SAMPLE REPORT - FICTIONAL ORGANISATION

GOVERNANCE DOCS

ISO/IEC 27001:2022

Gap Assessment Report

ISO/IEC 27001:2022 Information Security Management System

Harbour Logistics (sample)

Information security for the head office, the two regional warehouses and the customer order platform.

ASSESSED	25 September 2026
EDITION	2022, incorporating Amendment 1:2024 (climate action)
IN SCOPE	120 requirements, 115 applicable
PROFILE	Transport and logistics · 50 to 249 people
PREPARED BY	Governance Docs

CONTENTS

Where Harbour Logistics (sample) stands against ISO 27001

OVERALL READINESS

55.0%

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
115	20	95	34

STATUS OF EVERY REQUIREMENT

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

GAPS WITH AN OWNER	WITH A TARGET DATE	NOT ANSWERED
48 of 95	27 of 95	3

WHAT THIS ASSESSMENT TELLS YOU

- Overall readiness is 55.0% against ISO 27001 across 115 applicable controls. 20 of them are implemented and evidenced.
- Most open gaps: A.5 - Organizational controls, with 33 at 46%. Strongest area: Clause 5 - Leadership at 92%.
- 3 management-system clauses score under half: Clause 6 - Planning (40%); Clause 9 - Performance evaluation (25%); Clause 10 - Improvement (25%). Clauses cannot be excluded, and each is a likely major nonconformity at a certification audit.
- 28 controls are operating but not evidenced. Collecting their records alone lifts the score to 61.1% (+6.1 points), the cheapest gain available.
- 34 gaps are high priority (not started or only planned); 15 of them are in A.5 - Organizational controls.
- 3 controls were left unanswered and are excluded from the score, which will move when they are completed.

DO THESE FIRST

	PRIORITY	ACTION	OWNER	START FROM
1	HIGH	**Bring every management-system clause above 50%, starting with 6.1.2 Information security risk assessment; 9.2 Internal audit; 10.1 Continual improvement**	Compliance Lead	ISMS Risk Assessment and Treatment
2	HIGH	**Put an owner and date against the 15 high-priority gaps in A.5 - Organizational controls**	Compliance Lead	Threat Intelligence Policy
3	MEDIUM	**Adopt and tailor the Access Control Policy, which closes 7 open gaps**	To assign	Access Control Policy

Analysis and priorities

IN ONE SENTENCE

At 55% and Level 2, the ISMS is under way but not yet auditable; start internal audit and finish the risk process first.

AI-assisted analysis, generated from the information the organization provided and checked automatically against the scores and findings in this report. It supports planning and is not an audit opinion; see "Basis of this report and limitation of liability".

FOR SENIOR MANAGEMENT AND THE BOARD

Our information security programme is at Level 2 of 4, Developing, with a score of 55%. Day-to-day controls are partly in place, but the parts that prove they work, such as risk assessment, internal audit and management review, are largely missing. The main exposure is access control and supplier security. We need a named programme owner, time from department heads, and agreement to complete the risk assessment and first internal audit before seeking certification.

WHERE YOU STAND

The organization is at Level 2, Developing, with a readiness score of 55% across 115 applicable requirements. 20 requirements are implemented and evidenced, but 95 remain open and 34 of those are high priority. The management system clauses are uneven: leadership scores well at 91.7%, while planning sits at 40% and performance evaluation and improvement at 25%. That pattern usually means controls exist in practice but the system that plans, checks and improves them has not been built yet.

WHAT IT MEANS FOR THE ORGANIZATION

For a logistics business of 50 to 249 people, the practical consequence is that customers and partners asking for assurance will find gaps in exactly the areas they test first: risk assessment, internal audit and management review. Organizational controls are the largest pool of work, with 33 open gaps at 45.9%, followed by technological controls with 24 open gaps at 54%. Access control, supplier security and monitoring are where a real incident would expose the weakest links.

WHERE TO FOCUS FIRST

The fastest improvement comes from evidencing what already runs, which lifts the score to 61.1%, and from finishing what is partly in place, which takes it to 75.4%. Owners are named for 48 gaps but only 27 have a target date, so the first job is turning this list into a dated plan.

PRIORITIES

	PRIORITY	WHY IT MATTERS	FIRST STEP	START FROM	WITHIN
1	**Complete the information security risk assessment and treatment** 6.1.2 Information security risk assessment · 6.1.3 Information security risk treatment	Every other control decision depends on the risk assessment; without it, spending cannot be justified and an auditor will raise a major nonconformity.	Hold a two-hour workshop with operations, IT and finance to list assets and threats in the risk register.	ISMS Risk Assessment and Treatment ISO 27001 Toolkit - 165 Comprehensive Templates	30 DAYS
2	**Plan and run the first internal audit** 9.2 Internal audit	Internal audit has not started, so nobody independent has checked whether controls work before a customer or certification body does.	Appoint an internal auditor who does not own any of the controls and agree the audit scope.	ISMS Internal Audit Procedure ISO 27001 Toolkit - 165 Comprehensive Templates	60 DAYS
3	**Put access control and authentication on a written footing** A.5.15 Access control · A.5.17 Authentication information	Access control has not started, which is the most common route for account misuse and the first thing customers ask about.	Export the user list for the order platform and warehouse systems and remove leavers this week.	Access Control Policy ISO 27001 Toolkit - 165 Comprehensive Templates	30 DAYS
4	**Bring key suppliers under security terms** A.5.20 Addressing information security within supplier agreements · A.5.21 Managing information security in the ICT supply chain	Supplier security is only planned, so a courier or software vendor could introduce a weakness you have no contractual lever to fix.	List the five suppliers with access to your systems or data and check their current contract terms.	Vendor Security Agreement	60 DAYS
5	**Hold a management review and log improvements** 9.3 Management review · 10.1 Continual improvement	Management review is planned but not held, so leadership has no regular point to decide on risks, resources and results.	Book the first management review meeting for next month and circulate the agenda.	ISMS Management Review Meeting Agenda	90 DAYS

30 / 60 / 90-DAY ROADMAP

FIRST 30 DAYS

- Name a programme owner and confirm the scope with leadership
- Run the risk workshop and populate the risk register
- Remove leaver accounts and publish the access control policy

DAYS 31 TO 60

- Approve the risk treatment plan and Statement of Applicability
- Agree security terms with the five key suppliers
- Complete the first internal audit of the management system clauses

DAYS 61 TO 90

- Hold the first management review and record decisions
- Start collecting evidence for controls that already operate
- Re-run this assessment to measure progress

Maturity across the standard

Each bar shows how the requirements in one area break down by status, weakest on the left. The score is the average across applicable requirements; the chips count open gaps by priority.

MANAGEMENT SYSTEM CLAUSES	STATUS MIX	SCORE	GAPS H · M · L
Clause 4 - Context	1 · 2 · 1	75%	0 · 1 · 2
Clause 5 - Leadership	1 · 2	92%	0 · 0 · 1
Clause 6 - Planning	2 · 3	40%	2 · 3 · 0
Clause 7 - Support	1 · 2 · 3 · 1	64%	1 · 2 · 3
Clause 8 - Operation	1 · 2	58%	1 · 0 · 2
Clause 9 - Performance evaluation	1 · 1 · 1	25%	2 · 1 · 0
Clause 10 - Improvement	2	25%	2 · 0 · 0

ANNEX A CONTROLS	STATUS MIX	SCORE	GAPS H · M · L
A.5 - Organizational controls	6 · 9 · 11 · 7 · 4	46%	15 · 11 · 7
A.6 - People controls	1 · 3 · 3 · 1	63%	1 · 3 · 3
A.7 - Physical controls	6 · 4 · 2	77%	1 · 1 · 6
A.8 - Technological controls	4 · 5 · 11 · 4 · 7 · 3	54%	9 · 11 · 4

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

WHERE THE NEXT POINTS COME FROM

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

Today	55.0%	
Evidence what already runs 28 requirements	61.1%	+6.1
Finish what is partly in place 33 requirements	75.4%	+14.3
Implement what is planned 23 requirements	90.4%	+15.0
Start what has not begun 11 requirements	100.0%	+9.6

DOCUMENTS THAT CLOSE THE MOST GAPS

Each bar counts the open gaps that name the document as the way to close them.

Access Control Policy	7
Incident Response Procedure	6
IT Systems Monitoring Procedure	5
Security Incident Procedure	5
ISMS Management Plan	4
ISMS Risk Treatment Plan	4

All of these are in the ISO 27001 Toolkit (175 documents).

Every open gap, grouped by what has to happen next

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

HIGH **Not started · 11**

Start from a documented baseline: adopt and tailor the document named below, then put it into operation.

Ref	Requirement	Area	Owner · target	Closes it
9.2	Internal audit	Clause 9	Compliance Lead 26 Nov 2026	ISMS Internal Audit Procedure · ISMS Audit Plan +3 more
A.5.7	Threat intelligence	A.5	Compliance Lead 12 Nov 2026	Threat Intelligence Policy
A.5.10	Acceptable use of information and other associated assets	A.5	To assign	Acceptable Use Policy · Internet Acceptable Use Policy +1 more
A.5.15	Access control	A.5	Compliance Lead	Access Control Policy
A.5.17	Authentication information	A.5	Compliance Lead 12 Nov 2026	Password Reset Procedure · Access Control Policy +1 more
A.5.29	Information security during disruption	A.5	To assign	Business Continuity Plan · Roles and Responsibilities for Contingency Planning +1 more
A.5.33	Protection of records	A.5	Compliance Lead 21 Jan 2027	Control of Records Procedure · Data Retention Policy
A.8.16	Monitoring activities	A.8	IT Manager	IT Systems Monitoring Procedure · Log Monitoring Policy
A.8.21	Security of network services	A.8	To assign	Network Security Policy · Standard SLA
A.8.22	Segregation of networks	A.8	To assign	Network Security Policy
A.8.30	Outsourced development	A.8	IT Manager 12 Nov 2026	Model Policy on Outsourcing · Vendor Security Agreement +1 more

HIGH **Planned · 23**

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

Ref	Requirement	Area	Owner · target	Closes it
6.1.2	Information security risk assessment	Clause 6	Compliance Lead	ISMS Risk Assessment and Treatment · ISMS Information Risk Register +2 more
6.1.3	Information security risk treatment	Clause 6	Compliance Lead 24 Dec 2026	ISO 27001:2022 Statement of Applicability · ISMS Risk Treatment Plan +1 more
7.4	Communication	Clause 7	Compliance Lead 29 Oct 2026	ISMS Communication Plan

8.2	Information security risk assessment (operational)	Clause 8	Compliance Lead	ISMS Risk Assessment and Treatment · ISMS Information Risk Register
9.3	Management review	Clause 9	Compliance Lead 24 Dec 2026	ISMS Management Review Meeting Agenda · ISMS MRM Agenda
10.1	Continual improvement	Clause 10	To assign	Continuous Improvement Procedure · ISMS Continuous Improvement Log
10.2	Nonconformity and corrective action	Clause 10	Compliance Lead 29 Oct 2026	ISMS Nonconformity Management Procedure · Corrective Action Procedure +1 more
A.5.4	Management responsibilities	A.5	Compliance Lead 29 Oct 2026	ISMS Roles and Responsibilities · Model Policy on Information Security
A.5.5	Contact with authorities	A.5	Compliance Lead 12 Nov 2026	Incident Response Procedure · Security Incident Procedure
A.5.6	Contact with special interest groups	A.5	Compliance Lead	Threat Intelligence Policy
A.5.11	Return of assets	A.5	Compliance Lead	Employee Movement and Termination Checklist · Asset Handling Policy
A.5.20	Addressing information security within supplier agreements	A.5	To assign	Vendor Security Agreement · Standard SLA +1 more
A.5.21	Managing information security in the ICT supply chain	A.5	Compliance Lead	Vendor Management Policy · Vendor Evaluation Process
A.5.22	Monitoring, review and change management of supplier services	A.5	To assign	Vendor Management Policy · Vendor Access Procedure
A.5.28	Collection of evidence	A.5	Compliance Lead 12 Nov 2026	Incident Response Procedure · Security Incident Procedure
A.5.34	Privacy and protection of PII	A.5	Compliance Lead	Privacy Officer JD · Data Retention Policy +1 more
A.6.3	Information security awareness, education and training	A.6	HR Manager 10 Dec 2026	Awareness Presentation · Model Policy on Security Awareness and Training +1 more
A.7.10	Storage media	A.7	Facilities Manager	Removable Media Management Procedure · Media Disposal Procedure +1 more
A.8.14	Redundancy of information processing facilities	A.8	To assign	Business Continuity Plan · ISMS Business Impact Analysis (BIA) Procedure
A.8.15	Logging	A.8	IT Manager 4 Feb 2027	Log Monitoring Policy · IT Systems Monitoring Procedure
A.8.19	Installation of software on operational systems	A.8	IT Manager	Software Policy · Release Management Policy
A.8.20	Networks security	A.8	IT Manager 12 Nov 2026	Network Security Policy · Network Risk Manager JD
A.8.28	Secure coding	A.8	IT Manager	Secure Coding Policy

MEDIUM **Partially implemented · 33**

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

Ref	Requirement	Area	Owner · target	Closes it
4.3	Determining the scope of the ISMS	Clause 4	Compliance Lead 4 Feb 2027	ISMS Context and Scope · Organization of Information Security
6.1.1	Actions to address risks and opportunities	Clause 6	To assign	ISMS Management Plan · ISMS Risk Assessment and Treatment
6.2	Information security objectives and planning	Clause 6	To assign	ISMS Monitoring and Evaluation · ISMS Management Plan
6.3	Planning of changes	Clause 6	Compliance Lead 26 Nov 2026	Change Management Policy · Model Policy on Change Management and Control
7.5.2	Creating and updating documented information	Clause 7	Compliance Lead	Documented Information Control Procedure · Control of Records Procedure
7.5.3	Control of documented information	Clause 7	Compliance Lead	Documented Information Control Procedure · Data Retention Policy +1 more
9.1	Monitoring, measurement, analysis and evaluation	Clause 9	Compliance Lead	ISMS Monitoring and Evaluation · Information Security Program Maturity Assessment Tool +1 more
A.5.1	Policies for information security	A.5	Compliance Lead 29 Oct 2026	Information Security Policy · ISMS Policy +1 more
A.5.3	Segregation of duties	A.5	Compliance Lead 26 Nov 2026	Segregation of Duties Policy
A.5.8	Information security in project management	A.5	Compliance Lead	Project Management Security Policy · ISMS Project Initiation Document +1 more
A.5.16	Identity management	A.5	To assign	Access Control Policy · Permissions Manager JD
A.5.25	Assessment and decision on information security events	A.5	Compliance Lead 26 Nov 2026	Security Incident Procedure · Incident Response Procedure
A.5.26	Response to information security incidents	A.5	Compliance Lead 24 Dec 2026	Incident Response Procedure · Security Incident Procedure
A.5.27	Learning from information security incidents	A.5	To assign	Incident Response Procedure · ISMS Continuous Improvement Log
A.5.31	Legal, statutory, regulatory and contractual requirements	A.5	Compliance Lead	Legal and Regulatory Requirements Policy · Legal Responsibilities Policy
A.5.35	Independent review of information security	A.5	To assign	ISMS Internal Audit Procedure · ISMS Auditing Guideline +1 more
A.5.36	Compliance with policies, rules and standards	A.5	Compliance Lead 12 Nov 2026	Compliance Manager JD · ISMS Monitoring and Evaluation

A.5.37	Documented operating procedures	A.5	Compliance Lead	ISMS Operating Procedure · Documented Information Control Procedure
A.6.1	Screening	A.6	HR Manager 4 Feb 2027	Employee Screening Checklist · Recruitment and New Joiner Checklist
A.6.6	Confidentiality or non-disclosure agreements	A.6	HR Manager 7 Jan 2027	Standard NDA · Vendor Security Agreement
A.6.8	Information security event reporting	A.6	To assign	Security Incident Procedure · Incident Response Procedure
A.7.5	Protecting against physical and environmental threats	A.7	Facilities Manager	Physical Security Policy · Physical Security Design Policy
A.8.5	Secure authentication	A.8	To assign	Access Control Policy · Password Reset Procedure
A.8.6	Capacity management	A.8	To assign	IT Systems Monitoring Procedure
A.8.8	Management of technical vulnerabilities	A.8	To assign	Vulnerability Management Policy · Vulnerability Assessment Procedure
A.8.9	Configuration management	A.8	To assign	Configuration Management Procedure
A.8.13	Information backup	A.8	IT Manager	Backup Policy · Data Restoration Form
A.8.17	Clock synchronization	A.8	IT Manager 26 Nov 2026	IT Systems Monitoring Procedure
A.8.18	Use of privileged utility programs	A.8	To assign	Access Control Policy · Software Policy
A.8.23	Web filtering	A.8	IT Manager 29 Oct 2026	Internet Acceptable Use Policy · Internet Risk and Security Manager JD
A.8.25	Secure development life cycle	A.8	IT Manager	Secure Development Policy · Secure Systems Engineering Policy
A.8.27	Secure system architecture and engineering principles	A.8	IT Manager 21 Jan 2027	Secure Systems Engineering Policy
A.8.29	Security testing in development and acceptance	A.8	IT Manager	Secure Development Policy · Vulnerability Assessment Procedure

LOW **Implemented, not evidenced · 28**

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	Closes it
4.1	Understanding the organization and its context	Clause 4	To assign	ISMS Context and Scope
4.4	Information security management system	Clause 4	To assign	ISMS Management Plan · ISMS Operating Procedure +1 more

5.1	Leadership and commitment	Clause 5	To assign	Management Support Letter · ISMS Management Review Meeting Agenda +1 more
7.1	Resources	Clause 7	To assign	ISMS Management Plan · ISMS Implementation Project Estimator
7.2	Competence	Clause 7	To assign	Recruitment and New Joiner Checklist · Employee Screening Checklist
7.3	Awareness	Clause 7	To assign	Awareness Presentation · Model Policy on Security Awareness and Training
8.1	Operational planning and control	Clause 8	To assign	ISMS Operating Procedure · Model Policy on Outsourcing
8.3	Information security risk treatment (operational)	Clause 8	To assign	ISMS Risk Treatment Plan · ISMS Risk Treatment Plan
A.5.9	Inventory of information and other associated assets	A.5	To assign	ISMS Information Asset Inventory · Asset Inventory +2 more
A.5.12	Classification of information	A.5	To assign	Information Security Classification Policy · Information Classification Matrix +1 more
A.5.18	Access rights	A.5	To assign	Access Control Policy · Employee Movement and Termination Checklist
A.5.19	Information security in supplier relationships	A.5	To assign	Vendor Management Policy · Model Policy on Outsourcing
A.5.23	Information security for use of cloud services	A.5	To assign	Cloud Services Security Policy
A.5.30	ICT readiness for business continuity	A.5	To assign	ISMS Business Impact Analysis (BIA) Procedure · Business Continuity Plan +2 more
A.5.32	Intellectual property rights	A.5	To assign	Copyright Compliance Policy · Software Policy +1 more
A.6.2	Terms and conditions of employment	A.6	To assign	Employment Contract Clauses · Standard NDA
A.6.4	Disciplinary process	A.6	To assign	Employee Disciplinary Process
A.6.5	Responsibilities after termination or change of employment	A.6	To assign	Employee Movement and Termination Checklist · Standard NDA +1 more
A.7.3	Securing offices, rooms and facilities	A.7	To assign	Secure Areas Policy · Physical Security Design Policy
A.7.4	Physical security monitoring	A.7	To assign	Physical Security Policy · Physical Security Manager JD
A.7.7	Clear desk and clear screen	A.7	To assign	Physical Security Policy · Acceptable Use Policy
A.7.9	Security of assets off-premises	A.7	To assign	Offsite Assets Procedure · Mobile Computing Policy

A.7.11	Supporting utilities	A.7	To assign	Physical Security Policy · Business Continuity Plan
A.7.14	Secure disposal or re-use of equipment	A.7	To assign	Secure Data Disposal Policy · Media Disposal Procedure
A.8.3	Information access restriction	A.8	To assign	Access Control Policy
A.8.4	Access to source code	A.8	To assign	Secure Development Policy · Development Environment Policy
A.8.7	Protection against malware	A.8	To assign	Anti-Malware Policy · Model Policy on Malware +1 more
A.8.24	Use of cryptography	A.8	To assign	Cryptographic Policy

ANSWER **Not answered · 3**

Left blank, so not in the score yet. Answer these in the workbook or online; the score will move when you do.

Ref	Requirement	Area	Question to answer
A.8.31	Separation of development, test and production environments	A.8	Are development, testing and production environments separated and secured?
A.8.33	Test information	A.8	Is test information appropriately selected, protected and managed?
A.8.34	Protection of information systems during audit testing	A.8	Are audit tests and other assurance activities involving assessment of operational systems planned and agreed to minimise disruption?

A · ABOUT THIS REPORT

How it was scored

STATUS WEIGHTS

Status	Weight	Meaning
Not started	0.00	No policy, process or activity exists for this requirement.
Planned	0.25	Approach agreed and scheduled, but nothing is in place yet.
Partially implemented	0.50	In place for part of the scope, or inconsistently applied.
Implemented, not evidenced	0.75	Operating as intended, but you could not prove it to an auditor today.
Implemented and evidenced	1.00	Operating as intended, with records an auditor can sample.
Not applicable	—	A justified exclusion. Removed from the score - record why in your notes.

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%+)

Controls operate and are evidenced. Ready for an internal audit and a certification body.

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

WHAT THIS REPORT IS

BASIS OF THIS REPORT AND LIMITATION OF LIABILITY

This report is the output of a self-assessment. The scores, readiness levels, gaps, analysis and recommendations in this report are derived solely from the information entered by the organization, and have not been independently reviewed, verified, tested or audited by Governance Docs. Governance Docs did not conduct an independent assessment of the organization, its controls or its operations.

The accuracy and completeness of the results depend entirely on the accuracy and completeness of the information provided. Governance Docs gives no assurance, certification or audit opinion, and accepts no liability for any inaccuracy, omission or deviation arising from that information, or for any decision taken, or not taken, in reliance on this report.

The report, including any AI-assisted analysis, is provided for guidance and planning only. It does not constitute legal, regulatory or other professional advice, and it does not replace an independent assessment or a certification audit.

A control that is running but cannot be evidenced scores 0.75, not 1.00. Auditors sample records, not intentions. Closing that distance is usually the fastest route to a higher score.

All assessment questions and guidance are original wording by Governance Docs. Clause and control references are used as identifiers; no text from the standard is reproduced. You need your own licensed copy of the standard to implement it.

YOUR WORKBOOK

The Excel workbook that comes with this report follows the same sections and colours. Dashboard: sections 1 and 2, recalculated live. Assessment: every requirement; change a status and every score, chart and level updates. Remediation Plan: section 3, with owners, dates and progress since this report. How it was scored: this page.

Governance Docs · governancedocs.com