



SAMPLE OUTPUT PACK

Toolkit 1

AI Readiness Assessment™

Executive report, maturity dashboard, priority actions and 90-day roadmap, shown for a fictional organisation.

Build Once. Comply Twice.™

Illustrative fictional data only

The assessment workbook, question set, scoring engine and full maturity guidance are not included in this sample. The licensed toolkit provides the reusable system that generates these outputs.

Document control

Document ID	TK1-SAMPLE-OUTPUT-v1
Toolkit	Toolkit 1 - AI Readiness Assessment™
Document title	Sample Output Pack
Version	v1
Status	Final
Classification	Client-facing
Review date	30-09-2028
Core promise	Build Once. Comply Twice.™

Standards positioning

This sample shows an ISO/IEC 42001:2023-mapped readiness output for Toolkit 1. Clause and Annex A references are included to support readiness discussions and internal governance planning. They do not constitute certification, legal advice, external assurance or a formal audit opinion.

Related standards referenced for readiness context: ISO/IEC 42001:2023, ISO/IEC 42005:2025, ISO/IEC 23894:2023, ISO/IEC 22989:2022 and ISO/IEC 27001:2022.

About this sample

This document shows the executive-ready output format produced by Toolkit 1 - AI Readiness Assessment™. All organisation names, scores, findings and data are fictional and illustrative only.

It is complete in format and structure. It does not include the assessment workbook, question set, scoring engine, full maturity descriptors or workbook formulae. Those are included only in the licensed toolkit.

Use this sample to confirm that the output format fits your internal governance needs. If it does, the licensed toolkit provides the structured assessment system that produces these outputs consistently and defensibly.

Why this matters

The sample shows, at output level, how existing ISO/IEC 27001 governance can be reused and extended for ISO/IEC 42001 readiness through one evidence spine.

1. Sample executive report

FICTIONAL DATA - ILLUSTRATIVE ONLY

Organisation

Organisation	Northbridge Digital Services Ltd
Assessment date	15 September 2026
Scope	Corporate functions and Product (GenAI features in roadmap)
Primary AI use cases	Internal knowledge assistant; document summarisation; automated triage and routing
AI deployment model	Embedded SaaS AI (Microsoft Copilot, third-party APIs); no internal model builds currently
Assessor	Internal - Head of Information Security & Risk

Overall assessment result

Developing Overall AI readiness (Level 3)	2.6 / 5 Composite score across five domains	2 HIGH Priority risks to address first
---	---	--

Defined ownership and repeatable practices exist in key areas. Governance is not yet fully embedded across the AI lifecycle. Targeted investment is required before scaling higher-risk use cases.

Readiness interpretation

Commercial meaning	The organisation has enough structure to begin formalising AI governance, but not enough evidence to support confident external assurance.
Primary route	Prioritise AI inventory, supplier assurance, AI risk treatment evidence and lifecycle monitoring.
ISO/IEC 42001 relevance	Key gaps map to Clauses 5.3, 6.1, 8 and 9, plus Annex A.4, A.5, A.6, A.7 and A.10.

Top risks identified

Severity	Risk area	Finding	ISO/IEC 42001 reference
HIGH	Supplier AI risk	No structured assurance process for GenAI API providers. Contract terms do not address data processing, model drift or incident notification.	Clause 8; Annex A.10
HIGH	Incomplete AI system inventory	No confirmed register of all AI tools in use. Shadow AI usage likely in commercial and product functions.	Clauses 6, 8; Annex A.3, A.4

Severity	Risk area	Finding	ISO/IEC 42001 reference
MEDIUM	Inconsistent evidence of risk treatment	Risk register entries exist but approval records and treatment evidence are incomplete for 60% of AI-related entries.	Clauses 6.1.3, 8.3
MEDIUM	Data lineage gaps	Unclear lineage for prompts, embeddings and fine-tuning datasets used in the knowledge assistant.	Clause 8; Annex A.7
MEDIUM	Lifecycle monitoring absent	No regular cadence for reviewing AI system performance, drift or output quality after deployment.	Clauses 8, 9; Annex A.6
MEDIUM	HITL controls not documented	Human-in-the-loop controls exist informally for triage routing but are not documented or tested.	Clause 8; Annex A.6, A.9

Indicative strengths and gaps

Strengths	Gaps
Established ISO 27001-aligned ISMS provides a governance foundation	No formal AI system inventory or lifecycle register
Defined information security risk methodology with active ownership	Supplier AI assurance process undefined, leaving a gap in third-party risk
Initial AI usage policy in place (Acceptable Use)	AI risk ownership below CISO level is unclear
Management awareness of AI governance expectations is high	No structured pre-deployment review gate for new AI use cases
Existing ISMS review rhythm can be reused for AI governance cadence	Monitoring and performance review cadence absent

What this result means

The existing ISO 27001 governance spine can be reused, but AI-specific inventory, supplier, risk and lifecycle evidence need to be extended. That is the Build Once. Comply Twice.™ approach in practice.

2. Sample maturity dashboard

FICTIONAL DATA - ILLUSTRATIVE ONLY

The dashboard shows how the organisation scores across the five Toolkit 1 readiness domains. Each domain is scored 0 to 5 against defined maturity descriptors, and each score maps to the nearest maturity level (for example, 2.5 to 3.4 is Developing). The composite score sets the overall readiness band.

Domain	Score	Maturity band	ISO/IEC 42001 reference	Assessor notes
A - Strategy and Governance	3.1 / 5	Developing	Clauses 4, 5, 6; Annex A.2, A.3	Ownership defined at CISO level; governance charter drafted but not yet ratified.
B - Data Foundations	2.8 / 5	Developing	Clause 8; Annex A.7	Data classification policy partially covers AI inputs; lineage gaps for GenAI.
C - AI System Visibility	2.2 / 5	Emerging	Clauses 6, 8; Annex A.3, A.4	Known systems are partially tracked. Shadow AI and supplier-embedded AI remain incomplete.
D - AI Risk Management	2.6 / 5	Developing	Clauses 6.1, 8.2, 8.3; Annex A.5	Risk entries exist; treatment evidence and escalation paths incomplete.
E - AI Lifecycle Management	2.3 / 5	Emerging	Clauses 8, 9; Annex A.6, A.8	No formal deployment gates or post-deployment review process in place.
Composite score	2.6 / 5	Developing	Readiness view only	Governance foundations in place. Lifecycle management and supplier assurance require priority investment.

Maturity scale

Level	Description	Typical readiness implication
0 - Not in place	No defined approach. Activity is reactive, undocumented or unknown.	Not ready for meaningful ISO/IEC 42001 implementation activity.
1 - Ad hoc	Some activity exists but is informal and owner-dependent.	Basic governance foundations need to be created before scaling AI use.
2 - Emerging	Initial repeatable practices exist, but coverage is incomplete.	Prioritise ownership, inventory and risk assessment controls.
3 - Developing	Defined practices exist in key areas with partial evidence.	Suitable for structured remediation and management-system integration planning.
4 - Established	Controls are consistently applied and reviewed.	Ready for deeper ISO/IEC 42001 integration and internal assurance preparation.
5 - Optimised	Controls are measured, improved and embedded into business rhythm.	Suitable for mature monitoring, improvement and assurance cadence.

3. Sample priority action list

FICTIONAL DATA - ILLUSTRATIVE ONLY

The priority action list is generated from the assessment results. Actions are ranked by priority, assigned to owner roles and scheduled across the first 90 days. Clause references show the readiness area each action strengthens.

#	Priority	Action	Owner	Window	ISO/IEC 42001 reference	Notes
1	HIGH	Establish AI system inventory	Risk / InfoSec	Weeks 1-4	Clauses 6, 8; Annex A.4	Immediate sprint. Blocker for supplier assurance and lifecycle visibility.
2	HIGH	Define AI supplier assurance process	Procurement / CISO	Weeks 2-6	Clause 8; Annex A.10	Map critical AI suppliers; add AI-specific clauses to the vendor review template.
3	HIGH	Implement pre-deployment AI review gate	Product / Risk	Weeks 3-8	Clauses 6.1, 8; Annex A.5, A.6	Lightweight gate for new AI use cases. Connects to the AISIA workflow where applicable.
4	MEDIUM	Complete AI risk register treatment evidence	Risk	Weeks 4-8	Clauses 6.1.3, 8.3	Close evidence gaps on existing entries. Assign treatment owners.
5	MEDIUM	Document HITL controls for triage routing	Operations / Product	Weeks 5-8	Clause 8; Annex A.6, A.9	Formalise existing informal controls. Add to operating procedures.
6	MEDIUM	Define AI lifecycle monitoring cadence	InfoSec / Product	Weeks 6-12	Clauses 8, 9; Annex A.6	Quarterly review schedule for active AI systems. Link to the ISMS review cycle.
7	LOW	Ratify AI governance charter	CISO / Board	Weeks 8-12	Clauses 5.1, 5.3; Annex A.3	Build on the drafted charter. Board ratification adds defensibility.
8	LOW	Update AI Acceptable Use Policy	CISO / Policy owner	Weeks 5-8	Clause 5.2; Annex A.2	Reflect inventory, supplier requirements and lifecycle expectations.

What this sample does not include

This sample shows action structure and clause mapping only. It does not include the full workbook question set, weighted scoring logic, formulae or complete maturity guidance.

4. Sample 90-day roadmap

FICTIONAL DATA - ILLUSTRATIVE ONLY

The roadmap sequences the priority actions into three phases. Phase 1 establishes foundations and closes the highest-severity gaps. Phase 2 strengthens controls and puts governance into operation. Phase 3 embeds the cadence and produces the first assurance-ready output.

Phase 1: Establish foundations (days 1-30)

Action	Detail	ISO/IEC 42001 reference
AI system inventory	Create and baseline a register of all active and planned AI tools, APIs and models across the organisation.	Clauses 6, 8; Annex A.4
Ownership assignment	Confirm named accountability for each AI system. Map to existing risk and governance roles.	Clause 5.3; Annex A.3
Supplier AI risk review	Identify the top five AI suppliers by risk exposure. Start a gap review against AI-specific assurance criteria.	Clause 8; Annex A.10
Pre-deployment gate draft	Define a lightweight checkpoint process for new AI deployments, aligned with the existing change and risk process.	Clauses 6.1, 8; Annex A.5, A.6

Outcome: documented AI system inventory with confirmed ownership, supplier risk gaps identified and the governance gate process drafted.

Phase 2: Strengthen controls (days 31-60)

Action	Detail	ISO/IEC 42001 reference
Risk register completion	Close evidence gaps on existing AI risk entries. Confirm treatment owners and timelines.	Clauses 6.1.3, 8.3
HITL documentation	Formalise human-in-the-loop controls for automated triage routing. Add to operating procedures.	Clause 8; Annex A.6, A.9
Lifecycle monitoring design	Define the review cadence for active AI systems (performance, drift and output quality) and assign reviewers.	Clauses 8, 9; Annex A.6
Policy update	Update the AI Acceptable Use Policy to reflect inventory, supplier requirements and lifecycle expectations.	Clause 5.2; Annex A.2

Outcome: AI risk register updated with evidence and treatment, HITL controls documented and tested, and the monitoring schedule defined.

Phase 3: Embed and assure (days 61-90)

Action	Detail	ISO/IEC 42001 reference
Governance charter ratification	Present the AI governance charter to the board or leadership committee for ratification.	Clauses 5.1, 5.3; Annex A.3
First lifecycle review	Complete a structured review of the highest-risk active AI system using the new monitoring format.	Clauses 8, 9; Annex A.6
Supplier assurance letters	Issue or receive AI-specific assurance confirmations from critical AI suppliers.	Clause 8; Annex A.10
Baseline report	Produce the first quarterly AI governance report using the toolkit executive output format.	Clauses 9.1, 9.3

Outcome: board-ratified AI governance charter, first formal lifecycle review completed and quarterly reporting cadence established.

5. What is in the licensed toolkit

This sample shows the output structure. The licensed toolkit provides the reusable assessment system that produces these outputs consistently and defensibly.

What you get	What it does
Assessment workbook	Structured question set across the five Toolkit 1 readiness domains. Produces scores, maturity bands and narrative outputs.
ISO/IEC 42001-mapped scoring guidance	Full maturity descriptors for each criterion and level, including clause and Annex A references for readiness traceability.
Executive report template	Editable Word template for the output format shown in this sample. Designed for leadership, internal audit and assurance conversations.
Maturity roadmap logic	Maturity-aligned improvement actions for each level and domain, sequenced for real-world implementation.
Evidence spine	Evidence spine structure that connects ISO/IEC 42001 readiness outputs to an existing ISO/IEC 27001 ISMS, in line with the Build Once. Comply Twice.™ approach.
Editable templates	Priority action list, 90-day roadmap, board and executive deck, and quarterly review templates, all reusable across cycles.
Repeatable cadence design	Use the same rubric and templates for a quarterly or annual refresh without rebuilding from scratch.

Value at £349

One purchase, reusable each cycle, no consultancy required. A comparable internal readiness review typically requires multiple stakeholder sessions, consolidation and reporting. The toolkit compresses that effort into days while improving consistency and defensibility. Outputs are suitable for leadership, internal audit, customers and advisers as part of assurance preparation.

Use the licensed Toolkit 1 - AI Readiness Assessment™ to turn your current AI governance position into a scored baseline, an ISO/IEC 42001-mapped gap view and a 90-day board-ready action plan.

Decision-support notice

Decision support only. This toolkit supports governance decision-making and audit preparation. It is not certification, legal advice or external assurance. Organisations should obtain appropriate professional advice where required.

About AIBI Systems®

AIBI Systems® provides practical governance tools and frameworks to help organisations adopt AI safely, responsibly and with confidence. Our operating logic is Build Once. Comply Twice.™

www.aibisystems.co.uk | hello@aibisystems.co.uk