

GOVERNANCE DOCS

ISO/IEC 42001 Internal Audit Report

Halcyon Lending Technologies Ltd (fictional) · GD-IA-2026-S02

GD-IA-05 Internal Audit Report

1. Report details

Client organisation	Halcyon Lending Technologies Ltd (fictional)
Audit reference	GD-IA-2026-S02
Audit type	Internal audit of the AIMS under ISO/IEC 42001:2023 Clause 9.2, performed by an independent external auditor
Standard	ISO/IEC 42001:2023
AIMS scope	Development and operation of AI-based credit decisioning and customer-support AI systems for the lending platform, per AIMS scope statement AIMS-SC-01 v1.2.
AI systems in scope	CreditScore v2 (provider and deployer); SupportAssist chatbot built on a third-party foundation model (deployer)
Sites and environments	Head office (one site); Azure production environment
Headcount in scope	60
Statement of Applicability	SoA v1.1, dated 20 August 2026
Audit dates	Desk review 21-22 September 2026; remote sessions 24-29 September 2026; closing meeting 30 September 2026
Report date and version	5 October 2026 - v1.0
Audit lead	Lead Auditor, Governance Docs
Client representative	Head of Data Science and AIMS Manager
Distribution	Chief Technology Officer; Head of Data Science and AIMS Manager

2. Executive summary

Halcyon has established the core of its AIMS: the scope, AI policy, AI risk methodology and Statement of Applicability are approved, and the AI governance committee meets monthly with the CTO in the chair. The AI system inventory and the lifecycle process for CreditScore are well documented.

However, the AI system impact assessment required by Clause 6.1.4 has only been completed for CreditScore; no impact assessment exists for the SupportAssist chatbot, which handles customer conversations (NC-01, major). Three minor nonconformities concern fairness evaluation before release, supplier assurance for the foundation-model provider, and the SoA justification for one excluded control.

With the Stage 2 certification audit planned for January 2027, the priority is to complete and approve the SupportAssist impact assessment and feed its results into the AI risk register.

Major nonconformities	Minor nonconformities	Opportunities for improvement
1	3	3

Overall conclusion: The AIMS largely conforms to ISO/IEC 42001, but the major nonconformity NC-01 must be addressed before the AIMS can be considered effectively implemented and maintained.

3. Objectives, scope and criteria

Objectives. To determine whether the AIMS conforms to ISO/IEC 42001:2023 and to the organisation's own AIMS requirements; whether it is effectively implemented and maintained; and to identify nonconformities and opportunities for improvement as input to management review.

Scope. Development and operation of AI-based credit decisioning and customer-support AI systems for the lending platform, per AIMS scope statement AIMS-SC-01 v1.2. The audit covered all requirements of Clauses 4-10 and a risk-weighted sample of the Annex A controls declared applicable in the Statement of Applicability.

Criteria. ISO/IEC 42001:2023; the organisation's AI policy, AIMS procedures and objectives; and the legal, regulatory and contractual requirements for AI in its register.

4. Method, sampling and limitations

The audit was performed remotely. It comprised a desk review of documented information, four half-day remote sessions and opening and closing meetings, and review of records and system configurations on screen-share. Persons interviewed and documents reviewed are listed in Appendix B.

Records were sampled using auditor judgement, weighted towards higher-risk areas, previous findings and recent changes. For record populations, typically three to five items were examined.

Limitations. An audit is based on samples of the information available, so it cannot detect every nonconformity. The results reflect the evidence seen at the time of the audit. This internal audit is not a certification audit, and its results do not guarantee the outcome of any external audit.

5. Results by clause

Clause	Requirement area	Result	Finding ref
4.1	Understanding the organisation and its context	Conformity	-
4.2	Understanding the needs and expectations of interested parties	Conformity	-
4.3	Determining the scope of the AIMS	Conformity	-
4.4	AI management system	Conformity	-
5.1	Leadership and commitment	Conformity	-
5.2	AI policy	Conformity	-
5.3	Roles, responsibilities and authorities	Conformity	-
6.1.1	Actions to address risks and opportunities - general	Conformity	-
6.1.2	AI risk assessment	Conformity	-
6.1.3	AI risk treatment	Minor NC	NC-04
6.1.4	AI system impact assessment	Major NC	NC-01
6.2	AI objectives and planning to achieve them	Conformity	-
6.3	Planning of changes	Conformity	-
7.1	Resources	Conformity	-
7.2	Competence	Conformity	-
7.3	Awareness	OFI	OFI-02
7.4	Communication	Conformity	-
7.5	Documented information	Conformity	-

Clause	Requirement area	Result	Finding ref
8.1	Operational planning and control	Conformity	-
8.2	AI risk assessment (performed)	Conformity	-
8.3	AI risk treatment (implemented)	Conformity	-
8.4	AI system impact assessment (performed)	Major NC	NC-01
9.1	Monitoring, measurement, analysis and evaluation	OFI	OFI-01
9.2	Internal audit (programme and previous audits)	Conformity	-
9.3	Management review	Conformity	-
10.1	Continual improvement	Conformity	-
10.2	Nonconformity and corrective action	Conformity	-

6. Annex A summary

36 of the 38 Annex A controls are declared applicable in the Statement of Applicability. 22 of them (61%) were sampled in this audit; the remainder are planned for Years 2 and 3 of the internal audit programme.

Objective area	Applicable (SoA)	Sampled	Conformity	Minor NC	Major NC	OFI
A.2 Policies related to AI	3	3	3	0	0	0
A.3 Internal organisation	2	2	2	0	0	0
A.4 Resources for AI systems	5	2	2	0	0	0
A.5 Assessing impacts of AI systems	4	4	2	0	1	1
A.6 AI system life cycle	9	5	4	1	0	0
A.7 Data for AI systems	5	2	2	0	0	0
A.8 Information for interested parties	4	2	2	0	0	0
A.9 Use of AI systems	2	1	1	0	0	0
A.10 Third-party and customer relationships	2	1	0	1	0	0
Total	36	22	18	2	1	1

Full per-control results are recorded in the audit checklist and working papers (GD-IA-04). NC-01 is counted once under A.5 although it also relates to Clauses 6.1.4 and 8.4.

7. Detailed findings

Findings are listed in order of severity. Each is also entered in the Nonconformity and Corrective Action Register (GD-IA-06) supplied with this report.

NC-01	Major nonconformity · Clause / control: 6.1.4 / 8.4 / A.5.2
Requirement	The organisation must define and perform a process to assess the potential consequences of its AI systems for individuals, groups and society, retain the results and use them in the AI risk assessment.
Finding	No AI system impact assessment has been performed for the SupportAssist chatbot, which has been in production since June 2026 and handles customer conversations including complaints and vulnerability disclosures.
Objective evidence	AI System Impact Assessment Procedure AIMS-PR-04 v1.0 requires an assessment before deployment of any AI system. The AISIA register lists one completed assessment (CreditScore v2, approved 12 May 2026). SupportAssist release record REL-2026-014 (18 June 2026) has the AISIA field marked "n/a - vendor model". Interview with the Head of Data Science confirmed no assessment was carried out.
Guidance for corrective action	The action should produce and approve an impact assessment for SupportAssist, feed its results into the AI risk register and treatment plan, and address why a vendor-based system was treated as out of scope for the procedure.

NC-02	Minor nonconformity · Clause / control: A.6.2.4
Requirement	AI System Verification and Validation Standard AIMS-ST-02 v1.1 requires fairness metrics to be evaluated against defined thresholds before each release of a decisioning model.
Finding	The fairness evaluation for CreditScore v2.1 was not performed before release.
Objective evidence	Release records for v2.0, v2.1 and v2.2 were sampled. The v2.0 and v2.2 evaluation reports include fairness metrics within threshold. The v2.1 evaluation report (3 August 2026) covers accuracy and robustness only; the release was approved on 5 August 2026.
Guidance for corrective action	Consider why the release gate allowed approval without the fairness section, as well as evaluating v2.1 retrospectively.

NC-03	Minor nonconformity · Clause / control: A.10.3
Requirement	Supplier Management Procedure AIMS-PR-07 v1.0 requires an AI supplier assessment and documented responsibilities for any third-party model or AI service.
Finding	No supplier assessment exists for the foundation-model provider used by SupportAssist, and responsibilities for incidents and model changes are not documented.
Objective evidence	Supplier register (export 22 September 2026) lists the provider with assessment status "pending". The contract (signed April 2026) contains no AI-specific clauses on model changes, incident notification or data use.
Guidance for corrective action	Address the assessment and the allocation of responsibilities with the provider, for example through a supplement to the contract.

NC-04	Minor nonconformity · Clause / control: 6.1.3 / A.8.3
Requirement	The Statement of Applicability must justify the exclusion of any Annex A control.
Finding	Control A.8.3 External reporting is excluded in the Statement of Applicability without a justification.
Objective evidence	SoA v1.1: A.8.3 is marked "Not applicable"; the justification field is blank. Interview: customers can report chatbot problems through the general complaints form, which suggests the control may be applicable.
Guidance for corrective action	Review the applicability of A.8.3 and record the reasoning either way.

OFI-01	Opportunity for improvement · Clause / control: 9.1 / A.6.2.6
Requirement	The organisation should monitor AI system performance and evaluate the results.
Finding	CreditScore drift monitoring is in place and reviewed weekly, but no comparable monitoring exists for SupportAssist response quality.
Objective evidence	Drift dashboard and weekly review notes for CreditScore (July-September 2026). SupportAssist monitoring is limited to availability and latency.
Suggestion	Consider defining quality and safety measures for the chatbot, for example escalation rate and sampled conversation review.

OFI-02	Opportunity for improvement · Clause / control: 7.3
Requirement	People doing work under the organisation's control should be aware of the AI policy and their contribution to the AIMS.
Finding	Awareness training covers the data science team well, but customer-service staff who supervise SupportAssist have not received AI-specific awareness training.
Objective evidence	Training records: 14 of 14 data science and engineering staff completed the AI policy module; 0 of 9 customer-service staff. Interviews with two customer-service staff showed limited awareness of the escalation rules.
Suggestion	Consider extending the module to staff who operate or supervise AI systems.

OFI-03	Opportunity for improvement · Clause / control: A.5.5
Requirement	Societal impacts of AI systems should be assessed.
Finding	The CreditScore impact assessment considers impacts on individual applicants in depth, but societal and group-level impacts are covered in one sentence.
Objective evidence	AISIA for CreditScore v2 (12 May 2026), section 5: individual impacts 3 pages; societal impacts one paragraph stating "no societal impact identified" without analysis.
Suggestion	Consider documenting the reasoning on group-level effects, for example across protected characteristics and regions.

8. Positive observations

- AI governance (5.1, 5.3): the AI governance committee has met monthly since March 2026 with the CTO in the chair; minutes show risk acceptance decisions and follow-up.
- AI system inventory and lifecycle documentation (A.4.2, A.6.2.3): CreditScore has complete model cards, data provenance records and architecture documentation.
- Data provenance (A.7.5): all three sampled training datasets had documented sources, licences and preparation steps.

9. Follow-up of previous findings

This is the first internal audit of the AIMS, so there are no previous findings to follow up.

10. Next steps

- Record correction and corrective action for each finding in the NC & CAPA register (GD-IA-06) by 19 October 2026.
- NC-01 (major): complete and approve the SupportAssist impact assessment, and update the AI risk register, before the Stage 2 audit in January 2027.
- Minor nonconformities: action plans by 4 November 2026; closure by 3 January 2027.

- Present these results at the management review planned for November 2026.
- Corrective-action verification by Governance Docs has been requested for the week of 7 December 2026.

11. Auditor independence and competence

This audit was led by the Lead Auditor, Governance Docs. The auditor has had no responsibility for the design, implementation or operation of Halcyon's AIMS or its AI systems, and Governance Docs has not provided implementation consultancy to Halcyon in the past 24 months. A signed Auditor Competence and Independence Record (GD-IA-07), which identifies the auditor and evidences competence, has been issued to Halcyon separately. It may be shown to the certification body on request.

12. Report issue and acceptance

	Name / role	Signature	Date
Issued by	Lead Auditor, Governance Docs		5 Oct 2026
Accepted for Halcyon	Head of Data Science and AIMS Manager		7 Oct 2026

Appendix A - Finding classification

Grade	Definition
Major nonconformity	A requirement of ISO/IEC 42001 or of the organisation's AIMS is not addressed at all, or there is a systemic failure (including several minor nonconformities against the same requirement) that raises significant doubt about the AIMS achieving its intended outcomes. Normally must be corrected, with corrective action planned, before certification can be recommended.
Minor nonconformity	A single lapse or partial fulfilment of a requirement that does not, on its own, put the AIMS outcomes in doubt. Requires correction and corrective action within an agreed timescale.
Opportunity for improvement (OFI)	No requirement is breached, but the auditor identified a way to make the AIMS more effective or less exposed to future nonconformity. Action is at management's discretion.
Positive observation	Practice that is notably effective and worth maintaining or extending.

Appendix B - Documents reviewed and persons interviewed

Documents and records reviewed

- AIMS scope statement AIMS-SC-01 v1.2; AI system inventory (export 20 September 2026)
- AI Policy AIMS-PO-01 v2.0
- Context Analysis AIMS-CTX-01 v1.1 and Interested Parties Register v1.0
- AI Risk Assessment Methodology AIMS-PR-02 v1.2; AI Risk Register (export 15 September 2026)
- Statement of Applicability v1.1; AI Risk Treatment Plan v1.1
- AI System Impact Assessment Procedure AIMS-PR-04 v1.0; AISIA for CreditScore v2 (12 May 2026)
- AI Objectives AIMS-OBJ-01 v1.0
- AI governance committee minutes March-September 2026
- Verification and Validation Standard AIMS-ST-02 v1.1; evaluation reports and release records for CreditScore v2.0, v2.1, v2.2; SupportAssist release record REL-2026-014
- Supplier Management Procedure AIMS-PR-07 v1.0; supplier register; foundation-model provider contract
- Drift monitoring dashboard and weekly review notes July-September 2026

- Training records and AI awareness module completion (export 22 September 2026)

Persons interviewed (by role)

- Chief Technology Officer
- Head of Data Science and AIMS Manager
- Lead ML Engineer
- Product Owner, SupportAssist
- Procurement Manager
- Data Protection Officer
- Two customer-service staff (awareness interviews)