

## 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, 116 applicable                      |
| PROFILE     | Transport and logistics · 50 to 249 people            |
| PREPARED BY | Governance Docs                                       |

## CONTENTS

- 1 Executive summary
- 2 Readiness by area and where the next points come from
- 3 Remediation plan
- A About this report

Confidential. Prepared for Harbour Logistics (sample) from its own self-assessment; not independently verified by Governance Docs (see section A). Share on a need-to-know basis.

# Where Harbour Logistics (sample) stands against ISO 27001



|            |           |           |               |
|------------|-----------|-----------|---------------|
| APPLICABLE | EVIDENCED | OPEN GAPS | HIGH PRIORITY |
| <b>116</b> | <b>21</b> | <b>95</b> | <b>51</b>     |

## 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 |
| <b>50</b> of 95    | <b>23</b> of 95    | <b>0</b>     |

## WHAT THIS ASSESSMENT TELLS YOU

- Overall readiness is 48.5% against ISO 27001 across 116 applicable controls. 21 of them are implemented and evidenced.
- Most open gaps: A.5 - Organizational controls, with 31 at 44%. Strongest area: A.7 - Physical controls at 75%.
- 5 management-system clauses score under half: Clause 4 - Context (31%); Clause 5 - Leadership (42%); Clause 6 - Planning (45%); Clause 8 - Operation (33%); Clause 9 - Performance evaluation (0%). Clauses cannot be excluded, and each is a likely major nonconformity at a certification audit.
- 25 controls are operating but not evidenced. Collecting their records alone lifts the score to 53.9% (+5.4 points), the cheapest gain available.
- 51 gaps are high priority (not started or only planned); 18 of them are in A.8 - Technological controls.

## DO THESE FIRST

|   | PRIORITY | ACTION                                                                                                                                                                                                        | OWNER              | START FROM                         |
|---|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------------------------------|
| 1 | HIGH     | Bring every management-system clause above 50%, starting with 4.3 Determining the scope of the ISMS; 5.3 Roles, responsibilities and authorities; 6.1.1 Actions to address risks and opportunities and 2 more | Operations Manager | ISMS Context and Scope             |
| 2 | HIGH     | Put an owner and date against the 18 high-priority gaps in A.8 - Technological controls                                                                                                                       | Compliance Lead    | Configuration Management Procedure |
| 3 | MEDIUM   | Adopt and tailor the Incident Response Procedure, which closes 5 open gaps                                                                                                                                    | To assign          | Incident Response Procedure        |

# Analysis and priorities

## IN ONE SENTENCE

**At 48.5% readiness, the organization must establish management review, internal audit, and formal risk governance to address material gaps.**

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 self-assessment shows an overall score of 48.5% at the Developing level, with 95 open gaps and 51 high priority gaps. Our primary operational exposure stems from having 0% in performance evaluation, meaning we lack internal audit and management review mechanisms to verify security controls. Furthermore, only 23 gaps currently have target dates. Management must authorize the implementation roadmap, assign explicit ownership for all open gaps, and commit resources to formalize risk treatment and operational oversight.

## WHERE YOU STAND

The self-assessment places you at a readiness level of 2 of 4, categorized as Developing, with an overall score of 48.5%. Out of 116 applicable requirements, there are 95 open gaps, including 51 high priority gaps. Only 50 gaps have an assigned owner and 23 have target dates. Foundational management system clauses show significant deficits, including Clause 9 - Performance evaluation at 0%, Clause 4 - Context at 31.3%, and Clause 8 - Operation at 33.3%, indicating that core security governance processes are not yet established.

## WHAT IT MEANS FOR THE ORGANIZATION

While 21 requirements are implemented and evidenced, 25 are implemented without evidence and 28 are merely planned. Because Performance evaluation stands at 0%, the leadership team lacks formal mechanisms to verify controls, conduct internal audits, or perform management reviews. Without documented evidence and operational risk treatment, controls cannot be verified by external parties. The gap between planned controls and verified operations leaves critical transport and logistics systems exposed to operational disruption and unaddressed risks across organizational and technical control areas.

## WHERE TO FOCUS FIRST

Initial effort must target core management processes and operational risk treatment. Evidencing what already runs raises the score to 53.9%, while finishing partially implemented items reaches 62.1%. You should immediately define scope and security roles, activate internal audit and management reviews, and formalize incident response procedures. Establishing an incident response procedure and security policies addresses multiple high priority gaps simultaneously. Defining these basic operational governance controls provides the structure required before tackling technological and organizational control gaps.

## PRIORITIES

|   | PRIORITY                                                                                                                                                                      | WHY IT MATTERS                                                                                                                                                                                                                             | FIRST STEP                                                                           | START FROM                                                                                              | WITHIN  |
|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|---------|
| 1 | <b>Establish Performance Evaluation and Internal Audit</b><br>9.2 Internal audit · 9.3 Management review                                                                      | Clause 9 - Performance evaluation stands at 0%, leaving leadership without verification of security controls. External auditors will identify the absence of internal audits and management reviews as material failures.                  | Draft the internal audit procedure and schedule the first management review meeting. | <b>ISMS Internal Audit Procedure</b><br><a href="#">ISO 27001 Toolkit - 165 Comprehensive Templates</a> | 30 DAYS |
| 2 | <b>Define ISMS Scope and Security Governance Roles</b><br>4.3 Determining the scope of the ISMS · 5.3 Roles, responsibilities and authorities                                 | Without a clear scope and defined roles, accountability across the organization remains unassigned. This confusion prevents the effective rollout of both operational and technical security controls.                                     | Draft the ISMS Context and Scope document to delineate operational boundaries.       | <b>ISMS Context and Scope</b><br><a href="#">ISO 27001 Toolkit - 165 Comprehensive Templates</a>        | 30 DAYS |
| 3 | <b>Implement Operational Information Security Risk Treatment</b><br>8.3 Information security risk treatment (operational) · 6.1.3 Information security risk treatment         | Risk treatment remains not started at the operational level, exposing logistics processes to unmitigated vulnerabilities. Implementing risk treatment is essential to protect critical operations and meet baseline planning requirements. | Populate the risk treatment plan with actions for identified high priority risks.    | <b>ISMS Risk Treatment Plan</b><br><a href="#">ISO 27001 Toolkit - 165 Comprehensive Templates</a>      | 60 DAYS |
| 4 | <b>Operationalize Incident Response and Evidence Handling</b><br>A.5.24 Incident management planning and preparation · A.5.28 Collection of evidence                          | Unprepared incident response increases recovery time and magnifies operational disruption during security events. Standard procedures are required to identify incidents and preserve evidence.                                            | Review and approve the baseline incident response procedure for operational teams.   | <b>Incident Response Procedure</b><br><a href="#">ISO 27001 Toolkit - 165 Comprehensive Templates</a>   | 60 DAYS |
| 5 | <b>Secure Supply Chain and Supplier Relationships</b><br>A.5.19 Information security in supplier relationships · A.5.21 Managing information security in the ICT supply chain | Supply chain risks in transport and logistics can compromise key operational infrastructure if vendors are unmanaged. Establishing supplier controls prevents third-party vulnerabilities from impacting organizational operations.        | Draft the vendor management policy to evaluate third-party ICT suppliers.            | <b>Vendor Management Policy</b><br><a href="#">ISO 27001 Toolkit - 165 Comprehensive Templates</a>      | 90 DAYS |

**30 / 60 / 90-DAY ROADMAP****FIRST 30 DAYS**

- Document the ISMS scope and approve security leadership roles and responsibilities across the organization.
- Establish the internal audit procedure and set a formal schedule for management review meetings.
- Gather documented evidence for the 25 requirements currently implemented without documentation.

**DAYS 31 TO 60**

- Execute the risk assessment and approve the operational risk treatment plan.
- Finalize and distribute the incident response procedure and evidence collection guidelines.
- Assign formal owners and realistic target dates to all 51 high priority gaps.

**DAYS 61 TO 90**

- Enforce supplier security requirements using the updated vendor management policy.
- Conduct the first internal audit cycle across core management system processes.
- Convene the management review meeting to evaluate performance metrics and corrective actions.

## 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                | <div><div>2</div><div>1</div><div>1</div></div> | 31%   | <div><div>2</div><div>1</div><div>1</div></div> |
| Clause 5 - Leadership             | <div><div>1</div><div>1</div><div>1</div></div> | 42%   | <div><div>1</div><div>1</div><div>1</div></div> |
| Clause 6 - Planning               | <div><div>3</div><div>1</div><div>1</div></div> | 45%   | <div><div>3</div><div>1</div><div>0</div></div> |
| Clause 7 - Support                | <div><div>4</div><div>1</div><div>2</div></div> | 50%   | <div><div>4</div><div>1</div><div>0</div></div> |
| Clause 8 - Operation              | <div><div>1</div><div>1</div><div>1</div></div> | 33%   | <div><div>2</div><div>0</div><div>1</div></div> |
| Clause 9 - Performance evaluation | <div><div>3</div></div>                         | 0%    | <div><div>3</div><div>0</div><div>0</div></div> |
| Clause 10 - Improvement           | <div><div>1</div><div>1</div></div>             | 50%   | <div><div>1</div><div>0</div><div>1</div></div> |

  

| ANNEX A CONTROLS              | STATUS MIX                                                                           | SCORE | GAPS H · M · L                                   |
|-------------------------------|--------------------------------------------------------------------------------------|-------|--------------------------------------------------|
| A.5 - Organizational controls | <div><div>11</div><div>3</div><div>8</div><div>9</div><div>4</div><div>2</div></div> | 44%   | <div><div>14</div><div>8</div><div>9</div></div> |
| A.6 - People controls         | <div><div>1</div><div>3</div><div>3</div><div>1</div></div>                          | 59%   | <div><div>1</div><div>3</div><div>3</div></div>  |
| A.7 - Physical controls       | <div><div>2</div><div>4</div><div>5</div><div>2</div></div>                          | 75%   | <div><div>2</div><div>1</div><div>4</div></div>  |
| A.8 - Technological controls  | <div><div>4</div><div>14</div><div>3</div><div>5</div><div>8</div></div>             | 49%   | <div><div>18</div><div>3</div><div>5</div></div> |

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                                             | <div><div></div><div></div></div> | 48.5%           |
| Evidence what already runs<br>25 requirements     | <div><div></div><div></div></div> | 53.9%<br>+5.4   |
| Finish what is partly in place<br>19 requirements | <div><div></div><div></div></div> | 62.1%<br>+8.2   |
| Implement what is planned<br>28 requirements      | <div><div></div><div></div></div> | 80.2%<br>+18.1  |
| Start what has not begun<br>23 requirements       | <div><div></div><div></div></div> | 100.0%<br>+19.8 |

### DOCUMENTS THAT CLOSE THE MOST GAPS

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

|                             |                        |   |
|-----------------------------|------------------------|---|
| Incident Response Procedure | <div><div></div></div> | 5 |
| Security Incident Procedure | <div><div></div></div> | 5 |
| Standard NDA                | <div><div></div></div> | 5 |
| Access Control Policy       | <div><div></div></div> | 5 |
| Physical Security Policy    | <div><div></div></div> | 5 |
| ISMS Risk Treatment Plan    | <div><div></div></div> | 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 · 23

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

| Ref    | Requirement                                           | Area     | Owner · target                    | Closes it                                                                                      |
|--------|-------------------------------------------------------|----------|-----------------------------------|------------------------------------------------------------------------------------------------|
| 4.3    | Determining the scope of the ISMS                     | Clause 4 | Operations Manager<br>26 Nov 2026 | ISMS Context and Scope · Organization of Information Security                                  |
| 4.4    | Information security management system                | Clause 4 | Operations Manager<br>12 Nov 2026 | ISMS Management Plan · ISMS Operating Procedure +1 more                                        |
| 5.3    | Roles, responsibilities and authorities               | Clause 5 | IT Manager                        | ISMS Roles and Responsibilities · Chief Information Security Officer JD +2 more                |
| 8.3    | Information security risk treatment (operational)     | Clause 8 | To assign                         | ISMS Risk Treatment Plan · ISMS Risk Treatment Plan                                            |
| 9.1    | Monitoring, measurement, analysis and evaluation      | Clause 9 | Operations Manager<br>10 Dec 2026 | ISMS Monitoring and Evaluation · Information Security Program Maturity Assessment Tool +1 more |
| 9.2    | Internal audit                                        | Clause 9 | IT Manager                        | ISMS Internal Audit Procedure · ISMS Audit Plan +3 more                                        |
| 9.3    | Management review                                     | Clause 9 | IT Manager                        | ISMS Management Review Meeting Agenda · ISMS MRM Agenda                                        |
| A.5.1  | Policies for information security                     | A.5      | HR Manager                        | Information Security Policy · ISMS Policy +1 more                                              |
| A.5.2  | Information security roles and responsibilities       | A.5      | To assign                         | ISMS Roles and Responsibilities · Organization of Information Security                         |
| A.5.11 | Return of assets                                      | A.5      | To assign                         | Employee Movement and Termination Checklist · Asset Handling Policy                            |
| A.5.13 | Labelling of information                              | A.5      | Compliance Lead<br>10 Dec 2026    | Information Security Labelling Procedure                                                       |
| A.5.17 | Authentication information                            | A.5      | Operations Manager<br>10 Dec 2026 | Password Reset Procedure · Access Control Policy +1 more                                       |
| A.5.19 | Information security in supplier relationships        | A.5      | To assign                         | Vendor Management Policy · Model Policy on Outsourcing                                         |
| A.5.21 | Managing information security in the ICT supply chain | A.5      | Operations Manager                | Vendor Management Policy · Vendor Evaluation Process                                           |

|               |                                                            |     |                                   |                                                                                  |
|---------------|------------------------------------------------------------|-----|-----------------------------------|----------------------------------------------------------------------------------|
| <b>A.5.24</b> | Incident management planning and preparation               | A.5 | Risk Manager<br>24 Dec 2026       | Incident Response Procedure · Security Incident Procedure +1 more                |
| <b>A.5.28</b> | Collection of evidence                                     | A.5 | Risk Manager<br>24 Dec 2026       | Incident Response Procedure · Security Incident Procedure                        |
| <b>A.5.30</b> | ICT readiness for business continuity                      | A.5 | Operations Manager<br>21 Jan 2027 | ISMS Business Impact Analysis (BIA) Procedure · Business Continuity Plan +2 more |
| <b>A.5.34</b> | Privacy and protection of PII                              | A.5 | To assign                         | Privacy Officer JD · Data Retention Policy +1 more                               |
| <b>A.6.5</b>  | Responsibilities after termination or change of employment | A.6 | Operations Manager                | Employee Movement and Termination Checklist · Standard NDA +1 more               |
| <b>A.8.9</b>  | Configuration management                                   | A.8 | Risk Manager<br>26 Nov 2026       | Configuration Management Procedure                                               |
| <b>A.8.15</b> | Logging                                                    | A.8 | Compliance Lead<br>10 Dec 2026    | Log Monitoring Policy · IT Systems Monitoring Procedure                          |
| <b>A.8.21</b> | Security of network services                               | A.8 | Risk Manager<br>26 Nov 2026       | Network Security Policy · Standard SLA                                           |
| <b>A.8.29</b> | Security testing in development and acceptance             | A.8 | Compliance Lead<br>7 Jan 2027     | Secure Development Policy · Vulnerability Assessment Procedure                   |

**HIGH Planned · 28**

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

| Ref          | Requirement                                  | Area     | Owner · target                   | Closes it                                                                                      |
|--------------|----------------------------------------------|----------|----------------------------------|------------------------------------------------------------------------------------------------|
| <b>6.1.1</b> | Actions to address risks and opportunities   | Clause 6 | Risk Manager                     | ISMS Management Plan · ISMS Risk Assessment and Treatment                                      |
| <b>6.1.2</b> | Information security risk assessment         | Clause 6 | Operations Manager<br>4 Feb 2027 | ISMS Risk Assessment and Treatment · ISMS Information Risk Register +2 more                    |
| <b>6.1.3</b> | Information security risk treatment          | Clause 6 | To assign                        | ISO 27001:2022 Statement of Applicability · ISMS Risk Treatment Plan +1 more                   |
| <b>7.1</b>   | Resources                                    | Clause 7 | To assign                        | ISMS Management Plan · ISMS Implementation Project Estimator                                   |
| <b>7.4</b>   | Communication                                | Clause 7 | Risk Manager<br>29 Oct 2026      | ISMS Communication Plan                                                                        |
| <b>7.5.1</b> | Documented information - general             | Clause 7 | Risk Manager                     | ISMS Documented Information and Procedures Register · Documented Information Control Procedure |
| <b>7.5.2</b> | Creating and updating documented information | Clause 7 | To assign                        | Documented Information Control Procedure · Control of Records Procedure                        |

|               |                                                               |           |                                   |                                                                               |
|---------------|---------------------------------------------------------------|-----------|-----------------------------------|-------------------------------------------------------------------------------|
| <b>8.2</b>    | Information security risk assessment (operational)            | Clause 8  | Operations Manager                | ISMS Risk Assessment and Treatment · ISMS Information Risk Register           |
| <b>10.2</b>   | Nonconformity and corrective action                           | Clause 10 | Risk Manager<br>26 Nov 2026       | ISMS Nonconformity Management Procedure · Corrective Action Procedure +1 more |
| <b>A.5.7</b>  | Threat intelligence                                           | A.5       | Operations Manager<br>7 Jan 2027  | Threat Intelligence Policy                                                    |
| <b>A.5.22</b> | Monitoring, review and change management of supplier services | A.5       | To assign                         | Vendor Management Policy · Vendor Access Procedure                            |
| <b>A.5.36</b> | Compliance with policies, rules and standards                 | A.5       | To assign                         | Compliance Manager JD · ISMS Monitoring and Evaluation                        |
| <b>A.7.2</b>  | Physical entry                                                | A.7       | Operations Manager                | Physical Security Policy · Secure Areas Policy                                |
| <b>A.7.4</b>  | Physical security monitoring                                  | A.7       | Operations Manager<br>10 Dec 2026 | Physical Security Policy · Physical Security Manager JD                       |
| <b>A.8.1</b>  | User end point devices                                        | A.8       | To assign                         | Mobile Computing Policy · BYOD Policy +1 more                                 |
| <b>A.8.3</b>  | Information access restriction                                | A.8       | Risk Manager                      | Access Control Policy                                                         |
| <b>A.8.4</b>  | Access to source code                                         | A.8       | Operations Manager                | Secure Development Policy · Development Environment Policy                    |
| <b>A.8.7</b>  | Protection against malware                                    | A.8       | Compliance Lead<br>10 Dec 2026    | Anti-Malware Policy · Model Policy on Malware +1 more                         |
| <b>A.8.11</b> | Data masking                                                  | A.8       | IT Manager                        | Data Masking Policy                                                           |
| <b>A.8.12</b> | Data leakage prevention                                       | A.8       | Operations Manager                | Data Loss Prevention (DLP) Policy                                             |
| <b>A.8.14</b> | Redundancy of information processing facilities               | A.8       | To assign                         | Business Continuity Plan · ISMS Business Impact Analysis (BIA) Procedure      |
| <b>A.8.16</b> | Monitoring activities                                         | A.8       | HR Manager                        | IT Systems Monitoring Procedure · Log Monitoring Policy                       |
| <b>A.8.19</b> | Installation of software on operational systems               | A.8       | IT Manager                        | Software Policy · Release Management Policy                                   |
| <b>A.8.22</b> | Segregation of networks                                       | A.8       | Operations Manager                | Network Security Policy                                                       |
| <b>A.8.23</b> | Web filtering                                                 | A.8       | To assign                         | Internet Acceptable Use Policy · Internet Risk and Security Manager JD        |
| <b>A.8.24</b> | Use of cryptography                                           | A.8       | Compliance Lead<br>21 Jan 2027    | Cryptographic Policy                                                          |
| <b>A.8.28</b> | Secure coding                                                 | A.8       | Risk Manager                      | Secure Coding Policy                                                          |
| <b>A.8.33</b> | Test information                                              | A.8       | Compliance Lead                   | Data Masking Policy · Development Environment Policy                          |

**MEDIUM Partially implemented · 19**

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

| Ref           | Requirement                                                | Area     | Owner · target              | Closes it                                                                        |
|---------------|------------------------------------------------------------|----------|-----------------------------|----------------------------------------------------------------------------------|
| <b>4.1</b>    | Understanding the organization and its context             | Clause 4 | To assign                   | ISMS Context and Scope                                                           |
| <b>5.1</b>    | Leadership and commitment                                  | Clause 5 | Risk Manager                | Management Support Letter · ISMS Management Review Meeting Agenda +1 more        |
| <b>6.3</b>    | Planning of changes                                        | Clause 6 | HR Manager                  | Change Management Policy · Model Policy on Change Management and Control         |
| <b>7.2</b>    | Competence                                                 | Clause 7 | Operations Manager          | Recruitment and New Joiner Checklist · Employee Screening Checklist              |
| <b>A.5.3</b>  | Segregation of duties                                      | A.5      | Risk Manager<br>29 Oct 2026 | Segregation of Duties Policy                                                     |
| <b>A.5.5</b>  | Contact with authorities                                   | A.5      | IT Manager<br>10 Dec 2026   | Incident Response Procedure · Security Incident Procedure                        |
| <b>A.5.10</b> | Acceptable use of information and other associated assets  | A.5      | Compliance Lead             | Acceptable Use Policy · Internet Acceptable Use Policy +1 more                   |
| <b>A.5.14</b> | Information transfer                                       | A.5      | To assign                   | Information Transfer Procedure · Physical Media Transfer Procedure +1 more       |
| <b>A.5.20</b> | Addressing information security within supplier agreements | A.5      | HR Manager<br>21 Jan 2027   | Vendor Security Agreement · Standard SLA +1 more                                 |
| <b>A.5.31</b> | Legal, statutory, regulatory and contractual requirements  | A.5      | HR Manager                  | Legal and Regulatory Requirements Policy · Legal Responsibilities Policy         |
| <b>A.5.35</b> | Independent review of information security                 | A.5      | Operations Manager          | ISMS Internal Audit Procedure · ISMS Auditing Guideline +1 more                  |
| <b>A.5.37</b> | Documented operating procedures                            | A.5      | To assign                   | ISMS Operating Procedure · Documented Information Control Procedure              |
| <b>A.6.2</b>  | Terms and conditions of employment                         | A.6      | To assign                   | Employment Contract Clauses · Standard NDA                                       |
| <b>A.6.3</b>  | Information security awareness, education and training     | A.6      | IT Manager<br>21 Jan 2027   | Awareness Presentation · Model Policy on Security Awareness and Training +1 more |
| <b>A.6.4</b>  | Disciplinary process                                       | A.6      | Risk Manager                | Employee Disciplinary Process                                                    |
| <b>A.7.7</b>  | Clear desk and clear screen                                | A.7      | To assign                   | Physical Security Policy · Acceptable Use Policy                                 |
| <b>A.8.10</b> | Information deletion                                       | A.8      | To assign                   | Secure Data Disposal Policy · Data Retention Policy                              |
| <b>A.8.20</b> | Networks security                                          | A.8      | IT Manager                  | Network Security Policy · Network Risk Manager JD                                |

|               |                        |     |           |                                                                 |
|---------------|------------------------|-----|-----------|-----------------------------------------------------------------|
| <b>A.8.30</b> | Outsourced development | A.8 | To assign | Model Policy on Outsourcing · Vendor Security Agreement +1 more |
|---------------|------------------------|-----|-----------|-----------------------------------------------------------------|

**LOW Implemented, not evidenced · 25**

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                                                                              |
|---------------|--------------------------------------------------------|-----------|----------------|----------------------------------------------------------------------------------------|
| <b>4.2</b>    | Needs and expectations of interested parties           | Clause 4  | To assign      | ISMS Context and Scope · Legal and Regulatory Requirements Policy                      |
| <b>5.2</b>    | Information security policy                            | Clause 5  | To assign      | Information Security Policy · ISMS Policy +1 more                                      |
| <b>8.1</b>    | Operational planning and control                       | Clause 8  | To assign      | ISMS Operating Procedure · Model Policy on Outsourcing                                 |
| <b>10.1</b>   | Continual improvement                                  | Clause 10 | To assign      | Continuous Improvement Procedure · ISMS Continuous Improvement Log                     |
| <b>A.5.8</b>  | Information security in project management             | A.5       | To assign      | Project Management Security Policy · ISMS Project Initiation Document +1 more          |
| <b>A.5.9</b>  | Inventory of information and other associated assets   | A.5       | To assign      | ISMS Information Asset Inventory · Asset Inventory +2 more                             |
| <b>A.5.15</b> | Access control                                         | A.5       | To assign      | Access Control Policy                                                                  |
| <b>A.5.16</b> | Identity management                                    | A.5       | To assign      | Access Control Policy · Permissions Manager JD                                         |
| <b>A.5.23</b> | Information security for use of cloud services         | A.5       | To assign      | Cloud Services Security Policy                                                         |
| <b>A.5.25</b> | Assessment and decision on information security events | A.5       | To assign      | Security Incident Procedure · Incident Response Procedure                              |
| <b>A.5.26</b> | Response to information security incidents             | A.5       | To assign      | Incident Response Procedure · Security Incident Procedure                              |
| <b>A.5.29</b> | Information security during disruption                 | A.5       | To assign      | Business Continuity Plan · Roles and Responsibilities for Contingency Planning +1 more |
| <b>A.5.33</b> | Protection of records                                  | A.5       | To assign      | Control of Records Procedure · Data Retention Policy                                   |
| <b>A.6.1</b>  | Screening                                              | A.6       | To assign      | Employee Screening Checklist · Recruitment and New Joiner Checklist                    |
| <b>A.6.6</b>  | Confidentiality or non-disclosure agreements           | A.6       | To assign      | Standard NDA · Vendor Security Agreement                                               |
| <b>A.6.7</b>  | Remote working                                         | A.6       | To assign      | Remote Working Policy · Mobile Computing Policy +1 more                                |
| <b>A.7.3</b>  | Securing offices, rooms and facilities                 | A.7       | To assign      | Secure Areas Policy · Physical Security Design Policy                                  |

|               |                                                             |     |           |                                                                         |
|---------------|-------------------------------------------------------------|-----|-----------|-------------------------------------------------------------------------|
| <b>A.7.8</b>  | Equipment siting and protection                             | A.7 | To assign | Physical Security Policy                                                |
| <b>A.7.10</b> | Storage media                                               | A.7 | To assign | Removable Media Management Procedure · Media Disposal Procedure +1 more |
| <b>A.7.12</b> | Cabling security                                            | A.7 | To assign | Physical Security Policy · Network Security Policy                      |
| <b>A.8.13</b> | Information backup                                          | A.8 | To assign | Backup Policy · Data Restoration Form                                   |
| <b>A.8.18</b> | Use of privileged utility programs                          | A.8 | To assign | Access Control Policy · Software Policy                                 |
| <b>A.8.25</b> | Secure development life cycle                               | A.8 | To assign | Secure Development Policy · Secure Systems Engineering Policy           |
| <b>A.8.27</b> | Secure system architecture and engineering principles       | A.8 | To assign | Secure Systems Engineering Policy                                       |
| <b>A.8.31</b> | Separation of development, test and production environments | A.8 | To assign | Development Environment Policy · Data Masking Policy                    |

# 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](https://governancedocs.com)