SAMPLE REPORT - FICTIONAL ORGANISATION

GOVERNANCE DOCS

Information Security Risk Assessment

Harbour Logistics (sample)

Head office, the two regional warehouses, and the cloud systems that run orders and finance.

ASSESSED	25 September 2026
METHOD	ISO/IEC 27001:2022, clauses 6.1.2 and 6.1.3
IN SCOPE	11 scope items, 14 risks
APPETITE	Medium and below (level 9 or less) accepted without treatment
PROFILE	Transport and logistics
PREPARED BY	Governance Docs

Confidential. Prepared for Harbour Logistics (sample). Contains details of information security risks, weaknesses and planned controls; share on a need-to-know basis.
Based on a self-assessment using information supplied by the organization. Not independently verified by Governance Docs; see "Basis of this report and limitation of liability".

CONTENTS

Where the organization's risks stand

PROCESS SCORE

91 / 100

Level 2 · Developing

The risks are identified, but gaps in rating or treatment would not survive an audit.

Held at Developing while 2 critical findings are open; the score alone would place it higher.

The score measures how complete and defensible the assessment is, not how risky the organization is.

RISKS	ABOVE APPETITE	CRITICAL	ABOVE AFTER TREATMENT	FINDINGS
14	8	0	2	6

WHAT THIS ASSESSMENT TELLS YOU

- 8 of 13 rated risks sit above your appetite line (Medium and below is acceptable).
- The highest risk is R-01, phishing leads to stolen credentials, at level 16 (High), owned by IT Manager.
- 1 risk above the line has no treatment decision yet (R-05). Until it has one, the treatment plan is incomplete.
- Planned treatment brings the number of risks above the line from 8 to 2.
- 1 risk is not rated yet, so it is missing from the heat map and the priority order.

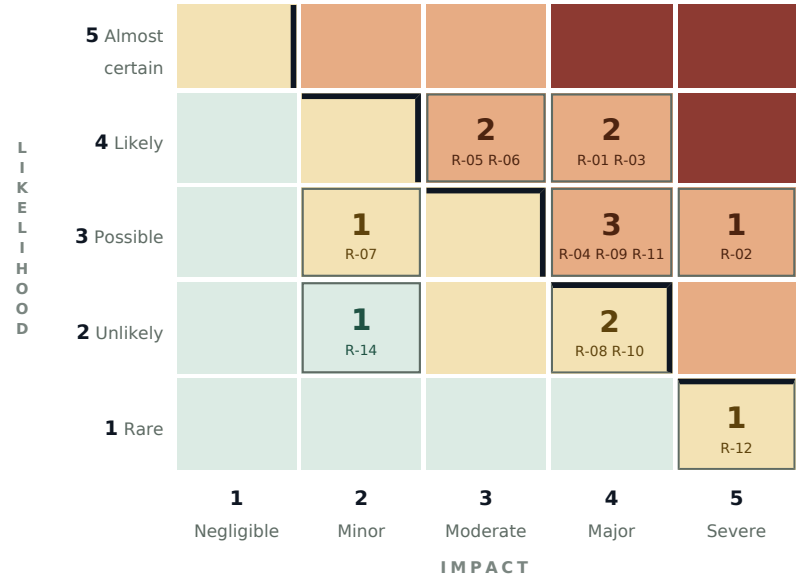
DO THESE FIRST

	SEVERITY	ACTION	RISKS	OWNER	DOCUMENT THAT CLOSES IT
1	CRITICAL	**Above the appetite line with no treatment decision** Choose modify, avoid, share or retain for each one, with the risk owner.	R-05	IT Manager	Risk treatment plan
2	CRITICAL	**Retained above the line without a recorded acceptance** Record who accepted each risk and when, after they have seen its level.	R-06	HR Manager	Risk acceptance form

Heat maps: today and after treatment

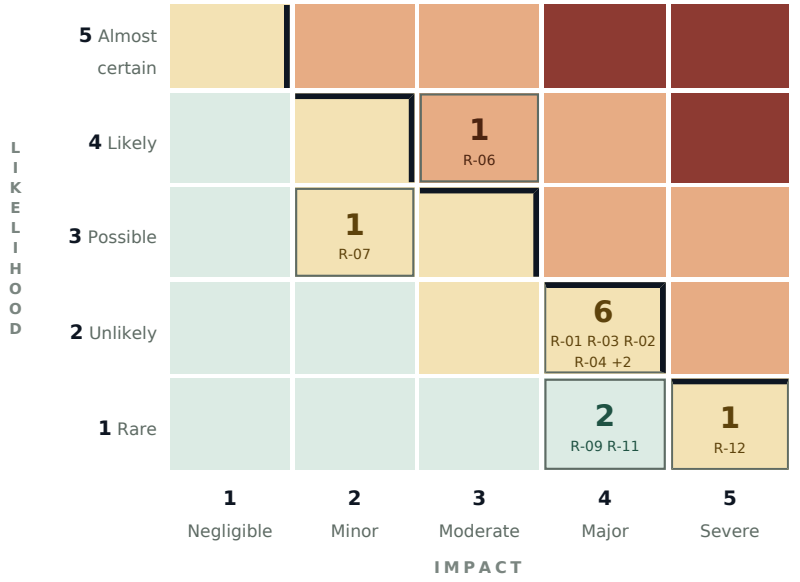
Each cell shows how many risks sit at that likelihood and impact, with their references. The heavy line is the appetite line: Medium and below (level 9 or less) is accepted without treatment. The second map shows where each risk is expected to be once its treatment is carried out; avoided risks are removed.

Current risk levels



13 of 14 risks rated.

Target levels after treatment



11 risks plotted; 1 removed by avoidance; risks above the line with no decision are not plotted.

Low 1–4 · Medium 5–9 · High 10–16 · Critical 17–25 · Appetite line

RISKS BY LEVEL

1 Low	4 Medium	8 High	1 Not rated

Analysis and priorities

IN ONE SENTENCE

The register is nearly complete; decide on the lost-device risk and record acceptance for leavers' access before anything else.

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

The organization has a largely complete information security risk assessment: 14 risks identified, 8 above our appetite line, and treatment planned that brings that number to 2. Two decisions are outstanding. We need a treatment decision on lost or stolen devices, and the owner of leavers' access must either approve a treatment or formally accept the risk. With those recorded, the assessment is ready for management review.

WHERE YOU STAND

You have identified 14 risks across all 11 scope items, and 13 are rated. Your process score is 91 out of 100, but the level is held at Developing because 2 critical findings remain: one risk above your appetite line has no treatment decision, and one is being retained above the line without a recorded acceptance. Everything else in the method is largely in place.

WHAT IT MEANS FOR THE ORGANIZATION

8 risks sit above your appetite line, all of them High, and they cluster around people and access: phishing, unpatched systems, ransomware, lost devices and leavers who keep their access. If these materialise together, the likely result is a data breach and an outage of the order and warehouse systems at the same time. Your planned treatment brings the number above the line from 8 to 2, which is a strong position once the gaps are closed.

WHERE TO FOCUS FIRST

Close the 2 critical findings first, because they are what an auditor would raise and what holds the level back. Then finish the loose ends: rate the managed IT provider's remote access, give the paper-policy risk an owner, and collect the residual-risk acceptance for unpatched systems. The treatments themselves are already scheduled and owned.

PRIORITIES

	PRIORITY	WHY IT MATTERS	FIRST STEP	START FROM	WITHIN
1	**Decide how to treat lost or stolen devices** R-05 A laptop or phone is lost or stolen · Above the appetite line with no treatment decision	This High risk sits above your appetite line with no decision, which leaves the treatment plan incomplete and caps the process score.	Meet the risk owner this week and choose modify, avoid, share or retain, with a target level.	Risk treatment plan	30 DAYS
2	**Resolve retained risk for leavers' access** R-06 Leavers keep access after they go · Retained above the line without a recorded acceptance	Keeping a High risk above your own line is only defensible with the owner's recorded acceptance; without it the risk reads as unmanaged.	Ask the owner to either approve a treatment or sign the acceptance with a name and date.	Risk acceptance form ISO 27001 Toolkit - 165 Comprehensive Templates	30 DAYS
3	**Rate the managed IT provider's remote access** R-13 A managed IT provider's remote access is abused · Not yet rated for likelihood and impact	An unrated risk has no level, so it is missing from the heat map and cannot be compared with the appetite line.	Rate likelihood and impact against your criteria, with a sentence of rationale.	Risk assessment and treatment methodology	30 DAYS
4	**Name an owner for the paper-policy risk** R-14 Security policies exist only on paper · Risk with no owner	ISO 27001 expects an accountable owner for every risk, even one you have decided to avoid.	Assign the risk to a role, such as the Information Security Manager.	Risk assessment and treatment methodology	60 DAYS
5	**Finish acceptance and rationale records** R-03 An unpatched vulnerability is exploited · R-09 Backups fail when they are needed · Residual risk not yet accepted by the owner	Residual risk for unpatched systems is not yet accepted, and the backup failure rating has no rationale; both are quick wins an auditor will check.	Collect the owner's acceptance for unpatched systems and add a rationale for backup failures.	Risk treatment plan	60 DAYS

30 / 60 / 90-DAY ROADMAP

FIRST 30 DAYS

- Record a treatment decision and target for lost or stolen devices.
- Obtain acceptance or a treatment plan for leavers' access.
- Rate the managed IT provider's remote access risk.

DAYS 31 TO 60

- Assign an owner to the paper-policy risk.
- Collect residual-risk acceptance for unpatched systems.
- Add a rationale to every High rating.

DAYS 61 TO 90

- Carry the selected Annex A controls into the Statement of Applicability.
- Present the updated register and treatment plan at management review.

What was in scope

The information, system or application, people, supplier, site and process the assessment covered, with their owners. How much confidentiality (C), integrity (I) and availability (A) matter for this item. H high, M medium, L low.

Type	Scope item	Owner	C	I	A	Risks
Information	**Customer personal data**	Data Protection Officer	H	M	M	4
Information	**Financial records**	Head of Finance	H	H	M	2
System or application	**Email and collaboration suite**	IT Manager	M	M	H	1
System or application	**ERP and order management system**	IT Manager	M	H	H	3
System or application	**Laptops and mobile devices**	IT Manager	M	L	M	1
System or application	**Warehouse management system**	Operations Manager	L	H	H	2
People	**All staff**	HR Manager	–	–	–	2
Supplier	**Cloud hosting provider**	IT Manager	H	M	H	2
Supplier	**Managed IT service provider**	IT Manager	H	H	H	1
Site	**Head office**	Facilities Manager	–	–	M	1
Process	**Payments and treasury**	Head of Finance	M	H	M	1

Risk register

Every risk, highest level first. Level = likelihood x impact, rated with the controls already in place. The rationale is the organization's own reason for the rating. The full scenario for each risk (threat, weakness and consequence) is in the workbook.

#	Ref	Risk scenario	Scope items	CIA	Owner	Existing controls	L	I	Level	Rationale
1	R-01	**Phishing leads to stolen credentials** Weakness: Staff not trained to spot phishing; passwords alone protect accounts	Email and collaboration suite, All staff, Customer personal data	C I	IT Manager	Spam filtering; annual awareness training	4	4	16 · High	Two staff clicked the last phishing test; one mailbox holds customer data and invoices.
2	R-03	**An unpatched vulnerability is exploited** Weakness: No patch management; no vulnerability scanning	Warehouse management system, ERP and order management system	C I A	IT Manager	Monthly patching of laptops; servers patched ad hoc	4	4	16 · High	Warehouse servers are six months behind on updates.
3	R-02	**Ransomware encrypts systems and data** Weakness: Unpatched systems, a flat network, backups the attacker can reach	ERP and order management system, Warehouse management system, Financial records	C I A	IT Manager	Anti-malware on laptops; nightly backups to the same network	3	5	15 · High	Backups are reachable from the office network; a hit would stop order processing.
4	R-04	**A supplier holding your data is breached** Weakness: Suppliers not assessed for security; no security terms in the contract	Cloud hosting provider, Customer personal data	C	Procurement Manager	Standard contracts	3	4	12 · High	Hosting provider holds all customer data; no security review done.
5	R-09	**Backups fail when they are needed** Weakness: Backups never test-restored, or kept where the same attack can reach them	Financial records, ERP and order management system	I A	IT Manager	Nightly backups	3	4	12 · High	
6	R-11	**Payment fraud through impersonation** Weakness: Bank detail changes are not verified by a call-back to a known number	Payments and treasury	I	Head of Finance	Two signatures above 10,000	3	4	12 · High	Two attempted invoice frauds last year.

7	R-05	**A laptop or phone is lost or stolen** Weakness: Devices not encrypted and cannot be wiped remotely	Laptops and mobile devices	C	IT Manager	Device encryption on laptops; phones not managed	4	3	12 · High	Sales staff carry customer lists on phones.
8	R-06	**Leavers keep access after they go** Weakness: No joiner, mover and leaver process tied to HR; shared accounts	All staff	CI	HR Manager	Leaver checklist	4	3	12 · High	Checklist exists but IT is often told late.
9	R-08	**A cloud provider outage stops key services** Weakness: No redundancy, fallback or tested recovery for cloud services	Cloud hosting provider	A	IT Manager	Provider SLA of 99.9%	2	4	8 · Medium	
10	R-10	**A personal data breach triggers regulator action** Weakness: Privacy obligations not mapped; no breach notification process	Customer personal data	C	Data Protection Officer	Privacy notice; breach log	2	4	8 · Medium	Regulator deadlines known.
11	R-07	**Confidential data sent to the wrong person** Weakness: No classification or labelling; no checks on outgoing email or sharing	Customer personal data	C	Data Protection Officer	Awareness training	3	2	6 · Medium	
12	R-12	**Fire, flood or water damage** Weakness: Equipment placed at risk; no detection or suppression	Head office	A	Facilities Manager	Smoke detection; server room above ground floor	1	5	5 · Medium	Low likelihood but the server room would be lost.
13	R-14	**Security policies exist only on paper** Weakness: Policies not approved, communicated or checked	**None linked**	CIA	**None**	Policies approved in 2024	2	2	4 · Low	
14	R-13	**A managed IT provider's remote access is abused** Weakness: Provider has standing admin access without MFA or monitoring	Managed IT service provider	CIA	IT Manager		–	–	Not rated	

What will be done, by whom and by when

Every risk with a treatment decision, earliest due date first. The Annex A controls listed are the ones the treatment relies on; they carry into the Statement of Applicability. Acceptance is the risk owner's approval of the plan and of the risk that remains.

Ref	Risk	Decision	Planned actions	Annex A controls	Owner and due date	Current to target	Accepted
R-11	**Payment fraud through impersonation** Head of Finance	**Modify**	Call-back check on any change of supplier bank details.	A.5.37 Documented operating procedures A.6.3 Information security awareness, education and training	Head of Finance 31 Oct 2026	12 · High → 4 · Low	Operations Director 24 Sep 2026
R-14	**Security policies exist only on paper**	**Avoid**	Retire the unused legacy remote access gateway.		IT Manager 15 Nov 2026	4 · Low → Removed	Not needed: risk removed
R-03	**An unpatched vulnerability is exploited** IT Manager	**Modify**	Put servers on the monthly cycle; add quarterly vulnerability scans.	A.8.8 Management of technical vulnerabilities	Managed IT service provider 30 Nov 2026	16 · High → 8 · Medium	**Not recorded**
R-01	**Phishing leads to stolen credentials** IT Manager	**Modify**	Turn on multi-factor authentication for all mail accounts; run quarterly phishing simulations.	A.8.5 Secure authentication A.6.3 Information security awareness, education and training	IT Manager 15 Dec 2026	16 · High → 8 · Medium	Operations Director 24 Sep 2026
R-09	**Backups fail when they are needed** IT Manager	**Modify**	Quarterly restore tests with a written record.	A.8.13 Information backup A.5.30 ICT readiness for business continuity	IT Manager 31 Dec 2026	12 · High → 4 · Low	Operations Director 24 Sep 2026
R-02	**Ransomware encrypts systems and data** IT Manager	**Modify**	Move backups to an isolated, immutable copy; segment the warehouse network; test a full restore.	A.8.13 Information backup A.8.22 Segregation of networks A.8.7 Protection against malware	IT Manager 31 Jan 2027	15 · High → 8 · Medium	Operations Director 24 Sep 2026

R-04	**A supplier holding your data is breached** Procurement Manager	**Share**	Add security and breach notification terms at renewal; review the provider's certification.	A.5.19 Information security in supplier relationships A.5.20 Addressing information security within supplier agreements	Procurement Manager 28 Feb 2027	12 · High → 8 · Medium	Head of Finance 24 Sep 2026
R-06	**Leavers keep access after they go** HR Manager	**Retain**	Risk retained at its current level.		–	12 · High → 12 · High **Still above the line**	**Not recorded**

ABOVE THE LINE WITH NO DECISION YET

Ref	Risk	Owner	Level
R-05	**A laptop or phone is lost or stolen**	IT Manager	12 · High

4 risks are within appetite (Medium and below) and need no treatment; 1 are not yet rated.

Where the assessment falls short

Each finding is a gap between the assessment as recorded and what ISO 27001 clauses 6.1.2 and 6.1.3 ask for, with the risks it applies to and the document that closes it.

Severity	Finding	Applies to	What it means	To fix	Document that closes it
CRITICAL	**Above the appetite line with no treatment decision**	R-05	These risks are rated above Medium, the highest level you accept without treatment, but nobody has decided what to do about them. ISO 27001 expects a treatment option to be chosen for every risk that fails the acceptance criteria.	Choose modify, avoid, share or retain for each one, with the risk owner.	Risk treatment plan
CRITICAL	**Retained above the line without a recorded acceptance**	R-06	Keeping a risk that sits above your own appetite line is a legitimate choice, but only when the risk owner has formally accepted it. Without a name and a date, an auditor will read it as a risk nobody has dealt with.	Record who accepted each risk and when, after they have seen its level.	Risk acceptance form
MAJOR	**Not yet rated for likelihood and impact**	R-13	Without both ratings a risk has no level, so it cannot be compared with the appetite line or placed in priority order.	Rate each one against the likelihood and impact scales in your criteria.	Risk assessment and treatment methodology
MAJOR	**Risk with no owner**	R-14	ISO 27001 requires a risk owner for every risk: the person with the accountability and authority to manage it.	Name an owner, by role, for each risk.	Risk assessment and treatment methodology
MINOR	**High or Critical rating with no rationale**	R-09	The reasoning behind a high rating is the first thing an auditor or a board member asks about.	Add a sentence on why the likelihood and impact were rated as they were.	Risk register
MINOR	**Residual risk not yet accepted by the owner**	R-03	ISO 27001 asks risk owners to approve the treatment plan and accept the risk that remains. A name and a date is enough to show it happened.	Record the owner's acceptance once they have approved the plan.	Risk treatment plan

PROCESS SCORE IN DETAIL

Criteria defined Every likelihood and impact level has a definition, and the appetite line is set.		100%	11 of 11	weight 10
Scope covered Every scope item has at least one risk linked to it.		100%	11 of 11	weight 10
Risk owners named Every risk has an owner accountable for it.		93%	13 of 14	weight 15
Risks rated Every risk has a likelihood and an impact, so it has a level.		93%	13 of 14	weight 15
Ratings explained Existing controls and a rationale are recorded for each risk.		79%	22 of 28	weight 10
Treatment decided Every risk above the appetite line has a treatment option chosen.		88%	7 of 8	weight 15
Targets within appetite Treatments bring each risk to a target at or below the line.		100%	6 of 6	weight 10
Treatments scheduled Each treatment has an owner and a due date.		100%	6 of 6	weight 5
Residual risk accepted Risk owners have accepted what remains after treatment, by name and date.		71%	5 of 7	weight 10

Findings by severity

1 · Initial (0+)

A start on a register, not yet an assessment that decisions can rest on.

2 · Developing (40+)

The risks are identified, but gaps in rating or treatment would not survive an audit.

3 · Defined (60+)

A complete, repeatable assessment with a treatment plan behind it.

4 · Managed (80+)

Owned, justified and accepted: ready for management review and audit.

A · APPENDIX

Criteria used and basis of this report

Clause 6.1.2 asks for risk criteria, including acceptance criteria, that give consistent, valid and comparable results. This is the record of the criteria every rating in this report was made against.

LIKELIHOOD SCALE

Value	Label	Definition
1	**Rare**	Not expected in the next 5 years; no known case here or in the sector
2	**Unlikely**	Could happen once in 2 to 5 years; has happened in the sector
3	**Possible**	Could happen about once a year
4	**Likely**	Expected several times a year
5	**Almost certain**	Expected monthly or more often, or already happening

IMPACT SCALE

Value	Label	Definition
1	**Negligible**	Under 10,000; nobody outside notices; fixed within a day
2	**Minor**	10,000 to 50,000; a few customers affected; internal escalation
3	**Moderate**	50,000 to 250,000; service disrupted for days; possible regulator query
4	**Major**	250,000 to 1 million; significant breach or outage; regulator notified; media interest
5	**Severe**	Over 1 million; sanctions or licence at risk; major customers lost

RISK LEVELS AND ACCEPTANCE

Band	Levels	Treatment
Low	1–4	Accepted without treatment
Medium	5–9	Accepted without treatment
High	10–16	Needs a treatment decision
Critical	17–25	Needs a treatment decision

Level = likelihood x impact. A risk above the appetite line may still be retained, but only with the risk owner's recorded acceptance.

Process score. Nine dimensions, each the share of risks (or of risks above the line) that meet it, multiplied by its weight; the weights add up to 100. A dimension with nothing in scope counts in full. Any critical finding holds the level at Developing, whatever the score.

Your workbook. The Excel workbook that comes with this report is the register as a working file. Change a likelihood or impact on the Risk register sheet and every level, the heat maps on the Dashboard and the process score recalculate. It also holds the treatment plan and a Statement of Applicability starter listing the Annex A controls your treatments rely on.

BASIS OF THIS REPORT AND LIMITATION OF LIABILITY

This report is the output of a self-assessment. The risks, ratings, risk levels, treatment decisions, findings, 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.

Information security risk assessment for Harbour Logistics (sample), generated 25 September 2026 by Governance Docs. This is a structured self-assessment based on the organization's own criteria and ratings. It is not a certification, an audit opinion or a substitute for an independent risk assessment.