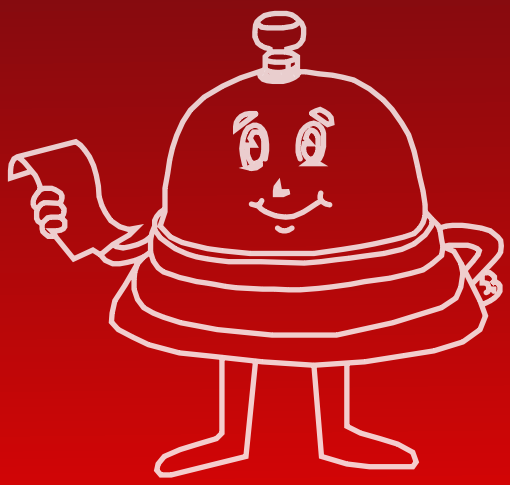
KLEAP

CYBERSECURITY

ISO 27001_2022 Checklist



Brief Overview

ISO/IEC 27001:2022 is a comprehensive standard, and understanding what certification actually requires at the clause level is not always straightforward.

This checklist breaks down every clause and sub-clause of the standard, clearly stating the core requirement of each and the specific questions that need to be answered to demonstrate that controls are in place.

It is structured to reflect how an auditor approaches the standard - so whether you are preparing for initial certification, a surveillance audit, or an internal readiness review, you have a clear and practical reference for how to go about it in detail.

Table of Contents

04

Context of the Organization

Understanding the organization & its context

Have the external and internal issues that affect the ISMS been determined?

Understanding the needs & expectations of interested parties

Have the organization determined the interested parties that are relevant to the ISMS?

Has the organization determined needs & expectations of the interested parties?

Determining the scope of the information security management system

Has the organization defined the scope of ISMS including the in Scope departments, interfaces, locations etc?

Is the range of the Scope accurately determined & documented, with clearly specified limits and relevance?

Information security management system

Does the created, documented, & implemented a comprehensive ISMS that meets the standards of ISO 27001 as well as continuously Improving It?

05 Leadership

Leadership and Commitment

Does the Top Management demonstrate leadership & commitment to the ISMS by providing resources & communication effectively?(See list **A** to **H**)

Policy

Is there an established information security policy that is appropriate to ISMS.

Does the information security policy gives a framework for setting objectives, & demonstrates commitment for continual improvement of ISMS

Has the organization determined needs & expectations of the interested parties?

Organizational roles,responsibilities and authorities

Are the roles, responsibilities & authorities relevant to ISMS scope clearly defined and communicated?

Is the range of the Scope accurately determined & documented, with clearly specified limits and relevance?

Are the responsibilities & authorities for conformance and reporting on ISMS performance assigned?

06 Planning

Actions to address risks & opportunities

General

- Have the internal and external issues, and the requirements of interested parties been considered to determine the risks & opportunities that need to be addressed to ensure that ISMS achieve its outcome.
- Have the internal and external issues, and the requirements of interested parties been considered to achieve continual improvement.
- Have actions to address risks & opportunities been planned and integrated in to the ISMS processes and are they evaluated for effectiveness?

Information Security Assesment

- Is a documented information security risk assessment process defined and applied?
- Does the risk assessment process identify risk associated with CIA for information within the scope of ISMS and risk owners identified?
- Are risks analysed to assess the realistic likelihood & potential consequences that would result, if they were to occur and have the levels of risks been determined?
- Is a documented information security risk assessment process defined and applied?

General

- Is there a documented information security risk treatment process?
- Have controls determined to implement risk treatment option chosen?
- Have controls determined, been compared with Annex A to verify that no necessary controls have been missed?
- Has a Statement of Applicability been created?
- Is there a formulated risk treatment plan available?
- Has the organization obtained risk owners for residual risk acceptance?
- Is there a documented information security risk treatment process?

Information security objectives & planning to achieve them

- Have measurable ISMS objectives and targets been established, communicated, and documented through out the organization?
- Is documented information on the information security objectives retained?
- In setting objectives, has organization determined what needs to be done, when and by whom?

Planning of changes

- Does the changes are carried out in a planned manner?

07

Support

Resources

Has the organization determined resources needed for the ISMS?

Competence

Has the organization determined the competency of the persons relevant to ISMS?

Has the organization taken corrective measures to acquire the necessary competence

Has the organization maintained documented information as evidence for showcasing that the persons relevant to ISMS have necessary competence?

Awareness

Does the organization ensures that the employees are aware about the information security policy?

Has the organization defined & documented the Information security awareness plan?

Does the organization have a method to evaluate the effectiveness of the awareness training?

Are the employees aware of the implications of not conforming the information security requirements?

Communication

Has the organization developed internal and external communication plan?

Does the communication plan include details of what to share ,when to share, with whom to shrae, how to share and whom to share?

Actions to address risks & opportunities

General

- Has the organization determined the documented information required & necessary for the effectiveness of the ISMS?

Creating and Updating

- Has the organization defined naming conventions including (document title, date, author & approval)?
- Is the documented information in the appropriate format, and it has been identifi-ed, reviewed and approved for suitability ?

Control of documented information

- Is the documented information is available when it is needed?
- Does the organization protects the documented information from the loss of CIA?
- Has the organization addressed the distribution, access, retrieval & use of the documented information?
- Is the documented information properly stored and adequately preserved for its legibility?
- Is the documented information maintained effective version control procedures to all changes?
- Is the documented information maintained & established policies for the retention & disposition ?

08 Operation

Operational planning and Control

Does the organization has a programme to ensure that the ISMS achieve its outcomes, requirements, and objectives have been implemented & developed?

Is documented evidence retained to demonstrate that processes have been carried out as planed?

Are changes planned & controlled, & unintended changes reviewed to mitigate any adverse results?

Information Security Risk Assessment

Are the risk assessments performed at planned intervals / when changes occur, and is documented information retained?

Information Security Risk Treatment

Has the risk treatment plan implemented & retain documented information of the results of the information security risk treatment.

09 Performance Evaluation

Monitoring, measurement, analysis and evaluation

- Does the organization determine the needs & methods for monitoring, measurement, analysis and evaluation of security processes & controls?
- Does the review consider changes to the internal & external issues
- Does the organization ensure that the selected methods produce comparable, repeatable and reproducible results?
- Has the organization determined the frequency & what needs to be monitored & measured, when and by whom?
- Has the organization determined what needs to be monitored & analysed ,when and by whom?
- Is the documented information retained as evidence of the results of monitoring and measurement?

General

- Does the Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness?

General

- Does the organization plan, establish, implement and maintain an internal audit program, also defined the frequency of internal audits?
- Has the organization defined the objective and criteria for the audit?
- Are the results of internal audit report to relevant management ?
- Are results of audits reported to management, and is documented information about audit program & results retained?

Management review

General

Does the top management review the effectiveness of ISMS at planned intervals?

Management review inputs

Does the review consider results from previous management reviews?

Does the review consider changes to the internal & external issues

Does the review consider changes to the needs & expectations of interested parties?

Does the review consider feedback on the information security performance?

Does the review consider feedback from interested parties?

Does the review consider results of risk assessment & risk treatment plan?

Does the review consider opportunities for continual improvement?

Management review results

Does the output of the review include decisions related to continual improvement opportunities and any needs for changes to the ISMS?

Has the organization retained documented information as evidence for the results of the management reviews?

Are Are the results of the management review documented, acted upon & communicated to interested parties as appropriate? results of internal audit report to relevant management ?

10 Improvement

Continual Improvement

Does the organization continually improve the suitability, adequacy and effectiveness of the ISMS?

Nonconformity and corrective action

Does the organization taken any steps on identified non-conformities?

Does the organization taken any actions to control & correct the non-conformities?

Does the organization identifies the root cause for the non-conformities?

Does the organization taken steps to eliminate the root cause?

Does the organization taken steps to identify similar non-conformities within the organization?

Does the organization take steps to review the effectiveness of corrective actions taken?

Is documented information retained as evidence of the nature of non-conformities, actions taken and the results?

KLEAP

CYBERSECURITY

https://kleapcybersecurity.com/

info@kleapcybersecurity.com

4111, Briargrove Circle, Raleigh,
North Carolina, 27607, USA