Curam-Ai Protocol™

Phase 3 – Compliance Shield

Pre-Audit Pack for Risk Assessment

Prepared for Partners and IT Governance

[REDACTED]

Date: December 2025

Executive Summary

The successful completion of the Feasibility Sprint (P1) and Readiness Roadmap (P2) has confirmed the technical viability and financial justification for implementing the Curam-Ai automation workflow. This **Phase 3** Pre-Audit Pack shifts focus to the project's **viability within the client's established security, governance, and insurance frameworks**.

This report proactively addresses CTO and IT Governance concerns by mapping the proposed Wave 1 deployment against critical compliance standards, specifically **ISO 27001**, and documenting risk mitigation strategies. The report includes:

- **Data Sovereignty:** Confirmation that all processing logic and data residency operate **100% within the client's existing secure cloud tenant** (M365/Azure), ensuring no data egress.
- **Risk Profile:** Identification, scoring, and mitigation of AI-specific risks via the established Human-in-the-Loop workflow and validation.
- **Audit Acceleration:** Streamlining the client's external audit process by providing pre-populated compliance questionnaires and evidence.

Stakeholder Alignment

Stakeholder	Key Question Answered	Pack Deliverables
CFO / Partners	Is the investment secure and defensible?	Board-ready cost/benefit analysis and risk hea
Risk Manager	What new risks are introduced by the AI?	Detailed risk control matrix and shadow IT inv
External Auditor	Is the solution compliant with ISO/PI rules?	Pre-filled ISO and PI questionnaires with evide
IT / CISO	How is the solution integrated securely?	Tenant control heat-map and remediation roac

Table of Contents

Risk Heat-Map (Executive View)

This summary visualizes the identified risks associated with the new AI workflow. Risks are assessed post-mitigation (i.e., after controls are implemented in Wave 1).

Risk Profile Overview

ID	Risk Area	Pre-Mitigation	Post-Mitigation	Detailed Analysis
R1	Data Leakage	High	**Low**	Data leakage risks were identified through a comprehensive data flow analysis. Post-mitigation, risk was reduced through strict access controls, encryption, and data residency within the client's secure cloud tenant.
R2	AI Hallucination/Error	High	**Low**	AI hallucination risks were reduced through the implementation of a three-layer validation system (Grounding, Confidence Scoring, and ERP Cross-Checks) proven in P1.
R3	Regulatory Non-Compliance	Medium	**Low**	Risks reduced through a gap analysis against ISO 27001 clauses and the implementation of a detailed compliance mapping and evidence documentation (see p. 9).
R4	Process Downtime (Flow Failure)	Medium	**Medium-Low**	Risks reduced through implementation of redundant systems and failover mechanisms within Power Platform.
R5	Data Egress (Cloud Security)	High	**Low**	Risks reduced through implementation of secure data transfer protocols and encryption; all data movement is restricted to Microsoft-certified secure connectors.

Key Mitigation Strategies

These strategies define the technical controls integrated into the Wave 1 solution that reduce the Residual Risk to an acceptable level (Post-Mitigation).

Mitigation Protocols

- **Data Egress (R5):** Solution architecture strictly limits all processing to the client's [REDACTED]M365/Azure tenant. The only data movement is to [REDACTED]local SharePoint lists or [REDACTED]Xero/ERP via secure connectors.
- **AI Error (R2):** The core AI model is governed by a three-layer validation system (Grounding, Confidence Scoring, and ERP Cross-Checks), requiring mandatory human approval for any confidence score below **90%**. This prevents flawed critical data (beam sizes, totals) from proceeding.
- **Regulatory (R3):** Deployment is mapped against [REDACTED]core ISO 27001 clauses (see p. 9) before deployment begins, ensuring alignment with client policy.

Risk Control Matrix (RCM)

This matrix details the specific controls applied to mitigate the risks introduced by the AI deployment.

RCM: AI Validation and Error Handling

Risk ID	Risk Description	Control Implemented	Status / Residual Risk
R2.1	AI misreads a critical field (e.g., steel grade).	**Confidence Scoring:** Items extracted with $\leq$ **90%** confidence are automatically flagged and routed to the [REDACTED]Teams Review Channel.	**Yes** / Low
R2.2	AI "guesses" or hallucinates a value not in the source PDF.	**Grounding:** AI model is constrained to extract **only** from the provided document text. It cannot generate external information.	**Yes** / Very Low
R2.3	Data entered into ERP does not match master vendor list.	**ERP Cross-Check:** Power Automate flow queries [REDACTED]SharePoint Approved_Vendors list before attempting Xero export.	**Yes** / Low

Table 1: AI Validation and Error Handling Controls

[REDACTED]

RCM: Security and Data Management

Risk ID	Risk Description	Control Implemented	Status / Residual Risk
R5.1	Source PDF files leave the client's network.	**Data Residency:** Files are processed using Azure services within the client's [REDACTED]Azure/M365 tenant. No external SaaS services are utilized.	**Yes** / Low
R5.2	Unauthorized personnel access extracted data lists.	**Access Control:** Extracted data lists (SharePoint/Dataverse) are secured via [REDACTED]M365 groups mirroring existing roles (e.g., "Finance-Only").	**Yes** / Low
R5.3	On-premise files are exposed during integration.	**Data Gateway:** Microsoft Power Platform Data Gateway utilized to access on-premise file shares. This operates inside the firewall with only encrypted outbound traffic.	**Yes** / Low

Table 2: Security and Data Management Controls

[REDACTED]

Shadow IT Inventory & Alignment

This section tracks third-party/unmanaged tools that could be made redundant by the Curam-Ai workflow. The implementation of Wave 1/2 is expected to formally retire these solutions, reducing attack surfaces and improving security.

Tool/App	Function	Managed?	Status Post-Wave 2
[REDACTED]	Invoice OCR	No (SaaS)	**Retired**
[REDACTED]	Drawing Register Man.	No (Manual/SharePoint)	**Retired**
[REDACTED]	Tender Scraper	No (Personal License)	**Migrated to M365**

Table 3: Inventory Snapshot of Redundant/Shadow Applications

[REDACTED]

END OF RISK MANAGER SECTION

Pre-Filled Compliance Questionnaire

The following is a partial index of control mappings relevant to the Curam-Ai implementation. This evidence is provided to accelerate the external auditor's review of the new workflow.

ISO 27001 Alignment (Excerpt)

ISO Clause	Control Name	Evidence Provided by Curam-Ai (Insurer Pack)
A.14.2.1	Secure Development Policy	AI logic operates via [REDACTED]M365 Power Platform; development standards conform to Microsoft security guidelines. Full source code transferred to Client Tenant (P4) with audit log.
A.12.1.2	Change Management	AI flows/logic are documented and version-controlled within [REDACTED]SharePoint/Azure DevOps. Changes require formal approval from [REDACTED]IT Admin.
A.18.1.3	Protection of Records	Extracted data is routed to secured SharePoint/Dataverse lists, adhering to the client's existing [REDACTED]data retention policy and access controls.
A.13.2.1	Information Transfer	Data movement between AI and ERP uses [REDACTED]Microsoft-certified encrypted connectors. All transfer events are logged for audit purposes.

Table 4: ISO 27001 Control Mapping

[REDACTED]

PI Insurance Questionnaire (Excerpt)

Q No.	Insurer Question	Curam-Ai Response (Evidence Index)
Q-14	Do you use AI/ML for critical design data?	**Yes**, for [REDACTED]beam schedules. Mitigation is [REDACTED]Human-in-the-Loop review for all low-confidence extractions.
Q-15	How is data integrity guaranteed?	**Three-Layer Validation** (Grounding, Confidence Scoring, ERP Cross-Checks). Errors are routed to staff [REDACTED]in real-time for correction.
Q-16	Do you retain IP for the solution?	**No. 100% of source code and IP is transferred** to the client (P4), enabling full internal audit and control.

Table 5: PI Insurance Questionnaire Mapping

[REDACTED]

Governance and Remediation Roadmap

Governance Framework (AI Ownership)

- **System Owner:** [REDACTED]Head of IT (Responsible for M365 Tenant and flow maintenance).
- **Process Owner:** [REDACTED]Head of Finance / Project Management (Responsible for user adoption and defining governance policies).
- **Model Maintenance:** Routine vendor list and simple logic changes handled by [REDACTED]IT Admin. Complex model retraining defined by [REDACTED]quarterly reviews.

[REDACTED]

Phase 3 Remediation Roadmap

This roadmap outlines any non-negotiable prerequisite tasks the client must complete before Phase 4 Deployment can commence.

Task ID	Description	Owner / Deadline
R-01	Synchronize the [REDACTED]ERP Vendor Master List to the [REDACTED]SharePoint Approved_Vendors list. (Prerequisite for ABN fraud check).	[REDACTED]IT Admin / Pre-Wave 1
R-02	Review and formally approve the AI-specific Governance Framework (p. 11).	[REDACTED]Partners / Pre-Wave 1
R-03	[REDACTED]	

Table 6: Mandatory Pre-Deployment Tasks

[REDACTED]

Conclusion & Next Steps

The **Phase 3** Compliance Shield has successfully mapped the proposed Curam-Ai solution against the client's critical security and insurance requirements. All major risks are identified, scored, and mitigated by technical and process controls. The project is now ready to proceed to implementation.

Final Recommendation

Proceed to **Phase 4 – Wave 1 Implementation** to realize the validated $\$214,500$ gross return by deploying the core Invoice Processing and Beam Schedule Extraction workflows.

Next Action: Sign the Phase 4 Statement of Work (SOW) to commence Wave 1 Deployment.
[REDACTED]

Strategic AI Consultant

APPENDIX

Supporting Documentation and References

Appendices and References

- **Appendix A: Detailed Technical Documentation:** Includes Power Automate logic traces (similar to Appendix C of the P2 report) and Azure consumption logs for audit review.
- **Appendix B: References to Industry Best Practices:** Index of relevant NIST and ISO control objectives referenced during the risk mapping process.
- **Appendix C: Supporting Material from Audits and Assessments:** Evidence index linking specific controls (e.g., A.14.2.1) to existing client policies reviewed during Phase 3.

SAMPLE END OF REPORT