

GOVERNANCE DOCS

ISO/IEC 27001 Internal Audit Report

Meridian Parcel Services Ltd (fictional) · GD-IA-2026-S01

GD-IA-05 Internal Audit Report

1. Report details

Client organisation	Meridian Parcel Services Ltd (fictional)
Audit reference	GD-IA-2026-S01
Audit type	Internal audit of the ISMS under ISO/IEC 27001:2022 Clause 9.2, performed by an independent external auditor
Standard	ISO/IEC 27001:2022 including Amendment 1:2024
ISMS scope	Provision of parcel tracking and delivery management services from the head office and the AWS-hosted tracking platform, per ISMS scope statement ISMS-SC-01 v2.0.
Sites and environments	Head office (one site); AWS eu-west-1 production environment
Headcount in scope	85
Statement of Applicability	SoA v1.3, dated 4 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 IT and ISMS Manager
Distribution	Chief Operating Officer; Head of IT and ISMS Manager

2. Executive summary

Meridian has established most of the ISMS framework: the scope, policy, risk methodology and Statement of Applicability are in place and approved, and top management is visibly engaged. Operational controls for change management and asset management are particularly well run.

However, the ISMS cannot yet show that its performance is evaluated. No monitoring or measurement results exist for the information security objectives set in January 2026 (NC-02, major). Four minor nonconformities concern SoA justifications, management review inputs, an access review and backup restore testing.

With the Stage 2 certification audit planned for December 2026, the priority is to close NC-02, with at least one cycle of measured results reported to management, and to have action plans for the minor findings.

Major nonconformities	Minor nonconformities	Opportunities for improvement
1	4	3

Overall conclusion: The ISMS largely conforms to ISO/IEC 27001, but the major nonconformity NC-02 must be addressed before the ISMS can be considered effectively implemented and maintained.

3. Objectives, scope and criteria

Objectives. To determine whether the ISMS conforms to ISO/IEC 27001:2022 and to the organisation's own ISMS requirements; whether it is effectively implemented and maintained; and to identify nonconformities and opportunities for improvement as input to management review.

Scope. Provision of parcel tracking and delivery management services from the head office and the AWS-hosted tracking platform, per ISMS scope statement ISMS-SC-01 v2.0. 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 27001:2022 including Amendment 1:2024; the organisation's ISMS policies, procedures and objectives; and the legal, regulatory and contractual requirements 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	OFI	OFI-03
4.2	Understanding the needs and expectations of interested parties	Conformity	-
4.3	Determining the scope of the ISMS	Conformity	-
4.4	Information security management system	Conformity	-
5.1	Leadership and commitment	Conformity	-
5.2	Policy	Conformity	-
5.3	Organisational roles, responsibilities and authorities	Conformity	-
6.1.1	Actions to address risks and opportunities - general	Conformity	-
6.1.2	Information security risk assessment	Conformity	-
6.1.3	Information security risk treatment	Minor NC	NC-01
6.2	Information security 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	Information security risk assessment (performed)	Conformity	-
8.3	Information security risk treatment (implemented)	Conformity	-
9.1	Monitoring, measurement, analysis and evaluation	Major NC	NC-02
9.2	Internal audit (programme and previous audits)	Conformity	-
9.3	Management review	Minor NC	NC-04
10.1	Continual improvement	Conformity	-
10.2	Nonconformity and corrective action	Conformity	-

6. Annex A summary

86 of the 93 Annex A controls are declared applicable in the Statement of Applicability. 42 of them (49%) were sampled in this audit; the remainder are planned for Years 2 and 3 of the internal audit programme.

Theme	Applicable (SoA)	Sampled	Conformity	Minor NC	Major NC	OFI
Organisational (5.1-5.37)	36	18	16	1	0	1
People (6.1-6.8)	8	5	5	0	0	0
Physical (7.1-7.14)	12	5	5	0	0	0
Technological (8.1-8.34)	30	14	13	1	0	0
Total	86	42	39	2	0	1

Full per-control results are recorded in the audit checklist and working papers (GD-IA-04).

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-02	Major nonconformity · Clause / control: 9.1
Requirement	The organisation must decide what needs to be monitored and measured, the methods, timing and responsibilities, and must analyse and evaluate the results, retaining them as evidence. The information security objectives (6.2) must be monitored.
Finding	Monitoring and measurement of information security performance has not been defined or carried out. None of the five information security objectives has a defined measure, frequency or owner for measurement, and no results have been recorded since they were set.
Objective evidence	Information Security Objectives ISMS-OBJ-01 v1.0 (approved 15 January 2026): five objectives with targets but no measures. No ISMS metrics or dashboard was available. The management review minutes of 12 March 2026 record the action "KPIs to be defined - Head of IT", still open at the audit date. Interview with the ISMS Manager confirmed no measurement has taken place.
Guidance for corrective action	The action should define, for each objective and for key controls, what is measured, how, how often and by whom, then produce and evaluate at least one cycle of results. Root-cause analysis should consider why the March 2026 action was not tracked to completion.

NC-01	Minor nonconformity · Clause / control: 6.1.3 d)
Requirement	The Statement of Applicability must justify the exclusion of any Annex A control.
Finding	Two Annex A controls are excluded in the Statement of Applicability without a justification.
Objective evidence	SoA v1.3: A.8.30 Outsourced development and A.7.12 Cabling security are marked "Not applicable"; the justification field is blank for both. Interview: development is partly outsourced to a third party for the mobile application, which suggests A.8.30 may in fact be applicable.
Guidance for corrective action	Review the applicability of both controls against the risk assessment. A.8.30 in particular should be re-assessed given the outsourced mobile development.

NC-04	Minor nonconformity · Clause / control: 9.3.2
Requirement	Management review must consider, among other inputs, changes in the needs and expectations of interested parties and feedback from interested parties.
Finding	The most recent management review did not consider changes in the needs and expectations of interested parties, or feedback from interested parties.
Objective evidence	Management review minutes, 12 March 2026: the agenda and minutes cover audit results, risks, objectives and incidents, but not interested parties. Two customer security questionnaires received in February 2026 were not discussed.
Guidance for corrective action	Align the management review agenda template to all required inputs in Clause 9.3.2.

NC-03	Minor nonconformity · Clause / control: A.5.18
Requirement	Access Control Procedure ISMS-PR-05 requires quarterly access reviews for the five key business systems.
Finding	The Q2 2026 access review for the ERP system was not performed.
Objective evidence	Access review records were sampled for three of the five key systems (CRM, ERP, Microsoft 365) for Q1 and Q2 2026. CRM and Microsoft 365 reviews were complete and signed. No ERP review exists for Q2; the review owner left the company in May 2026 and the task was not reassigned.
Guidance for corrective action	Address the instance and the reason it was missed, for example ownership cover when staff leave.

NC-05	Minor nonconformity · Clause / control: A.8.13
Requirement	Backup Policy ISMS-PO-12 requires a quarterly restore test of production databases.
Finding	No restore test of the warehouse management system (WMS) database has been performed since February 2026.
Objective evidence	Backup job reports were complete and successful for the period sampled (July-September 2026). The restore test log shows the last WMS restore test on 18 February 2026. Restore tests of the tracking platform database were performed in May and August 2026.
Guidance for corrective action	Confirm that restore tests cover all databases named in the policy, and track them on a schedule.

OFI-01	Opportunity for improvement · Clause / control: A.5.7
Requirement	Threat intelligence should be collected and analysed to produce threat intelligence.
Finding	Threat intelligence sources are in place, but the analysis and the decisions taken are not recorded.
Objective evidence	Subscriptions to the national CERT advisories and a vendor threat feed. The ISMS Manager described reviewing them weekly, but no record of relevance decisions was available.
Suggestion	Consider a simple log of the advisories assessed as relevant and the actions taken. This would also give evidence for A.8.8.

OFI-02	Opportunity for improvement · Clause / control: 7.3
Requirement	People doing work under the organisation's control must be aware of the policy, their contribution and the implications of not conforming.
Finding	Awareness training is effective for employees, but contractors are not included in phishing simulations.
Objective evidence	Training completion 92% (78 of 85 employees). Phishing simulation reports for Q2 and Q3 2026 cover employees only; six long-term contractors have system access.
Suggestion	Consider including contractors with system access in the simulation programme.

OFI-03	Opportunity for improvement · Clause / control: 4.1
Requirement	The organisation must determine whether climate change is a relevant issue (Amendment 1:2024).
Finding	Climate change has been recorded as "not relevant", but the reasoning is not documented.
Objective evidence	Context Analysis ISMS-CTX-01 v2.0: the climate change row reads "Not relevant" with no rationale. The head office is in a flood-risk area noted in the business continuity plan.
Suggestion	Consider recording the reasoning, taking the flood-risk assessment in the business continuity plan into account.

8. Positive observations

- Change management (A.8.32): all three sampled production changes had a documented risk assessment, approval, test evidence and a rollback plan.
- Asset inventory (A.5.9): complete, with named owners. All five assets sampled from the floor matched the inventory.
- Leadership (5.1): the Chief Operating Officer attended the whole first session and could explain the risk acceptance decisions.

9. Follow-up of previous findings

This is the first internal audit of the ISMS, so there are no previous findings to follow up. The Stage 1 certification audit in August 2026 raised two areas of concern, both of which were found to be closed.

10. Next steps

- Record correction and corrective action for each finding in the NC & CAPA register (GD-IA-06) by 19 October 2026.
- NC-02 (major): implement measurement and evaluate at least one cycle of results before the Stage 2 audit in December 2026.

- 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 23 November 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 Meridian's ISMS, and Governance Docs has not provided implementation consultancy to Meridian 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 Meridian 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 Meridian	Head of IT and ISMS Manager		7 Oct 2026

Appendix A - Finding classification

Grade	Definition
Major nonconformity	A requirement of ISO/IEC 27001 or of the organisation's ISMS 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 ISMS 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 ISMS 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 ISMS 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

- ISMS scope statement ISMS-SC-01 v2.0
- Information Security Policy ISMS-PO-01 v3.1
- Context Analysis ISMS-CTX-01 v2.0 and Interested Parties Register v1.2
- Risk Assessment Methodology ISMS-PR-02 v1.4; Risk Register (export 15 September 2026)
- Statement of Applicability v1.3; Risk Treatment Plan v1.3
- Information Security Objectives ISMS-OBJ-01 v1.0
- Management review minutes, 12 March 2026
- Access Control Procedure ISMS-PR-05 v2.0; access review records Q1-Q2 2026 (CRM, ERP, Microsoft 365)
- Backup Policy ISMS-PO-12 v1.1; backup job reports July-September 2026; restore test log
- Change records CHG-2207, CHG-2231 and CHG-2244
- Asset inventory (export 20 September 2026)
- Training records and phishing simulation reports Q2-Q3 2026

Persons interviewed (by role)

- Chief Operating Officer
- Head of IT and ISMS Manager
- HR Manager
- Infrastructure Lead
- Lead Developer
- Procurement Officer
- Two customer service staff (awareness interviews)