SAMPLE REPORT · FICTIONAL ORGANISATION

INSPECTION, TESTING & ASSURANCE

ISO/IEC 27001

Gap Assessment Report

ISO/IEC 27001:2022 Information Security Management System

Oasis Logistics (sample)

Head office, two regional warehouses and the online customer order platform

ASSESSED	16 November 2026
STANDARD	ISO/IEC 27001:2022 Information Security Management System
IN SCOPE	47 requirements, 46 applicable
PROFILE	Transport and logistics · 180 people
PREPARED BY	Quality and Information Security Team

CONTENTS

1 Executive summary

2 Readiness by area

3 Remediation plan

A How it was scored and how ITA can help

Confidential. Prepared for Oasis Logistics (sample) from its own self-assessment using the free ITA gap assessment tool. It has not been verified by ITA (see section A). Share on a need-to-know basis.

Where Oasis Logistics (sample) stands against ISO/IEC 27001

OVERALL READINESS

58.2%

Level 2 · Developing

The programme is under way, with material gaps an auditor would find.

Initial | **Developing** | Established | Audit-ready

APPLICABLE	EVIDENCED	OPEN GAPS	HIGH PRIORITY
46	11	35	14

STATUS OF EVERY REQUIREMENT



Not started · Planned · Partially implemented · Implemented, not evidenced · Implemented and evidenced · Not applicable

GAPS WITH AN OWNER	WITH A TARGET DATE	NOT ANSWERED
25 OF 35	20 OF 35	0

WHAT THIS ASSESSMENT TELLS YOU

- Overall readiness is 58.2% against ISO/IEC 27001 across 46 applicable requirements; 11 are implemented and evidenced.
- Most work is needed in Performance evaluation (29%). The strongest area is Support (75%).
- 2 management system clauses score under half. Clauses cannot be excluded, so each is a likely major nonconformity at a certification audit.
- 11 requirements operate but are not evidenced. Collecting their records alone lifts the score to 64.1% (+6.0 points).
- 14 gaps are high priority (not started or only planned); 4 of them are in Performance evaluation.
- 10 open gaps have no owner yet. Work without an owner rarely gets done.

DO THESE FIRST

	PRIORITY	ACTION	OWNER
1	HIGH	**Monitoring and measurement** 9.1 · Agree a short list of indicators, their frequency and owner, and review them monthly.	HR Manager
2	HIGH	**Internal audit** 9.2 · Train two or three internal auditors, plan an audit programme covering all requirements and run the first audits.	IT Manager
3	HIGH	**Management review** 9.3 · Schedule the first management review and use an agenda that covers every required input.	Information Security Officer

Analysis and priorities

IN ONE SENTENCE

At 58.2%, the work is under way, but Performance evaluation and the high-priority gaps still need attention before an auditor arrives.

FOR SENIOR MANAGEMENT AND THE BOARD

Our self-assessment against ISO/IEC 27001 gives an overall score of 58.2%, which places us at level 2 of 4 (Developing). There are 35 open gaps, 14 of them high priority. Our weakest area is Performance evaluation (29%) and our strongest is Support (75%). 11 requirements already operate but cannot yet be proven; collecting their records alone would lift the score to 64.1%. We ask management to approve the remediation plan, give every open gap an owner and a date, and review progress monthly.

WHERE YOU STAND

The self-assessment places Oasis Logistics (sample) at level 2 of 4 (Developing), with an overall score of 58.2% across 46 applicable requirements. 11 requirements are implemented and evidenced, and 35 remain open. Some management system clauses score under half: Performance evaluation (29%), Planning (46%).

WHAT IT MEANS

14 requirements are not started or only planned. These are the ones an auditor reaches first, and in management system clauses each one is a likely major nonconformity. 10 are partly in place: the approach exists but is not yet applied across the whole scope. 11 operate without records. Auditors sample records, not intentions, so these will be raised as findings until the evidence is in place. Until these gaps are closed, a certification audit is unlikely to recommend certification.

WHERE TO FOCUS FIRST

Start with the high-priority gaps in the weakest areas, because they carry the most audit risk. In parallel, gather the evidence for what already runs: it is the cheapest gain and takes the score to 64.1%. Finishing what is partly in place then takes it to 75.0%. Give each gap an owner and a target date; today 25 of 35 have an owner and 20 have a date.

PRIORITIES

	PRIORITY	WHY IT MATTERS	FIRST STEP	WITHIN
1	**Monitoring and measurement** 9.1	Without measurement you cannot tell whether the system works or where to improve.	Agree a short list of indicators, their frequency and owner, and review them monthly.	30 DAYS
2	**Internal audit** 9.2	A certification body expects at least one full internal audit cycle before the certification audit.	Train two or three internal auditors, plan an audit programme covering all requirements and run the first audits.	30 DAYS
3	**Management review** 9.3	Management review is mandatory evidence that leadership oversees the system; it cannot be skipped.	Schedule the first management review and use an agenda that covers every required input.	60 DAYS
4	**Risks and opportunities** 6.1	Risk-based planning is at the heart of every modern management system standard and is examined closely at audit.	Create a risk and opportunity register for each main process, with an owner, an action and a review date.	60 DAYS
5	**Information security risk assessment** 6.1.2	The risk assessment is the backbone of the ISMS; every control decision depends on it.	Agree a risk method with criteria and owners, then assess risks for your main information assets.	90 DAYS

30 / 60 / 90-DAY ROADMAP

FIRST 30 DAYS

- Agree a short list of indicators, their frequency and owner, and review them monthly.
- Train two or three internal auditors, plan an audit programme covering all requirements and run the first audits.
- Gather documented evidence for the 11 requirements that already operate.

DAYS 31 TO 60

- Schedule the first management review and use an agenda that covers every required input.
- Create a risk and opportunity register for each main process, with an owner, an action and a review date.
- Give an owner and a realistic target date to every high-priority gap.
- Train internal auditors and plan the internal audit programme.

DAYS 61 TO 90

- Agree a risk method with criteria and owners, then assess risks for your main information assets.
- Run the first full internal audit cycle and close its findings.
- Hold a management review to confirm readiness and resources.
- Repeat this self-assessment, then agree the audit dates with a certification body.

2 · READINESS BY AREA

Maturity across the standard

Each bar shows how the requirements in one area break down by status. The score is the average across applicable requirements; the chips count open gaps by priority (high, medium, low).

AREA	STATUS MIX	SCORE	GAPS H · M · L
Context of the organisation	1 · 1 · 1 · 2	70%	1 · 1 · 1
Leadership	1 · 1 · 1 · 2	70%	1 · 1 · 1
Planning	1 · 2 · 2 · 1 · 1	46%	3 · 2 · 1
Support	1 · 1 · 2 · 3	75%	1 · 1 · 2
Operation	1 · 1 · 1	50%	1 · 1 · 1
Performance evaluation	2 · 2 · 1 · 1	29%	4 · 1 · 1
Improvement	1 · 1	63%	0 · 1 · 1
Annex A controls	1 · 2 · 2 · 3 · 3 · 1	61%	3 · 2 · 3

Not started · Planned · Partially implemented · Implemented, not evidenced · Implemented and evidenced · Not applicable

WHERE THE NEXT POINTS COME FROM

The score after each kind of work, cheapest first. Gold is what that step adds.

Today		58.2%
Evidence what already runs 11 requirements		64.1% +6.0
Finish what is partly in place 10 requirements		75.0% +10.9
Implement what is planned 10 requirements		91.3% +16.3
Start what has not begun 4 requirements		100.0% +8.7

HOW ITA CAN HELP

Close the gaps faster with support from people who implement and audit these systems every day.

Consultancy and gap analysis
Implementation support until certification
View the service

Implementation course
Three days, practical, for the team that builds the system
View the course

Internal Auditor course
Plan and run your internal audits
View the course

Talk to an expert
Free call to review this report with you
Contact us

Every open gap, grouped by what has to happen next

Work from the top. Requirements not yet started or only planned are the ones an auditor reaches first; the last group already operates and needs only its records.

HIGH Not started · 4

Start from a documented baseline: agree the approach, write it down, then put it into operation.

REF	REQUIREMENT	AREA	OWNER · TARGET	NEXT STEP
6.1.2	Information security risk assessment Is there a defined risk assessment method with criteria, risk owners and repeatable results?	Planning	HR Manager 2 May 2027	Agree a risk method with criteria and owners, then assess risks for your main information assets.
9.1	Monitoring and measurement Are results analysed and evaluated to judge performance and the effectiveness of the system?	Performance evaluation	Operations Manager 26 Jan 2027	Agree a short list of indicators, their frequency and owner, and review them monthly.
9.2	Internal audit Are audit results reported to management and findings followed up to closure?	Performance evaluation	IT Manager 13 Feb 2027	Train two or three internal auditors, plan an audit programme covering all requirements and run the first audits.
A	ICT readiness for business continuity (A.5.30) Are ICT continuity requirements defined, implemented and tested?	Annex A controls	IT Manager 14 Jan 2027	Define recovery objectives for critical systems and test a restore.

HIGH Planned · 10

Move from plan to implementation. Assign an owner and a date, then put the arrangement into operation.

REF	REQUIREMENT	AREA	OWNER · TARGET	NEXT STEP
4.4	System and its processes Are the processes needed, their sequence, interactions, owners, criteria and indicators defined?	Context of the organisation	Compliance Lead 19 Feb 2027	Draw a one-page process map and give each process an owner, inputs, outputs and one or two indicators.
5.2	Policy Is the policy communicated, understood and available to relevant interested parties?	Leadership	To assign 27 Mar 2027	Review the policy with top management, approve it, and brief every team on what it means for their work.
6.1	Risks and opportunities Is the effectiveness of the actions taken on risks and opportunities evaluated?	Planning	To assign	Create a risk and opportunity register for each main process, with an owner, an action and a review date.
6.2	Objectives and planning Do plans for each objective state what, resources, who, when and how results are evaluated, and are they monitored?	Planning	IT Manager	Set three to five measurable objectives for the year, each with an owner, resources, a deadline and a tracking method.

REF	REQUIREMENT	AREA	OWNER · TARGET	NEXT STEP
7.5	Documented information Is documented information controlled for identification, review, approval, version, access and protection?	Support	HR Manager 2 Apr 2027	Set up a master list of documents with owners and versions, and agree where records are kept and for how long.
8.1	Operational planning and control Are externally provided processes, products and services that affect the system identified and controlled?	Operation	IT Manager	Pick the three most critical processes and define their criteria, controls and the records that prove them.
9.1	Monitoring and measurement Is it defined what is monitored and measured, the methods, frequency and who analyses the results?	Performance evaluation	HR Manager	Agree a short list of indicators, their frequency and owner, and review them monthly.
9.3	Management review Does top management review the system at planned intervals, covering all required inputs?	Performance evaluation	Information Security Officer	Schedule the first management review and use an agenda that covers every required input.
A	Supplier and cloud security (A.5.19, A.5.23) Are security requirements agreed with suppliers and cloud providers and their performance monitored?	Annex A controls	To assign 26 Apr 2027	List critical suppliers and cloud services and agree security requirements with each.
A	Malware and vulnerability management (A.8.7, A.8.8) Are malware protection and timely patching of technical vulnerabilities in place?	Annex A controls	To assign 19 Feb 2027	Set patching timelines by severity and track compliance monthly.

MEDIUM **Partially implemented · 10**

Extend the existing approach to the whole scope and apply it consistently, then evidence it.

REF	REQUIREMENT	AREA	OWNER · TARGET	NEXT STEP
4.2	Interested parties Are interested parties and their relevant requirements identified, including which become compliance obligations?	Context of the organisation	To assign 1 Feb 2027	Build a simple table of interested parties, their needs, and whether each need is a binding obligation for you.
5.1	Leadership and commitment Are the system requirements integrated into business processes rather than run in parallel?	Leadership	Information Security Officer 9 Mar 2027	Put the system on the agenda of the monthly management meeting, with results, decisions and resources recorded.
6.1	Risks and opportunities Are risks and opportunities determined, with actions planned and integrated into processes?	Planning	IT Manager 14 Apr 2027	Create a risk and opportunity register for each main process, with an owner, an action and a review date.
6.2	Objectives and planning Are measurable objectives set at relevant functions and levels, consistent with the policy?	Planning	To assign 20 Jan 2027	Set three to five measurable objectives for the year, each with an owner, resources, a deadline and a tracking method.

REF	REQUIREMENT	AREA	OWNER · TARGET	NEXT STEP
7.2	Competence Are training and other actions taken to close competence gaps, and is their effectiveness evaluated?	Support	Compliance Lead	Build a competence matrix for key roles and close the biggest gaps with targeted training.
8.1	Operational planning and control Are operational processes planned and controlled against defined criteria, with records showing they ran as planned?	Operation	Compliance Lead 20 Apr 2027	Pick the three most critical processes and define their criteria, controls and the records that prove them.
9.2	Internal audit Is there an internal audit programme covering all requirements, run by competent and impartial auditors?	Performance evaluation	To assign	Train two or three internal auditors, plan an audit programme covering all requirements and run the first audits.
10.1	Continual improvement Is continual improvement visible in indicator trends, completed improvement actions and lessons learned?	Improvement	Operations Manager	Keep an improvement log and show at each management review what was improved and what results changed.
A	Access control and privileged access (A.5.15, A.8.2) Are access rights granted on need-to-know, reviewed periodically and privileged rights restricted?	Annex A controls	HR Manager	Run an access review for key systems and remove unnecessary and privileged rights.
A	Awareness and training (A.6.3) Do staff receive regular security awareness, including phishing and reporting duties?	Annex A controls	HR Manager 1 Feb 2027	Launch a short awareness programme and a phishing simulation.

LOW **Implemented, not evidenced · 11**

Collect and file evidence an auditor can sample. The control is operating; what is missing is the record of it.

REF	REQUIREMENT	AREA	OWNER · TARGET	NEXT STEP
4.1	Organisation and its context Have you determined whether climate change is a relevant issue for the organisation?	Context of the organisation	Information Security Officer	Run a one-hour workshop with managers to list internal and external issues (SWOT or PESTLE), then record them with a review date.
5.2	Policy Is there an approved policy appropriate to the organisation, with a commitment to meet requirements and improve?	Leadership	HR Manager	Review the policy with top management, approve it, and brief every team on what it means for their work.
6.1.3	Risk treatment and Statement of Applicability Is there a risk treatment plan approved by risk owners and a Statement of Applicability justifying each Annex A control?	Planning	Operations Manager	Prepare a risk treatment plan and a Statement of Applicability justifying each Annex A control.
7.2	Competence Are competence requirements defined for each role affecting performance, with evidence of competence?	Support	Operations Manager 25 Feb 2027	Build a competence matrix for key roles and close the biggest gaps with targeted training.

3 · REMEDIATION PLAN

REF	REQUIREMENT	AREA	OWNER · TARGET	NEXT STEP
7.4	Communication Are internal and external communications planned: what, when, with whom, how and who communicates?	Support	Information Security Officer	Prepare a one-page communication plan: what, when, with whom, how and who is responsible.
8.2	Performing risk assessments Are risk assessments repeated at planned intervals and when significant changes occur?	Operation	To assign 8 May 2027	Set a review frequency and triggers for repeating the risk assessment.
9.3	Management review Do review outputs record decisions on improvement, changes and resources, with actions followed up?	Performance evaluation	To assign 3 Mar 2027	Schedule the first management review and use an agenda that covers every required input.
10.2	Nonconformity and corrective action Are nonconformities corrected, root causes analysed, corrective actions taken and their effectiveness checked?	Improvement	Compliance Lead 21 Mar 2027	Use one corrective action form with root cause analysis (5 Whys or fishbone) and an effectiveness check.
A	Inventory and classification of information (A.5.9, A.5.12) Is there an inventory of information and assets with owners, and is information classified and labelled?	Annex A controls	Information Security Officer 8 Apr 2027	Create an asset inventory with owners and a simple classification scheme.
A	Legal and contractual requirements (A.5.31) Are legal, regulatory and contractual security requirements, including national cybersecurity controls, identified?	Annex A controls	To assign	List legal, regulatory and contractual security requirements, including national controls such as NCA ECC.
A	Backup, logging and monitoring (A.8.13, A.8.15, A.8.16) Are backups tested for restore, and are logs collected, protected and reviewed?	Annex A controls	IT Manager	Test a restore from backup and confirm logs are collected for critical systems.

How it was scored

STATUS WEIGHTS

STATUS	WEIGHT	MEANING
Not started	0.00	No policy, process or activity exists yet.
Planned	0.25	Approach agreed and scheduled, but nothing in place yet.
Partially implemented	0.50	In place for part of the scope, or applied inconsistently.
Implemented, not evidenced	0.75	Working as intended, but you could not prove it today.
Implemented and evidenced	1.00	Working as intended, with records an auditor can sample.
Not applicable	–	A justified exclusion, removed from the score.

READINESS LEVELS

1 · Initial (0%+)

Most requirements are not yet in place. Build the foundations before thinking about an audit.

2 · Developing (40%+)

The programme is under way, with material gaps an auditor would find.

3 · Established (65%+)

Most controls operate. Remaining work is closing specific gaps and evidencing what runs.

4 · Audit-ready (85%+)

Requirements operate and are evidenced. Ready for an internal audit and an external audit.

A management system clause scoring under 50% holds the level at Developing, because clauses cannot be excluded from a certification scope.

BASIS OF THIS REPORT AND LIMITATION OF LIABILITY

This report is the output of a self-assessment. The scores, levels, findings and recommendations come only from the information entered by the organisation. ITA has not reviewed, verified, tested or audited that information or the organisation's systems.

The accuracy of the results depends entirely on the accuracy and completeness of those answers. ITA gives no assurance, certification or audit opinion, and accepts no liability for decisions taken, or not taken, in reliance on this report.

The analysis is generated automatically from the scores, for planning only. It is not legal or professional advice and does not replace an independent assessment or a certification audit.

A requirement that operates but cannot be evidenced scores 0.75, not 1.00. Auditors sample records, not intentions, so closing that distance is usually the fastest route to a higher score. All questions are written in ITA's own words; clause numbers are used as references only and no text of the standard is reproduced. Work from your licensed copy of the standard.

YOUR WORKBOOK

The Excel workbook from the same tool follows the same sections and colours. Change a status there and every score, level and summary updates.

TALK TO ITA

Consultancy and gap analysis
Implementation support until certification
View the service

Implementation course
Three days, practical, for the team that builds the system
View the course

Internal Auditor course
Plan and run your internal audits
View the course

Talk to an expert
Free call to review this report with you
Contact us

ITA – Inspection, Testing & Assurance Company · ita-cert.co.uk · info@ita-cert.co.uk