Armoryze
Be More Secure

ISO 27001 (INFORMATION SECURITY) CHECKLIST

1 CLAUSE 4: Know your organisation

- **List the internal and external issues that drive the need for information security** □
- **List your stakeholders and their information security requirements** □
- **List relevant information security laws and regulations.** □

Before you can begin to design your information security controls you need to be able to define your organisation. An organisation is not just defined by what it does, but also by what shapes and influences it.

There will be stakeholders and data security laws and regulations that have a say in what matters to your organisation. They might influence your planning.

2 CLAUSE 4: Limit your information security management system to what really matters.

- **List the parts of the organisation that should be in the scope** □
- **List the internal activities, including how they interact, that should be in the scope** □
- **List any activities that are performed externally, such as by suppliers or outsourced to third parties, that should be in scope.** □

By knowing your organisation and armed with your mission or business goals, you can set a boundary to your Information Security Management System (ISMS).

You might not need an ISMS for the entire organisation; constrain the scope to the things that matter to you and your stakeholders.

3 CLAUSE 5: Make sure your top management is committed to continual improvement.

- **Write an Information Security Policy. This is the high-level policy for the organisation. Make sure it meets all the requirements of the standard.** □
- **Disseminate the policy to everyone affected by it (both internal and external)** □
- **Define roles and responsibilities for information security** □
- **Provide resources for information security and for the ISMS** □
- **Make sure someone from your senior leadership is responsible for the ISMS and document what their responsibilities are. They will be interviewed during the audit** □

Just as senior leaders direct and resource an organisation so it fulfills its purpose, they must do the same for information security.

It starts with a policy that is a statement of intent, which in turn drives the need, the activities and the resources.

4 CLAUSE 6.1.1: Address risks to the ISMS and to continual improvement

The ISMS is important to the organisation so you must list the risks that could prevent it being effective, and then have plans to mitigate them. Take into account the matters identified during Clause 4. □

5 CLAUSE 6.1.2: Define an information security risk assessment process

Define criteria for accepting risks you subsequently identify. This is your risk appetite. □

The process should ensure it considers risks to the confidentiality, integrity and availability of information in the scope of the ISMS and that each of the risks is assigned an owner. □

The process should ensure it considers risks to the confidentiality, integrity and availability of information in the scope of the ISMS and that each of the risks is assigned an owner. □

As a minimum, risks comprise the likelihood of something bad happening and the impact when it does. Your criteria for ensuring repeatable and consistent results should include impact and likelihood criteria, and then criteria for the risk levels. □

The process should ensure the risk acceptance criteria is used to determine the order of treatment for any risks that you find are unacceptable. □

Decide what security controls are needed to treat the risks and compare them against the controls in Annex A to make sure you have all those needed □

The information security risk assessment is at the heart of the standard (this is a separate process to the risks identified in 6.1.1).

The process must be defined to ensure it produces consistent and repeatable results.

6 CLAUSE 6.1.3 : Do something about the risks that are unacceptable

Decide what security controls are needed to treat the risks and compare them against the controls in Annex A to make sure you have all those needed □

Compile a Statement of Applicability (SoA), which is a list of all the Annex A controls. For each control you must explain why or why not you are implementing it, and if it is implemented. You can add in extra controls that aren't in Annex A if they're necessary to mitigate the risks. □

The information security risk treatment is where you bring risks down to acceptable levels by defining a risk treatment plan.

ISO 27001 is unusual in that it lists industry best practice information security controls in Annex A. These will form the basis of the risk treatment plan.

Produce a risk treatment plan. This is typically based on plans to implement and operate the security controls in the SoA. You must get the risk owners approval for the risk treatments. □

Rerun the risk assessment, taking into account of the risk treatment plan, to calculate the residual risk, and get the risk owners acceptance of the new risk levels. □

7 CLAUSE 6.2: Have some objectives

Plan what you need to achieve them and who is responsible □

Decide how you're going to monitor and measure performance towards the objectives □

Communicate them to everyone who need to know □

Once you have an information security policy and the risk treatment plans, you can set information security objectives

8 CLAUSE 7: Are your resources Aware, Competent and Sufficient?

Decide what resources are required (personnel, technology and infrastructure) to operate the ISMS. In the case of personnel determine the knowledge and skills required and confirm that they're present in your organisation □

Have a communications plan to make sure staff and third parties are aware of their role in supporting the ISMS and your information security policy. □

Document everything required by the standard (there's a list at the end of this checklist) and anything else you think necessary. Control the changes to your document and keep them secure. □

The ISMS and your information security operations won't work without the right resources.

27001 Mandatory Documents

CLAUSES	
clause 4.3	Scope of the ISMS
clauses 5.2 and 6.2	Information security policy and objectives
clause 6.1.2	Risk assessment and risk treatment methodology
clause 6.1.3 d	Statement of Applicability
clauses 6.1.3 e and 6.2	Risk treatment plan
clause 8.2	Risk assessment report

MANDATORY RECORDS:	
clause 7.2	Scope of the ISMS
clause 9.1	Information security policy and objectives
clause 9.2	Risk assessment and risk treatment methodology
clause 9.2	Statement of Applicability
clause 9.3	Risk treatment plan
clause 10.1	Risk assessment report
clauses A.12.4.1 and A.12.4.3	Logs of user activities, exceptions, and security events

9 CLAUSE 8: Plan and control your information security

Information security is a broad and complicated subject, so it will need planning and monitoring, and changes will need to be managed.

- **Implement the information security objectives' plans** □
- **Document everything you think necessary to ensure that the information security processes are operating** □
- **Implement change management on your information security controls and perform reviews when things aren't going as intended (don't forget your suppliers)** □
- **Carry out the risk assessment process you defined in 6.1.2** □
- **Implement the risk treatment plan you defined in 6.1.3** □

10 CLAUSE 10: Continuously monitor your information security performance

Given everything defined in the preceding clauses, this is where you measure how well your ISMS is performing. You need to know what you should measure, by whom, how and by when. The standard tells you: - you need an ongoing internal audit programme and regular management reviews. □

11 CLAUSE 10: Continuously improving

Sometimes things go wrong (non-conformities) so you must have a process for:

- **Controlling them** □
- **Fixing them** □
- **Working out why they went wrong** □
- **Taking steps to prevent it happening again** □