

ISO 27001

Information Security Management System Gap Analysis Checklist

Welcome to the **MOD1** gap analysis checklist for ISO 27001 information security management systems.

We developed this checklist to support you in conducting an initial assessment of the shortcomings of your existing information security management posture compared to the ISO 27001 certification requirements.

The checklist is intended for use by any organisation considering embarking on a project to implement an information security management system (ISMS) that can eventually be certified to the ISO international standard for information security management.

Completing the checklist should help you approximate the proposed scope of your management system implementation and determine the resources (people, time, and finances) necessary to pass the ISO certification audit.

We hope this checklist serves as a helpful resource in your ISO 27001 certification journey. At the end of this document, you can find further information on how the MOD1 ISO 27001 Gap analysis Service can help you expedite your ISMS implementation and ISO 27001 certification journey.



What is an information security management system?

An information security management system (ISMS) is a structured framework of policies, procedures, processes, practices, controls, roles, responsibilities, and resources to treat risks to confidentiality, integrity, and availability of information assets in line with organisational objectives.

Why should my organisation implement an ISMS?

Implementing an ISMS helps organisations reduce the likelihood of cybersecurity and data privacy incidents, optimise information security controls and effectively respond to threats. In addition to reducing risk, a centrally managed framework for information security and privacy governance plays a foundational role in helping companies maximise their return on security investment, enhance their reputation and gain an advantage over their competitors.

What is the purpose of an ISMS gap analysis?

An ISMS gap analysis is, for many organisations, an essential first step in planning for a successful implementation. The primary aim of a gap analysis is to support businesses in assessing the shortcomings of their existing information security management capabilities compared to a set of best practice requirements for information security, such as the NIST Cybersecurity Framework or ISO/IEC 27001.

How can an **ISMS** gap analysis help my organisation prepare for certification to **ISO 27001**?

In addition to highlighting deficiencies in your existing capabilities, a gap analysis can help approximate the proposed implementation scope and determine the resources (people, time, and finances) necessary to achieve certification readiness. The results of a gap analysis can also provide valuable insight into the feasibility of undertaking a full-blown ISO 27001 certification project before investing significant time and money into it.

What are the benefits of an **ISO 27001** certification?

An ISO 27001 certification demonstrates a genuine commitment to information security management. It goes beyond simply claiming compliance to the standard by requiring an audit performed by an accredited certification body to certify the organisation's management system. ISO 27001 is an internationally recognised and externally assured standard that conveys to stakeholders that your organisation is credible and trustworthy. It can improve customer confidence, reduce the need for customer audits and help you win new business by keeping you ahead of uncertified competitors.

Table of content

| | |
|--|----|
| Instructions for use | 1 |
| 0. Introduction | 2 |
| 1. Scope | 2 |
| 2. Normative references | 2 |
| 3. Terms and definitions | 2 |
| 4. Context of the organisation | 3 |
| 5. Leadership | 4 |
| 6. Planning | 5 |
| 7. Support | 7 |
| 8. Operation | 9 |
| 9. Performance evaluation | 10 |
| 10. Improvement | 11 |
| ISO 27001 gap analysis results | 12 |
| Annex A. Controls and Statement of Applicability | 13 |
| Kick start your journey to ISO 27001 certification with the MOD1 ISMS gap analysis service. | 15 |

Instructions for use

This gap analysis checklist provides an essential overview of requirements in questionnaire format, aligned to the structure of ISO 27001, the internationally recognised specification for an information security management system (ISMS).

Those interested in performing a preliminary assessment of their existing information security management capabilities or ISO 27001 certification readiness should review each question in the following sections to determine whether or not current measures fulfil each condition.

The number of requirements met for each clause can be calculated as a percentage of total requirements to give a quantitative estimate of certification readiness. If there is any uncertainty about whether a condition has been satisfied, the overriding view should be whether an external auditor would accept the existing provision.

The final section of the document contains an example table for a Statement of Applicability that outlines the ISO 27001 Annex A controls applicable to a particular organisation's management system.

The assessor should use this document in conjunction with an official copy of the ISO 27001 requirements and the ISO 27002 code of practice for information security controls (ISO 27002). The ISO 27000 series of standards for information security management systems are available for purchase directly from the International Standards Organisation or via their network of certified resellers.



0. Introduction

This section introduces the standard and contains no specific requirements.

1. Scope

This section states that the requirements set out in the standard apply to all organisations, regardless of type, size or nature. It also mentions that the requirements specified in clauses 4 to 10 are mandatory for an organisation to claim conformance to the standard.

2. Normative references

This section contains references to other documents in the standard series and has no specific requirements.

3. Terms and definitions

This section introduces some fundamental terms and definitions. It contains no specific requirements.

4. Context of the organisation

Clause 4 of the standard requires an assessment of internal and external issues and the needs and expectations of stakeholders relevant to the information security management system (ISMS). It also involves the determination of a suitable scope for the information security management system and a process for its implementation, maintenance and continual improvement.

Audit checklist

- ☐ Have you documented the internal and external factors affecting your ISMS?
- ☐ Have you documented the needs and expectations (including requirements) of interested parties relevant to the ISMS?
- ☐ Have you determined the scope (i.e., the boundaries and applicability) of your ISMS?
- ☐ Have you formally established the ISMS and ensured its continual improvement?

Results

| Clause 4 requirements (Checked) | Clause 4 requirements (Total) |
|---------------------------------|-------------------------------|
| | 4 |

Mandatory documentation

| ISO 27001 clause | Mandatory document |
|------------------|--------------------|
| 4.3 | ISMS scope |

Notes

5. Leadership

Clause 5 is probably the most critical component of any information security management system since even the most well-planned implementation is sure to fail without the total commitment of senior management. The leadership clause requires the establishment of an information security policy and definition of information security roles, responsibilities, and authorities.

Audit checklist

- ☐ Has top management demonstrated leadership and commitment to information security?
- ☐ Has top management committed to providing budget and resources for the establishment, implementation, maintenance and continual improvement of the ISMS?
- ☐ Has top management communicated a documented information security policy throughout the organisation?
- ☐ Has top management assigned and communicated defined information security roles, responsibilities and accountability throughout the organisation?

Results

| Clause 5 requirements (Checked) | Clause 5 requirements (Total) |
|---------------------------------|-------------------------------|
| | 4 |

Mandatory documentation

| ISO 27001 clause | Mandatory document |
|------------------|-----------------------------|
| 5.2 | Information security policy |

Notes

6. Planning

Clause 6 of the standard requires the general risks and opportunities that may impact the intended outcomes of the management system to be reviewed and treated. It also involves the creation of processes to assess and treat information security risks and a "statement of applicability" used to document the ISO 27001 Annex A controls that have been deemed relevant to the ISMS as a result of the initial risk assessment. Finally, clause 6 requires the definition of information security objectives that align with organisational objectives.

Audit checklist

- ☐ Do you have a well-defined and documented procedure for identifying information security risks and opportunities for improvement relevant to the context of the organisation and the needs, expectations and requirements of interested parties?
- ☐ Do you have a well-defined and documented procedure for assessing information security risks and opportunities for improvement?
- ☐ Do you have a well-defined and documented procedure for treating information security risks and opportunities for improvement?
- ☐ Have you completed an initial risk assessment as per the documented procedure for assessing information security risks and opportunities for improvement?
- ☐ Have you completed an initial risk treatment plan following the above risk assessment and document the results?
- ☐ Have you created a "statement of applicability" that documents the ISO 27001 Annex A controls that have been deemed relevant to the ISMS?
- ☐ Do you have a well-defined and documented procedure for identifying information security objectives and creating specific, measurable, achievable, relevant, and time-bound plans for achieving them?

Results

| Clause 6 requirements (Checked) | Clause 6 requirements (Total) |
|---------------------------------|-------------------------------|
| | 7 |

Mandatory documentation

| ISO 27001 clause | Mandatory document |
|------------------|---------------------------------|
| 6.1.2 | Risk assessment process |
| 6.1.3 | Risk treatment process |
| 6.1.3 | Risk treatment plan |
| 6.1.3 | Statement of applicability |
| 6.2 | Information security objectives |

Notes



7. Support

Clause 7 requires the organisation of the management of documented information. Its requirements also cover resources and communication, the management of competency, and awareness training for information security and the information security management system.

Audit checklist

- ☐ Have you determined and provided the resources necessary for the establishment, implementation, maintenance and continual improvement of the ISMS?
- ☐ Have you ensured that personnel with ISMS-related roles have the necessary levels of information security education, training and experience?
- ☐ Have the competencies of personnel with ISMS-related roles been documented appropriately?
- ☐ Do you ensure organisation-wide awareness of information security policies and procedures and individual roles and responsibilities concerning information security?
- ☐ Do you have well-defined and documented policies and procedures for handling internal and external communications about the ISMS?
- ☐ Do you have an official documentation structure or hierarchy that includes both documentation directly required by ISO 27001 and documentation deemed necessary for an effective information security program?
- ☐ Do you have well-defined and documented policies and procedures for ensuring the proper review and approval of new or updated ISMS documentation?
- ☐ Do you have well-defined and documented policies and procedures for ensuring proper control and handling of ISMS documentation?

Results

| Clause 7 requirements (Checked) | Clause 7 requirements (Total) |
|---------------------------------|-------------------------------|
| | 8 |

Mandatory documentation

| ISO 27001 clause | Mandatory document |
|------------------|--|
| 7.2 | Documented information as evidence of competence (records of education, training and experience) |

Notes



8. Operation

Clause 8 of the standard involves the execution of the risk assessment and treatment process established in clause 6. The clause also requires the implementation of plans for the control of outsourced operations and the scheduling of regular risk assessments at predetermined intervals.

Audit checklist

- ☐ Do you have a process by which you plan, implement, control and review ISMS operations and keep evidence to verify that the overall strategy and related information security policies and procedures are being followed?
- ☐ Does your organisation undergo risk assessments at planned intervals or whenever significant changes occur and document the results?
- ☐ Do you create and carry out documented risk treatment plans following risk assessments and record the results?

Checklist

| Clause 8 requirements (Checked) | Clause 8 requirements (Total) |
|---------------------------------|-------------------------------|
| | 3 |

Mandatory documentation

| ISO 27001 clause | Mandatory document |
|------------------|---|
| 8.1 | Documented information to the extent necessary to have confidence that the processes have been carried out as planned |
| 8.2 | Risk assessment results |
| 8.3 | Risk treatment results |

Notes

9. Performance evaluation

Clause 9 of the standard requires the implementation of measures and metrics to evaluate the management system's performance. It entails the planning and execution of internal audits and management reviews to ensure that the management system continues to meet its objectives and can be continuously improved.

Audit checklist

- ☐ Do you use metrics for evaluating the performance and effectiveness of your information security program?
- ☐ Do you carry out internal audits of the ISMS against the ISO 27001 standard at defined intervals?
- ☐ Do you conduct management reviews of the ISMS at defined intervals?

Checklist

| Clause 9 requirements (Checked) | Clause 9 requirements (Total) |
|---------------------------------|-------------------------------|
| | 3 |

Mandatory documentation

| ISO 27001 clause | Mandatory document |
|------------------|--|
| 9.1 | Documented information as evidence of the monitoring and measurement results |
| 9.2 | Documented information as evidence of the audit program |
| 9.2 | Documented results as evidence of the audit results |
| 9.3 | Documented results as evidence of the results of management reviews |

Notes

10. Improvement

The 10th and final clause of the standard addresses requirements for the definition, identification and elimination of nonconformities. It also requires the implementation of measures to continually improve the suitability, adequacy and effectiveness of the information security management system.

Audit checklist

- ☐ Do you have a well-defined and documented corrective procedure for addressing nonconformities with the ISO 27001 standard?
- ☐ Do you ensure and document evidence of the continual improvement of your information security program?

Checklist

| Clause 10 requirements (Checked) | Clause 10 requirements (Total) |
|----------------------------------|--------------------------------|
| | 2 |

Mandatory documentation

| ISO 27001 clause | Mandatory document |
|------------------|--|
| 10.1 | Documented information as evidence of the nature of the nonconformities, subsequent corrective actions and their results |

Notes

ISO 27001 gap analysis results

| Clause | Requirements (Met) | Requirements (Total) |
|--------------------------------|--------------------|----------------------|
| 4. Context of the organisation | | 4 |
| 5. Leadership | | 4 |
| 6. Planning | | 7 |
| 7. Support | | 8 |
| 8. Operation | | 3 |
| 9. Performance evaluation | | 3 |
| 10. Improvement | | 2 |
| Totals | | |

% Certification readiness

Requirements (Met) ÷ Requirements (Total) x 100 = |



Annex A. Controls and Statement of Applicability

ISO 27001 Annex A is a catalogue of best practice information security controls split into 14 domains. The following “Example Statement of Applicability (Annex A.5 – Information Security Policies)” can be used as a template and extended to cover the 144 Annex A controls.

It is the responsibility of the organisation to determine which of the 114 controls are relevant to the scope of their information security management system. The standard requires that any Annex A control deemed “not applicable” includes a description of justification for its exclusion as part of the statement of applicability.

Example Statement of Applicability

| Annex A Control | | Applicable (Y/N) | Implemented (Y/N) | Justification for inclusion or exclusion |
|-----------------|---|---------------------|----------------------|---|
| Reference | Description | | | |
| A.5.1.1 | Policies for information security | Y | Y | An information security policy is essential to establish a general approach to protecting the confidentiality, integrity and availability of the organisation's information assets. |
| A.5.1.2 | Review of the policies for information security | Y | N | Regular reviews of policies and procedures help ensure that the organisation keeps up to date with the latest regulations, technology, and industry best practices. |

Mandatory documentation

The following documents are mandatory requirements for ISO 27001 certification based on the assumption that they are “in scope” per the statement applicability:

| ISO 27001 Annex A control | Mandatory document |
|---------------------------|---|
| A.6.1.1 | Documented evidence of responsibilities for information security |
| A.8.1.1 | Information asset inventory |
| A.8.1.3 | Acceptable use policy |
| A.9.1.1 | Access control policy |
| A.12.1.1 | Operating procedures |
| A.13.2.4 | Requirements for confidentiality or non-disclosure agreements |
| A.14.2.5 | Policy and procedures for secure systems engineering for all operations concerning the implementation of information systems |
| A.15.1.1 | Policy and procedures for mitigating risks associated with third party supplier access to the organisation's information assets |
| A.16.1.5 | Incident management policy and procedures |
| A.17.1.2 | Business continuity policy, procedures |
| A.18.1.1 | Overview of legislative statutory, regulatory, contractual requirements, and description of the approach to meet these requirements for every information system and organisation |

Notes

Kick start your journey to ISO 27001 certification with the MOD1 ISMS gap analysis service

We trust you will find this checklist a helpful resource in support of your journey to establish an ISMS that meets the requirements of ISO 27001.

We also appreciate that embarking on a project to implement a certifiable ISMS can seem daunting, especially if your organisation lacks the relevant internal expertise to accurately assess the shortcomings of your existing information security capabilities compared to the standard's requirements.

That's why we created the MOD1 ISMS Gap Analysis Service, a comprehensive assessment that provides the following benefits:

- Indicates what you need to do, how long it might take and how much it might cost
- Assesses the feasibility of undertaking an ISO27001 certification project
- Serves as input to subsequent scoping and road-mapping exercises
- Informs your leadership of critical problem areas and concerns
- Reduces effort and cost by identifying duplicate processes
- Outlines the requirements that you have already met
- Identifies problems and areas for improvement

Here's how it works:

Step 1 - Gap analysis initiation workshop

We present a detailed explanation of the gap assessment process in the context of the full ISO 27001 implementation and agree on the appointment of an internal project coordinator to liaise between the consultant and staff. Assigning an internal project coordinator ensures that our requests for information about existing policies, procedures, processes and controls are managed to minimise disruption whilst ensuring the gap analysis is prioritised appropriately.

Step 2 - Interviews with key personnel

We undertake a series of interviews and walkthroughs with key personnel to establish which processes and procedures have been implemented and the extent to which they are executed. These discussions help us understand how the guidelines are followed and identify possible control weaknesses not evident from documentation reviews.

Step 3 - Analysis and assessment

Our accredited cybersecurity, privacy, risk, and compliance experts conduct a detailed analysis of the documented evidence and operation of critical processes. We then compare the assessment's findings against the standard's requirements to identify opportunities for improvement, address shortfalls and mitigate the risk of data breaches.

Step 4 - Report

The results of our assessment form the basis of a gap analysis report that summarises your existing capabilities, highlights deficiencies and provides recommendations on measures required to meet the certification objectives. The report addresses the requirements of ISO 27001 Clause 4 - 10, and each of the 114 Annex A controls to provide a concise description of the following:

- What arrangements are currently in place (policies, procedures and technical controls)
- Whether the current arrangements could be adapted to meet the standard's requirements
- An indication of resource requirements for process development
- An estimate of the timeframe for implementation
- Potential challenges in meeting the requirements
- Implications for certification by an external auditor

The report will indicate your compliance status (red/amber/green) against the management system clauses and our expert recommendations on the steps necessary to satisfy each requirement.

Why MOD1?

Our success is founded on ethics, agility, credibility and execution excellence – these guiding principles ensure we deliver consistent value to our clients.

Our cybersecurity, privacy, risk and compliance consultants are professionally certified in information security management systems (ISO 27001 Lead Implementor).

We are accustomed to working in highly regulated business sectors, such as digital life sciences and financial services, where the protection of critical information assets is key to the achievement of organisational objectives.


We appreciate that no two organisations are the same, which is why we tailor each implementation to the size, complexity, risk appetite and budget of each and every client.

Our structured implementation strategy and well-established methodology ensure consistent, repeatable and measurable results.



Take the first step to aligning your information security management posture with ISO 27001 best practices

Claim your free and non-binding 30-minute consultation with a MOD1 cybersecurity, data privacy, risk and compliance consultant for further information on how we can support you in your path to ISO 27001 certification.



< August >

| SUN | MON | TUE | WED | THU | FRI | SAT |
|-----|-----|-----|-----|-----|-----|-----|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| 29 | 30 | 31 | 1 | 2 | 3 | 4 |
| 5 | 6 | 7 | 8 | 9 | 10 | 11 |

Meeting duration

30 mins

What time works best?

UTC +07:00 Central European Time

5:30 pm

5:45 pm

6:00 pm

6:15 pm

6:30 pm

6:45 pm

www.mod1consulting.com