

---

## SELF-ASSESSMENT WORKSHEET

# ISO/IEC 27001 — Information Security

Work through each clause, record what you do today, rate where you are and agree the actions that close the gap.

ORGANISATION

COMPLETED BY

DATE

How to rate: 0 = nothing in place 1 = partly in place 2 = in place, little evidence 3 = in place and evidenced  
Fill in on screen or print. Always work from the current published standard.

## How to complete this worksheet

- 1 Get the right people together**  
Ask the person who runs each area to help. Allow 1–2 hours per sitting; you don't have to finish in one go.
- 2 Read each clause and the evidence prompt**  
The grey box tells you what an auditor will look for. The examples underneath show the kind of records that count.
- 3 Write what you actually do today**  
Describe the real practice, not what you'd like to happen. Name the document, system or record and where it's kept, e.g. 'Training matrix — SharePoint/HR, updated monthly'.
- 4 Rate honestly from 0 to 3**  
0 nothing in place · 1 partly in place or informal · 2 in place but little written proof · 3 in place, followed and evidenced with records. If you can't show it, it isn't a 3.
- 5 Agree actions, owners and due dates**  
For anything rated 0–2, write the next practical step, who will do it and by when. Small, specific actions get done.
- 6 Summarise and review**  
List your top three priorities on the final page. Revisit the worksheet every few months to track progress.

### What counts as good evidence?

- Good evidence is current, approved, dated and actually used — a policy nobody follows isn't evidence.
- Records beat documents: a completed checklist proves more than the procedure that describes it.
- Photos, screenshots, emails and system exports all count if they show the activity happening.
- Leave a box blank rather than guess — blanks show you where to look first.

CLAUSES 1-3

Scope, references and definitions

These opening clauses explain what ISO/IEC 27001 covers, list any documents it relies on and define its key terms. They contain no requirements you are audited against.

Evidence to look for: Read the definitions once — words like 'shall', 'interested party' and 'documented information' have precise meanings in an audit.

Examples of suitable evidence

- ✓ Copy of the current ISO/IEC 27001 standard
- ✓ Copy of ISO/IEC 27000 vocabulary and overview
- ✓ Reference list identifying standards cited by ISO/IEC 27001
- ✓ Internal glossary explaining information security terms

What we do today / evidence we hold

Actions to close the gap

|       |  |     |  |        |              |              |              |              |
|-------|--|-----|--|--------|--------------|--------------|--------------|--------------|
| Owner |  | Due |  | Rating | <div>0</div> | <div>1</div> | <div>2</div> | <div>3</div> |
|-------|--|-----|--|--------|--------------|--------------|--------------|--------------|

CLAUSE 4

Context of the organisation

Define the scope of the information security management system (ISMS), the issues that affect information security, and the interested parties and their requirements, including legal and contractual ones.

Evidence to look for: A scope naming locations, systems and services covered, and any interfaces with third parties.

Examples of suitable evidence

- ✓ Approved ISMS scope document listing sites, systems and organisational boundaries
- ✓ Context register recording internal and external information security issues
- ✓ Interested parties register listing customers, regulators and their security requirements
- ✓ Legal and contractual requirements register covering UK GDPR and customer agreements

What we do today / evidence we hold

Actions to close the gap

|       |  |     |  |        |   |   |   |   |
|-------|--|-----|--|--------|---|---|---|---|
| Owner |  | Due |  | Rating | 0 | 1 | 2 | 3 |
|-------|--|-----|--|--------|---|---|---|---|

CLAUSE 5

Leadership

Top management must own the information security system: set the policy, assign roles and responsibilities, provide resources and make it part of normal business decisions. Responsibility can be delegated; accountability cannot.

Evidence to look for: Directors can explain the policy, review results at board level and remove obstacles. A signed policy alone is not enough.

Examples of suitable evidence

- ✓ Information security policy signed by the managing director
- ✓ Responsibility matrix naming security roles and accountable senior managers
- ✓ Board minutes recording security decisions and approved resources
- ✓ Business planning minutes showing management consideration of information security risks

What we do today / evidence we hold

Actions to close the gap

|       |  |     |  |        |                                    |                                    |                                    |                                    |
|-------|--|-----|--|--------|------------------------------------|------------------------------------|------------------------------------|------------------------------------|
| Owner |  | Due |  | Rating | <div><div></div><div>0</div></div> | <div><div></div><div>1</div></div> | <div><div></div><div>2</div></div> | <div><div></div><div>3</div></div> |
|-------|--|-----|--|--------|------------------------------------|------------------------------------|------------------------------------|------------------------------------|

**CLAUSE 6****Planning**

Run an information security risk assessment, choose how to treat each risk, produce a Statement of Applicability (SoA) showing which Annex A controls apply and why, and set security objectives.

Evidence to look for: A risk register, risk treatment plan and SoA that genuinely match your environment rather than a template.

**Examples of suitable evidence**

- ✓ Risk assessment register recording threats, likelihood, impact and risk owners
- ✓ Risk treatment plan listing actions, owners, deadlines and approval
- ✓ Statement of Applicability recording control applicability, justifications and implementation status
- ✓ Security objectives register with measurable targets, owners and review dates

**What we do today / evidence we hold****Actions to close the gap**

|              |                      |            |                      |               |                       |                       |                       |                       |
|--------------|----------------------|------------|----------------------|---------------|-----------------------|-----------------------|-----------------------|-----------------------|
| <b>Owner</b> | <input type="text"/> | <b>Due</b> | <input type="text"/> | <b>Rating</b> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
|              |                      |            |                      |               | 0                     | 1                     | 2                     | 3                     |

**CLAUSE 7****Support**

Provide the people, competence, awareness, communication, infrastructure and controlled documents and records the information security system needs.

Evidence to look for: Training is based on the work people actually do, current instructions are easy to find and old versions are withdrawn.

**Examples of suitable evidence**

- ✓ Security training records showing attendance and competence assessments
- ✓ Staff awareness briefing records covering policies and incident reporting
- ✓ Communication plan naming audiences, messages, responsible people and timings
- ✓ Controlled document register showing versions, approvals, owners and review dates

**What we do today / evidence we hold****Actions to close the gap**

|              |                      |            |                      |               |                       |                       |                       |                       |
|--------------|----------------------|------------|----------------------|---------------|-----------------------|-----------------------|-----------------------|-----------------------|
| <b>Owner</b> | <input type="text"/> | <b>Due</b> | <input type="text"/> | <b>Rating</b> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
|              |                      |            |                      |               | 0                     | 1                     | 2                     | 3                     |

**CLAUSE 8****Operation**

Carry out the risk treatment plan, repeat risk assessments at planned intervals or when things change, and control outsourced processes.

Evidence to look for: Evidence that controls such as access reviews, backups, patching and supplier security checks really happen.

**Examples of suitable evidence**

- ✓ Risk treatment action log with completion dates and supporting evidence
- ✓ Scheduled risk reassessment reports approved by risk owners
- ✓ Change records showing security risk assessments before new system deployments
- ✓ Supplier review records checking outsourced service security against agreed requirements

**What we do today / evidence we hold****Actions to close the gap****Owner**

**Due**

**Rating**
☐ 0

☐ 1

☐ 2

☐ 3
**CLAUSE 9****Performance evaluation**

Decide what to monitor and measure for information security, analyse the results, run a planned programme of impartial internal audits and hold management reviews at planned intervals.

Evidence to look for: Use a handful of meaningful indicators, audit real work rather than paperwork, and minute the decisions management review actually takes.

**Examples of suitable evidence**

- ✓ Security performance dashboard tracking agreed measures against targets
- ✓ Internal audit programme showing scope, frequency and independent auditor assignments
- ✓ Completed internal audit reports recording findings and supporting evidence
- ✓ Management review minutes recording performance discussions, decisions and assigned actions

**What we do today / evidence we hold****Actions to close the gap****Owner**

**Due**

**Rating**
☐ 0

☐ 1

☐ 2

☐ 3

## CLAUSE 10

### Improvement

When something goes wrong, deal with the immediate effect, find the root cause, take action so it does not recur and check the action worked. Keep improving the system over time.

Evidence to look for: A nonconformity is only closed when you have evidence the cause was fixed — not when the form is completed.

#### Examples of suitable evidence

- ✓ Incident record documenting immediate containment and correction
- ✓ Root cause analysis report following an information security nonconformity
- ✓ Corrective action register recording owners, deadlines and effectiveness checks
- ✓ Continual improvement log recording implemented changes and measured benefits

#### What we do today / evidence we hold

#### Actions to close the gap

|              |                      |            |                      |               |                       |                       |                       |                       |
|--------------|----------------------|------------|----------------------|---------------|-----------------------|-----------------------|-----------------------|-----------------------|
| <b>Owner</b> | <input type="text"/> | <b>Due</b> | <input type="text"/> | <b>Rating</b> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
|              |                      |            |                      |               | 0                     | 1                     | 2                     | 3                     |

## ANNEX A

### 93 reference controls

Annex A lists 93 controls grouped as organisational (37), people (8), physical (14) and technological (34). You choose which apply based on your risk assessment.

Evidence to look for: Excluding a control is fine if you justify it in the SoA. Including one means you must show it operating.

#### Examples of suitable evidence

- ✓ Supplier security review records and signed confidentiality agreements
- ✓ Staff screening records and completed leaver access removal checklists
- ✓ Server room access logs and photographs of locked equipment cabinets
- ✓ System patching reports and successful backup restoration test records

#### What we do today / evidence we hold

#### Actions to close the gap

|              |                      |            |                      |               |                       |                       |                       |                       |
|--------------|----------------------|------------|----------------------|---------------|-----------------------|-----------------------|-----------------------|-----------------------|
| <b>Owner</b> | <input type="text"/> | <b>Due</b> | <input type="text"/> | <b>Rating</b> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
|              |                      |            |                      |               | 0                     | 1                     | 2                     | 3                     |

## Summary and next steps

### Top three priorities

### Resources or support needed

### Target date for certification or review

### Want a second pair of eyes?

Send your completed worksheet to our success team for a free review call.

**[success@isology.co.uk](mailto:success@isology.co.uk) · [www.isology.co.uk/contact](http://www.isology.co.uk/contact)**