system certification remains separate. [S4]
ISO 14001	Environmental management	Framework for environmental responsibilities and continual improvement.	Can inform obligations, monitoring and corrective-action workflows; regulatory applicability remains contextual. [S5]

© 2026 Axiom Systems Pty Ltd. All rights reserved.

Framework	Primary focus	What it contributes	Relation to URE
NIST CSF 2.0	Cybersecurity risk outcomes	Governance and cybersecurity outcomes organised for risk-based use.	Can seed target profiles and evidence expectations; it does not assess evidence automatically. [S8]
ASD Essential Eight	Cyber mitigation and maturity	Prioritised mitigations with maturity guidance.	A bounded cyber-readiness vertical can connect strategies to implementation evidence and remediation. [S9]
ISO 19650 family	Built-asset information management	Information-management principles and processes using BIM.	Relevant to versioned information requirements and common data environments; a readiness layer can connect artefacts to project gates. [S6]

3.1 What standards do well

- define recognised concepts and governance expectations
- provide controlled vocabularies and auditable criteria
- support repeatability across organisations
- establish management-system and continual-improvement disciplines
- create credible reference points for domain-pack co-design

3.2 What remains an implementation task

- determining applicability to a specific case
- mapping requirements to actual evidence sources
- representing evidence quality and uncertainty
- routing items to authorised reviewers
- turning gaps into owned actions
- integrating existing systems
- producing a versioned readiness decision without misrepresenting certification

4. Process orchestration and durable workflow

Business-process and durable-workflow technologies are mature foundations for executing defined sequences, decisions, tasks, timers and external calls. BPMN standardises process notation, while commercial and open platforms implement orchestration, user tasks and long-running execution. [S10] [S21] [S22]

Approach	Established strength	Residual readiness question
BPMN / process engines	Model activities, gateways, events, roles and task routing.	Process execution can be strong even when evidence sufficiency and provenance semantics are application-specific.
Durable execution platforms	Persist long-running workflows, retries and external activities.	Excellent for resilient jobs and asynchronous operations; they do not supply a domain evidence model by default.
Low-code workflow	Rapidly compose forms, approvals and automations.	Useful for local workflows, but cross-domain governance, versioned configuration and evidence semantics vary by platform.
Case management	Supports less predictable knowledge work	Closer to readiness use cases, though target-

© 2026 Axiom Systems Pty Ltd. All rights reserved.

Approach	Established strength	Residual readiness question
	and human tasks.	state and evidence-quality models remain implementation choices.

4.1 Implication for URE

URE should not re-invent durable workflow execution. Its differentiated research focus is the application-level model that binds target states, contextual requirements, evidence provenance, review dispositions, actions and readiness outcomes. A production implementation can use established workflow patterns underneath the domain contract.

5. GRC, controls and compliance-management platforms

Integrated risk management and GRC platforms connect risks, controls, policies, assessments, issues and remediation at enterprise scale. ServiceNow IRM, Archer and Microsoft Purview Compliance Manager illustrate this category. [S18] [S19] [S20]

GRC capability	State of practice	URE research/positioning question
Control libraries and mappings	Mature support for control sets, cross-framework mapping and ownership.	URE can reuse the pattern but orient it to a bounded target state and mixed operational evidence.
Assessments	Questionnaires, attestations, scores and compliance assessments.	Readiness research should test whether evidence-linked review is more informative than self-attestation or aggregate scoring.
Issues and remediation	Strong issue, risk and action workflows.	URE similarly needs owned actions, but with direct traceability to the source evidence and decision gate.
Enterprise reporting	Dashboards, executive views and audit support.	URE can provide domain-specific case views while integrating rather than replacing enterprise GRC.
Regulatory content	Some platforms provide content subscriptions and control mappings.	URE should not claim universal or automatically current obligations; source governance and configuration ownership remain explicit.

> **No “GRC replacement” claim**
>
> For large organisations, a URE vertical may complement an established GRC platform by managing a project-, asset- or intervention-level evidence workflow and exchanging findings/actions with the enterprise system. The appropriate boundary must be tested with partners.

6. Document intelligence and AI-assisted extraction

Major cloud providers offer mature document extraction, layout, form and table processing. These services can reduce manual transcription and support classification, but extraction does not establish that a value is correct, current, applicable or sufficient for a readiness decision. [S15] [S16] [S17]

© 2026 Axiom Systems Pty Ltd. All rights reserved.

Capability	Established value	Required readiness control
OCR and text extraction	Convert scanned or image-based content into machine-readable text.	Requires quality flags, page/source references and human correction.
Layout, form and table extraction	Recover structured fields and relationships from documents.	Field extraction should create review candidates, not accepted evidence by default.
Classification	Predict document type or route to a processor.	Low-confidence and unknown outcomes must remain valid states.
Generative summarisation	Produce summaries, suggested findings or candidate actions.	Grounding, structured output, claim checks and explicit human disposition are required.
Semantic search / retrieval	Locate relevant passages across corpora.	Retrieved passages still require source, scope, currency and authority review.

6.1 Automation-bias and authority boundary

The state of the art supports powerful assistance but not a universal basis for autonomous professional or regulatory determination. The URE review-proposal pattern is therefore a safety and accountability mechanism: machine outputs are candidates; users see provenance and limitations; no project mutation occurs until explicit acceptance and application.

7. Provenance and structured assurance arguments

W3C PROV defines interoperable concepts for describing entities, activities and agents involved in producing data. OMG SACM provides a structured model for claims, argumentation and evidence in assurance cases. [S11] [S12] These standards address two important parts of the readiness problem: where evidence came from and how evidence supports a claim.

Concept	Contribution	Design implication
Provenance representation	Source, generation activity and responsible agent can be represented explicitly.	URE can adopt compatible concepts while keeping the operational UI simpler for domain users.
Assurance claims	Claims can be linked through structured argument to evidence.	URE target states and requirements can be treated as operational claims, but full assurance-case authoring may exceed many pilot needs.
Change impact	Versioned evidence and claims make supersession visible.	A readiness outcome should be recomputable or reviewable when evidence/configuration changes.
Interoperability	Standard models enable exchange across tools.	Research can test a minimal export profile without burdening users with specialist notation.

© 2026 Axiom Systems Pty Ltd. All rights reserved.

7.1 Opportunity

Many operational teams need provenance and assurance discipline but do not need to author a formal safety case. A research opportunity is to identify the smallest understandable evidence-and-claim model that improves decisions and auditability while remaining usable in routine professional work.

8. Maturity and readiness models

NASA Technology Readiness Levels and capability-maturity models are widely recognised ways to describe progression. [S13] [S14] They are useful but operate at a different level from a case-specific evidence workflow.

Model	Strength	Limitation addressed by evidence orchestration
Technology Readiness Levels	Classify maturity from basic principles to operational proof.	A TRL claim still needs supporting evidence, scope and environment; the engine can hold that evidence and decision record.
Capability maturity models	Assess process capability across defined practices and levels.	Maturity can become a target state, but assessment evidence and improvement actions still need orchestration.
Stage-gate methods	Structure investment or project progression decisions.	Gates are useful; URE emphasises contextual evidence, conditions and actions behind a gate result.
Readiness checklists	Provide simple, repeatable prompts.	Checklists are accessible but can flatten uncertainty, applicability and evidence quality.
Composite scores	Summarise multiple dimensions.	Scores aid communication but can obscure blockers and should remain subordinate to traceable evidence.

9. Vertical information-management systems

Each candidate vertical already has specialist tools: planning/property platforms, common data environments and BIM systems, security/GRC systems, farm-management platforms, laboratory and quality systems, environmental monitoring, asset-management platforms and research portfolio tools. These systems often contain authoritative data and should be treated as potential integration partners or systems of record.

Vertical	Existing system categories	Potential orchestration gap
Planning and built environment	Spatial/property intelligence, planning portals, document management, BIM/CDE, project controls.	Cross-source evidence assembly, professional review, conditions and readiness for a nominated project gate.
Cyber and AI governance	GRC, vulnerability, security operations, model registries and policy systems.	Case-level evidence sufficiency, human approval and remediation around a particular assurance target.
Agriculture and biosecurity	Farm-management, sensor, traceability, scheme and government systems.	Decision-specific provenance, uncertainty, adviser review and action closure across heterogeneous data.

© 2026 Axiom Systems Pty Ltd. All rights reserved.

Vertical	Existing system categories	Potential orchestration gap
Energy and infrastructure	Project controls, GIS, asset management, digital twins and engineering systems.	Cross-discipline dependency and evidence readiness for project or operational gates.
Quality and manufacturing	QMS, MES, ERP, PLM and supplier systems.	Release-gate evidence, exceptions and reviewer-controlled readiness across systems.
Research translation	Research information, grant, IP, CRM and portfolio systems.	Evidence-backed progression decisions across technical, market, regulatory and partnership dimensions.

Integration-first position

The strongest partner proposition is not “replace your systems.” It is “configure a bounded readiness application that preserves authoritative sources, makes evidence and uncertainty reviewable, and drives unresolved matters to closure.”

10. Comparative synthesis and opportunity space

Category	Established contribution	Residual question
Standards/frameworks	Define expectations, controls and governance.	Do not provide a complete, usable case-level application or live evidence trail.
BPM/workflow	Execute tasks, decisions, timers and integrations reliably.	Evidence sufficiency, provenance and target-state semantics are application-specific.
GRC/IRM	Manage enterprise risks, controls, assessments and issues.	May be heavy for domain pilots and not centred on a bounded project/asset/intervention readiness question.
Document intelligence	Extract and structure information efficiently.	Extraction is not acceptance, applicability or professional judgement.
Assurance/provenance standards	Represent claims, evidence and lineage rigorously.	Operational usability and action workflow require application design.
Maturity/readiness models	Provide understandable progression scales and gates.	Can obscure evidence quality, conditions and context when used alone.
Vertical systems	Hold authoritative domain data and specialist workflows.	Cross-system readiness and handover may remain fragmented.
URE hypothesis	Integrates target state, evidence, provenance, review, actions and outcome through configurable domain packs.	Must prove usability, transferability, decision quality, efficiency and commercial value through partner-led validation.

10.1 Specific synthesis hypothesis

The potential contribution of URE is the synthesis of established patterns into a reusable operational layer: a domain expert can configure what readiness means; evidence is registered with provenance and uncertainty; machine assistance creates review proposals; authorised users decide; gaps become actions; and the resulting status remains traceable to the accepted evidence and configuration version.

© 2026 Axiom Systems Pty Ltd. All rights reserved.

This is an inference from the reviewed landscape, not a claim that no product offers overlapping capabilities. Competitive and patent research would be required before making stronger exclusivity or novelty statements.

10.2 What could be differentiating if validated

- brief-first, target-state-oriented interaction rather than tool- or document-first intake;
- a reusable canonical evidence/review/action model with domain packs rather than separate greenfield applications;
- explicit representation of unknown, stale, conflicting and low-confidence evidence;
- review proposal and explicit apply boundary for AI and extraction;
- non-blocking async UX across extraction, source checks and AI tasks;
- deterministic readiness outputs and typed state transitions;
- integration above systems of record with provenance and warnings;
- research-ready baseline and guardrail measurement embedded in pilot configuration.

11. Research hypotheses and validation design

Hypothesis	Candidate test
H1 Transferability	A common evidence/review/action schema can be configured for at least three materially different domains without changing the core orchestration model.
H2 Decision traceability	Reviewers can reconstruct why a readiness state was reached faster and more accurately than with the current document/email workflow.
H3 Evidence quality	The system increases detection of stale, conflicting or insufficient evidence before the decision gate.
H4 Human control	Review-proposal gating lowers inappropriate automated acceptance while maintaining useful time savings.
H5 Workflow efficiency	The configured workflow reduces repeated retrieval, re-entry and follow-up activity.
H6 Action closure	Linking findings to owned actions improves closure rate and reduces lost follow-up.
H7 Usability	Domain experts can understand and use the readiness model without becoming assurance-modelling specialists.
H8 Commercial relevance	At least one target user group identifies a recurring, budgeted readiness problem for which the configured application is preferable to extending existing tools.

11.1 Suggested comparative study design

8. Select a bounded, recurring decision and document the current workflow and systems.
9. Define the target state, evidence map, domain roles, blockers and non-claims with subject-matter experts.
10. Create a baseline dataset of representative cases and known issues.
11. Configure the URE domain pack and integrations at the minimum viable level.
12. Run matched or sequential cases through current and configured workflows.
13. Measure time, evidence completeness, issue detection, reviewer agreement, action closure, workload and trust.
14. Conduct failure analysis, especially false readiness, missed blockers, stale evidence and automation bias.

© 2026 Axiom Systems Pty Ltd. All rights reserved.

15. Refine configuration, repeat critical cases and document transferability and limitations.
16. Assess deployment, IP, data governance and commercialisation options separately from technical performance.

11.2 Guardrail measures

- false “ready” outcome rate
- blocking matter omitted from reviewer view
- unsupported machine-generated claim accepted
- evidence linked outside its valid scope
- privacy/security incident
- reviewer override rate and rationale
- user reliance on score without evidence inspection
- integration or job failure hidden from the user

12. Conclusions, limitations and references

The public landscape contains mature standards, workflow engines, GRC platforms, document-intelligence services, provenance models, assurance-case methods, maturity scales and vertical systems. These provide substantial prior art and practical building blocks. The credible opportunity for URE is not to claim invention of those components, but to test whether their most useful patterns can be assembled into a simpler, reusable, domain-configurable readiness layer that preserves human authority and evidence traceability.

The strongest next step is partner-led validation against a real recurring decision, with an explicit baseline and guardrails. A positive result would be evidence that the configured layer improves decision preparation, transparency, handover and action closure without creating automation bias or duplicating systems of record.

12.1 Limitations

- The review is selective and based on public descriptions, not hands-on evaluation of every product.
- Vendor capabilities and product packaging change over time.
- Standards overview pages do not substitute for licensed standard texts or professional certification advice.
- The review does not address patents, source-code similarity, data-licensing rights or detailed procurement requirements.
- Market overlap may be greater in specialised products not identified by this cross-domain review.
- Claims about efficiency, quality, adoption and commercial value require empirical validation.

References and source register

Access note. URLs were assembled from official source pages for this discussion pack and should be re-checked before external circulation. Access date: 19 August 2026. The review summarises publicly available descriptions; it does not reproduce controlled standards text.

S1 ISO/IEC 42001 - Artificial intelligence management systems

International Organization for Standardization. Management-system requirements for responsible development, provision and use of AI systems. https://www.iso.org/standard/81230.html

S2 ISO 37301 - Compliance management systems

International Organization for Standardization. Compliance-management system requirements and guidance. https://www.iso.org/standard/75080.html

S3 ISO 31000 - Risk management

International Organization for Standardization. Principles and guidance for risk management. https://www.iso.org/iso-31000-risk-management.html

S4 ISO 9001 - Quality management systems

© 2026 Axiom Systems Pty Ltd. All rights reserved.

International Organization for Standardization. Quality-management system framework. https://www.iso.org/iso-9001-quality-management.html

S5 ISO 14001 - Environmental management systems

International Organization for Standardization. Environmental-management system framework. https://www.iso.org/iso-14001-environmental-management.html

S6 ISO 19650 information-management standards overview

International Organization for Standardization. Information management using BIM across the built-asset lifecycle. https://www.iso.org/standard/68078.html

S7 AI Risk Management Framework

US National Institute of Standards and Technology. Voluntary framework for managing AI risks. https://www.nist.gov/itl/ai-risk-management-framework

S8 Cybersecurity Framework 2.0

US National Institute of Standards and Technology. Risk-based cybersecurity outcomes and governance. https://www.nist.gov/cyberframework

S9 Essential Eight

Australian Signals Directorate / Australian Cyber Security Centre. Prioritised mitigation strategies and maturity model. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight

S10 Business Process Model and Notation (BPMN)

Object Management Group. Standard notation for business-process modelling. https://www.omg.org/spec/BPMN/2.0/About-BPMN

S11 Structured Assurance Case Metamodel (SACM)

Object Management Group. Metamodel for structured assurance arguments, evidence and claims. https://www.omg.org/spec/SACM

S12 PROV Overview

World Wide Web Consortium. Standards for representing provenance of entities, activities and agents. https://www.w3.org/TR/prov-overview/

S13 Technology Readiness Levels

NASA. Nine-level technology maturity scale. https://www.nasa.gov/directorates/somd/space-communications-navigation-program/technology-readiness-levels/

S14 CMMI model overview

CMMI Institute / ISACA. Capability and process-maturity model. https://cmmiinstitute.com/cmmi

S15 Microsoft Azure AI Document Intelligence

Microsoft. Document extraction, classification and structured-data services. https://learn.microsoft.com/azure/ai-services/document-intelligence/overview

S16 Google Cloud Document AI overview

Google Cloud. Document understanding and extraction services. https://cloud.google.com/document-ai/docs/overview

S17 Amazon Textract

Amazon Web Services. Machine-learning extraction of text, forms and tables. https://docs.aws.amazon.com/textract/latest/dg/what-is.html

S18 ServiceNow Integrated Risk Management

ServiceNow. Enterprise risk, compliance and resilience workflows. https://www.servicenow.com/products/integrated-risk-management.html

S19 Archer Integrated Risk Management

Archer. Integrated risk-management platform. https://www.archerirm.com/

S20 Microsoft Purview Compliance Manager

Microsoft. Compliance assessments, controls and improvement actions. https://learn.microsoft.com/purview/compliance-manager

S21 Temporal documentation

Temporal Technologies. Durable execution for long-running workflows. https://docs.temporal.io/

S22 Camunda documentation

Camunda. Process orchestration using BPMN/DMN and related components. https://docs.camunda.io/

© 2026 Axiom Systems Pty Ltd. All rights reserved.

Internal evidence basis

ID	Internal record	Date/baseline	Use in this pack
E1	Axiom Universal Readiness Engine Product Brief	August 2026	Defines the URE operating model, value proposition and human-decision boundary.
E2	AxiomReady - HIN0027 TRL 6 and Prototype Evidence	12 August 2026 baseline	Records a functional cloud-deployed planning-readiness vertical, its bounded workflow and 204/204 passing backend tests.
E3	AxiomReady Deployment and Pilot Readiness Statement	15 August 2026	Records deployment, private workspaces, controlled support and current pre-commercial status.

Boundary. The demonstrated maturity claim applies to the existing AxiomReady planning-readiness implementation and its bounded tested workflow. Other domain implementations in this package are prospective configurations requiring co-design, domain verification and pilot validation.

© 2026 Axiom Systems Pty Ltd. All rights reserved.