ISO 27001 Checklist & Gap Analysis: Determine Initial & On

Overview: Fill out the following checklist as you complete your ISO 27001 ce
These steps will help you prepare for ISO 27001 implementation and certifica
cure-all solution - every company has unique security needs which should be

To speak to our experts about hands-on ISO 27001 consulting, visit **https://v**
or e-mail **info@pivotpointsecurity.com**.

ISO 27001 clause	Mandatory requirement for the ISMS
4	**Information Security Management System**
4.1	**Understanding the organization and its context**
4.1	The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.
4.2	**Understanding the needs and expectations of interested**
4.2	The organization shall determine: a) interested parties that are relevant to the information security management system; and b) the requirements of these interested parties relevant to information security
4.3	**Determining the scope of the information security manag**
4.3	The organization shall determine the boundaries and applicability of the information security management system to establish its scope.
4.4	**Information security management system**
4.4	The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.
5	**Leadership**
5.1	**Leadership and commitment**
5.1	Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by:
5.1 (a)	ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;
5.1 (b)	ensuring the integration of the information security management system requirements into the organization's processes;
5.1 (c)	ensuring that the resources needed for the information security management system are available;
5.1 (d)	communicating the importance of effective information security management and of conforming to the information security management system requirements;

5.1 (e)	ensuring that the information security management system achieves its intended outcome(s);
5.1 (f)	directing and supporting persons to contribute to the effectiveness of the information security management system;
5.1 (g)	promoting continual improvement; and
5.1 (h)	supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.
5.2	
5.2	Top management shall establish an information security policy that: a) is appropriate to the purpose of the organization; b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives; c) includes a commitment to satisfy applicable requirements related to information security; and d) includes a commitment to continual improvement of the information security management system. The information security policy shall: e) be available as documented information; f) be communicated within the organization; and g) be available to interested parties, as appropriate
5.3	**Organizational roles, responsibilities and authorities**
5.3	Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.
6	**Planning**
6.1	**Actions to address risks and opportunities**
6.1.1	**General**
6.1.1	When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to: a) ensure the information security management system can achieve its intended outcome(s); b) prevent, or reduce, undesired effects; and c) achieve continual improvement
6.1.1 (d)	The organization shall plan actions to address these risks and opportunities; and
6.1.1 (e)	The organization shall plan how to: 1) integrate and implement these actions into its information security management system processes; and 2) evaluate the effectiveness of these actions.
6.1.2	**Information security risk assessment**
6.1.2	The organization shall define and apply an information security risk assessment process that:

6.1.2 (a)	establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria; and 2) criteria for performing information security risk assessments;
6.1.2 (b)	ensures that repeated information security risk assessments produce consistent, valid and comparable results;
6.1.2 (c)	identifies the information security risks: 1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and 2) identify the risk owners;
6.1.2 (d)	analyses the information security risks: 1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize; 2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and 3) determine the levels of risk;
6.1.2 (e)	evaluates the information security risks: 1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and 2) prioritize the analyzed risks for risk treatment.
6.1.3	**Information security risk treatment**
6.1.3	The organization shall define and apply an information security risk treatment process to:
6.1.3 (a)	select appropriate information security risk treatment options, taking account of the risk assessment results;
6.1.3 (b)	determine all controls that are necessary to implement the information security risk treatment option(s) chosen;
6.1.3 (c)	compare the controls determined in 6.1.3 (b) above with those in Annex A and verify that no necessary controls have been omitted;
6.1.3 (d)	produce a Statement of Applicability that contains the necessary controls (see 6.1.3.b and c) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A;
6.1.3 (e)	formulate an information security risk treatment plan; and
6.1.3 (f)	obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.
6.2	**Information security objectives and plans to achieve ther**
6.2	The organization shall establish information security objectives at relevant functions and levels.

6.2	The information security objectives shall: a) be consistent with the information security policy; b) be measurable (if practicable); c) take into account applicable information security requirements, and risk assessment and risk treatment results; d) be communicated; and e) be updated as appropriate.
6.2	When planning how to achieve its information security objectives, the organization shall determine: f) what will be done; g) what resources will be required; h) who will be responsible; i) when it will be completed; and j) how the results will be evaluated.
7	**Support**
7.1	**Resources**
7.1	The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.
7.2	**Competence**
7.2	The organization shall:
7.2 (a)	determine the necessary competence of person(s) doing work under its control that affects its information security performance;
7.2 (b)	ensure that these persons are competent on the basis of appropriate education, training, or experience;
7.2 (c)	where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and
7.2 (d)	retain appropriate documented information as evidence of competence.
7.3	**Awareness**
7.3	Persons doing work under the organization’s control shall be aware of:
7.3 (a)	the information security policy;
7.3 (b)	their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and
7.3 (c)	the implications of not conforming with the information security management system requirements.
7.4	**Communication**
7.4	The organization shall determine the need for internal and external communications relevant to the information security management system including:
7.4 (a)	on what to communicate;
7.4 (b)	when to communicate;
7.4 (c)	with whom to communicate;
7.4 (d)	who shall communicate; and

7.4 (e)	the processes by which communication shall be effected.
7.5	**Documented information**
7.5.1	**General**
7.5.1	The organization’s information security management system shall include:
7.5.1 (a)	documented information required by this International Standard; and
7.5.1 (b)	documented information determined by the organization as being necessary for the effectiveness of the information security management system.
7.5.2	**Creating and updating**
7.5.2	When creating and updating documented information the organization shall ensure appropriate:
7.5.2 (a)	identification and description (e.g. a title, date, author, or reference number);
7.5.2 (b)	format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and
7.5.2 (c)	review and approval for suitability and adequacy.
7.5.3	**Control of documented information**
7.5.3	Documented information required by the information security management system and by this International Standard shall be controlled to ensure:
7.5.3 (a)	it is available and suitable for use, where and when it is needed; and
7.5.3 (b)	it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).
7.5.3	For the control of documented information, the organization shall address the following activities, as applicable:
7.5.3 (c)	distribution, access, retrieval and use;
7.5.3 (d)	storage and preservation, including the preservation of legibility;
7.5.3 (e)	control of changes (e.g. version control); and
7.5.3 (f)	retention and disposition.
7.5.3	Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.
8	**Operation**
8.1	**Operational planning and control**
8.1	The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2.
8.1	The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.

8.1	The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.
8.1	The organization shall ensure that outsourced processes are determined and controlled.
8.2	**Information security risk assessment**
8.2	The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2.a.
8.2	The organization shall retain documented information of the results of the information security risk assessments.
8.3	**Information security risk treatment**
8.3	The organization shall implement the information security risk treatment plan.
8.3	The organization shall retain documented information of the results of the information security risk treatment.
9	**Performance evaluation**
9.1	**Monitoring, measurement, analysis and evaluation**
9.1	The organization shall evaluate the information security performance and the effectiveness of the information security management system. The organization shall determine:
9.1 (a)	what needs to be monitored and measured, including information security processes and controls;
9.1 (b)	the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;
9.1 (c)	when the monitoring and measuring shall be performed;
9.1 (d)	who shall monitor and measure;
9.1 (e)	when the results from monitoring and measurement shall be analyzed and evaluated; and
9.1 (f)	who shall analyze and evaluate these results.
9.2	**Internal audit**
9.2	The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:
9.2 (a)	conforms to 1) the organization’s own requirements for its information security management system; and 2) the requirements of this International Standard;
9.2 (b)	is effectively implemented and maintained.
9.2	The organization shall:
9.2 (c)	plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits;
9.2 (d)	define the audit criteria and scope for each audit;

9.2 (e)	select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;
9.2 (f)	ensure that the results of the audits are reported to relevant management; and
9.2 (g)	retain documented information as evidence of the audit programme(s) and the audit results.
9.3	**Management review**
9.3	Top management shall review the organization’s information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness. The management review shall include consideration of:
9.3 (a)	the status of actions from previous management reviews;
9.3 (b)	changes in external and internal issues that are relevant to the information security management system;
9.3 (c)	feedback on the information security performance, including trends in: 1) nonconformities and corrective actions; 2) monitoring and measurement results; 3) audit results; and 4) fulfilment of information security objectives;
9.3 (d)	feedback from interested parties;
9.3 (e)	results of risk assessment and status of risk treatment plan; and
9.3 (f)	opportunities for continual improvement.
9.3	The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system. The organization shall retain documented information as evidence of the results of management reviews.
10	**Improvement**
10.1	**Nonconformity and corrective action**
10.1	When a nonconformity occurs, the organization shall:
10.1 (a)	react to the nonconformity, and as applicable: 1) take action to control and correct it; and 2) deal with the consequences;
10.1 (b)	evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by: 1) reviewing the nonconformity; 2) determining the causes of the nonconformity; and 3) determining if similar nonconformities exist, or could potentially occur;
10.1 (c)	implement any action needed;
10.1 (d)	review the effectiveness of any corrective action taken; and
10.1 (e)	make changes to the information security management system, if necessary.
10.1	Corrective actions shall be appropriate to the effects of the nonconformities encountered. The organization shall retain documented information as evidence of:

10.1 (f)	the nature of the nonconformities and any subsequent actions taken, and
10.1 (g)	the results of any corrective action.
10.2	**Continual improvement**
10.2	The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.

Legend

Count	Status Code - Meaning
0	Process is defined / documented and practiced / implemented
0	Process is practiced / implemented without adequate documentation; Process must be defined / documented to ensure repeatability of process and mitigate the risks.
100	Process is defined and not practiced
0	Process is not applicable for the company as per the scope
100	

ı-Going Status of ISO 27001 Implementation

ertification journey to help track your progress.
ation, but this checklist is not meant to serve as a 100%
evaluated by an expert before pursuing certification.

vww.pivotpointsecurity.com/company/contact/

Status
Not Implemented
parties
Not Implemented
jement system
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented

Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented

Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
n
Not Implemented

Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented

Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented

Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented

Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented
Not Implemented

Not Implemented
Not Implemented
Not Implemented

Status Code
Fully Implemented
Partially Implemented
Not Implemented
NA (Not Applicable)

Do You Have Documents / Records to Reference to Prove Compliance?	Notes on Your Findings

Website:

https://www.pivotpointsecurity.com/company/contact/

Email:

info@pivotpointsecurity.com

Notes on Your Recommendations & Next Steps