ISO 27001 2013
Translated into Plain English

This page is a summary only. It does not present our entire product.
If you would like to see the rest of this material, please place an order.
Our products use language that is clear, precise, and easy to understand.

ISO 27001 2013 is an Information Security Management standard.
Use it to manage and control your information security risks, to protect and preserve the confidentiality, integrity, and availability of information, and to establish your information security management system (ISMS).

4. Contextual Requirements

4.1 Understand your organization and its context

- Identify and understand your organization's context before you establish its information security management system (ISMS).
- Identify the *internal* issues that are relevant to your organization's purpose and consider the influence these issues could have on its ability to achieve the outcomes that its ISMS intends to achieve.
  - Determine the influence your *internal stakeholders* could have.
  - Determine the influence your approach to *governance* could have.
  - Determine the influence your organization's *capabilities* could have.
  - Determine the influence your organization's *culture* could have.
  - Determine the influence your organization's *contracts* could have.
- Identify the *external* issues that are relevant to your organization's purpose and consider the influence these issues could have on its ability to achieve the outcomes that its ISMS intends to achieve.
  - Determine the influence *environmental conditions* could have.
  - Determine the influence *key trends and drivers* could have.
  - Determine the influence *external stakeholders* could have.

4.2 Define the needs and expectations of interested parties

- Identify all of the parties that have an interest in your organization's ISMS.
- Identify their requirements including their needs and expectations.

4.3 Figure out what your ISMS should apply to and clarify its scope

- Figure out what your organization's ISMS should apply to and what its boundaries should be.
- Use boundaries and applicability information to clarify the scope of your organization's ISMS.
- Document the scope of your organization's ISMS.
- Control your organization's ISMS scope document.

4.4 Develop an ISMS that complies with this international standard

- Establish an ISMS in accordance with the ISO IEC 27001 standard.

5. Leadership Requirements

5.1 Provide leadership and show that you support your ISMS

- Demonstrate a commitment to your ISMS.
  - Ensure that ISMS policies are established.
  - Ensure that ISMS objectives are established.
  - Ensure that ISMS achieves its intended outcomes.
  - Ensure that ISMS requirements become an integral part of your organization's processes.
  - Ensure that necessary ISMS resources are available when they are needed.
- Communicate a commitment to your ISMS.
  - Make sure that people understand how important information security actually is.
  - Encourage managers to demonstrate their leadership and commitment to information security within their own areas.

5.2 Establish an information security policy

- Establish an information security policy for your organization.
  - Make sure that your information security policy is appropriate and supports your organization's purpose.
  - Make sure that your information security policy either includes security objectives or can be used to establish these objectives.
  - Make sure that your information security policy makes a commitment to comply with all relevant information security requirements.

5.3 Assign responsibility and authority for your ISMS

- Allocate responsibility and authority for carrying out information security roles to the appropriate people within your organization.
- Communicate all relevant information security management roles, responsibilities, and authorities.

6. Planning Requirements

6.1 Specify actions to manage risks and address opportunities

6.1.1 Consider risks and opportunities when you plan your ISMS

- Identify the risks and opportunities that could influence the effectiveness of your organization's ISMS or disrupt its operation.
  - Consider how your internal and external issues could affect how well your ISMS is able to achieve intended outcomes.
  - Consider how your legal and regulatory requirements could affect how well your ISMS is able to achieve its intended outcomes.
- Figure out what you need to do to address the risks and opportunities that could influence the effectiveness of your organization's ISMS or disrupt its operation.

6.1.2 Establish an information security risk assessment process

- Define an information security risk assessment process.
  - Figure out how you're going to perform risk assessments.
  - Figure out how you're going to identify risk owners.
  - Figure out how you're going to ensure that your risk assessments produce consistent and valid results.
- Assess your organization's information security risks.
  - *Identify* your organization's information security risks.
  - *Analyze* your organization's information security risks.
  - *Evaluate* your organization's information security risks.
  - *Prioritize* your organization's information security risks.
- Document your information security risk assessment process.

6.1.3 Develop an information security risk treatment process

- Define an information security risk treatment process.
  - Figure out how you're going to select appropriate information security risk treatment options.
  - Figure out how you're going to select the controls that will be needed to implement your risk treatment options.
  - Figure out how you're going to formulate an information security risk treatment plan.
- Apply your information security risk treatment process.
- Document your information security risk treatment process.

6.2 Set security objectives and develop plans to achieve them

- Establish your organization's information security objectives.
- Establish plans to achieve information security objectives.
  - Specify what must be done to achieve your objectives.
  - Specify who will be responsible for achieving objectives.

7. Support Requirements

7.1 Support your ISMS by providing the necessary resources

- Identify and provide the resources that your ISMS needs.

7.2 Support your ISMS by making sure that people are competent

- Identify the competence requirements of those under your organization's control who have an impact on its information security performance.
- Acquire the necessary competence whenever current personnel fail to meet your organization's information security competence requirements.
- Evaluate the effectiveness of any actions taken to acquire the information security competence your organization needs to have.

7.3 Support your ISMS by making people aware of their responsibilities

- Make sure that the people who work for your organization understand and are aware of its information security policy.
- Make sure that the people who work for your organization understand how they can support and help enhance the effectiveness of your ISMS.

7.4 Support your ISMS by identifying your communication needs

- Identify your organization's *internal* ISMS communication needs.
- Identify your organization's *external* ISMS communication needs.

7.5 Support your ISMS by managing all relevant information

7.5.1 Include the information and documents that your ISMS needs

- Figure out how extensive your ISMS documentation needs to be.
- Identify all the documents and records that your ISMS needs.

7.5.2 Manage the creation and modification of your ISMS documents

- Manage the creation and modification of your organization's ISMS documents and records (documented information).
  - Make sure that your ISMS documents and records are properly identified and described.
  - Make sure that your ISMS documents and records are properly formatted and presented.
  - Make sure that your ISMS documents and records are properly reviewed and approved.

7.5.3 Control your organization's ISMS information and documents

- Control all of the information security documents and records (documented information) that your organization needs.
  - Control all documents and records that your ISMS needs in order to preserve the confidentiality, integrity, and availability of information.
  - Control all the documents and records required by this standard.
- Control how ISMS documents and records are controlled.
  - Control how ISMS documents and records are *created*.
  - Control how ISMS documents and records are *identified*.
  - Control how ISMS documents and records are *distributed*.
  - Control how ISMS documents and records are *stored*.
  - Control how ISMS documents and records are *retrieved*.
  - Control how ISMS documents and records are *accessed*.
  - Control how ISMS documents and records are *used*.
  - Control how ISMS documents and records are *protected*.
  - Control how ISMS documents and records are *changed*.
  - Control how ISMS documents and records are *preserved*.

8. Operational Requirements

8.1 Carry out operational planning and control processes

- Establish the processes that your organization needs in order to meet its information security requirements and implement the actions needed to address its information security risks and opportunities.
  - Plan the development of your ISMS processes.
  - Develop your organization's ISMS processes.
  - Implement your organization's ISMS processes.
  - Control internal and outsourced ISMS processes.
  - Maintain your organization's ISMS processes.
- Implement plans to achieve your organization's information security objectives (these plans were developed in part 6.2).

8.2 Conduct regular information security risk assessments

- Perform regular information security risk assessments.
- Prioritize your risks whenever risk assessments are done.
- Maintain a record of your of risk assessment results.

8.3 Implement your information security risk treatment plan

- Implement your information security risk treatment plan.
- Maintain a record of your risk treatment results.

9. Evaluation Requirements

Detailed PDF SAMPLE

9.1 Monitor, measure, analyze, and evaluate your information security

- Figure out how you're going to assess the performance of your information security and determine the effectiveness of your ISMS.
  - Figure out how you're going to *monitor* the performance of your organization's information security and the effectiveness of its ISMS.
  - Figure out how you're going to *measure* the performance of your organization's information security and the effectiveness of its ISMS.
  - Figure out how you're going to *analyze* the performance of your organization's information security and the effectiveness of its ISMS.
  - Figure out how you're going to *evaluate* the performance of your organization's information security and the effectiveness of its ISMS.
- Assess the performance of your information security and determine the effectiveness of your ISMS.

9.2 Set up an internal audit program and use it to evaluate your ISMS

- Plan the development of an internal ISMS audit program.
  - Make sure that your audit program is capable of determining whether or not your ISMS conforms to requirements.
  - Make sure that your audit program is capable of determining whether or not your ISMS has been implemented effectively.
- Establish your internal ISMS audit program.
  - Establish your internal audit methods.
  - Establish internal audit responsibilities.
  - Establish internal audit planning requirements.
  - Establish internal audit schedules and routines.
  - Establish internal audit reporting requirements.
- Implement your internal ISMS audit program.
- Maintain your internal ISMS audit program.

9.3 Review performance of your ISMS at planned intervals

- Establish a management review process.
- Plan your organization's ISMS review process.
- Review the performance of your ISMS.
- Generate management review outputs.
- Retain a record of management review results.

10. Improvement Requirements

10.1 Identify nonconformities and take corrective actions

- Identify nonconformities when they occur.
- React to your organization's nonconformities.
- Evaluate the need to eliminate or control causes.
- Implement corrective actions to address causes.
- Review the effectiveness of your corrective actions.
- Change your organization's ISMS whenever necessary.

10.2 Enhance the overall performance of your ISMS

- Improve the suitability, adequacy, and effectiveness of your ISMS.

This page is a summary only. It does not present our entire product.
If you would like to see the rest of this material, please place an order.
Our products use language that is clear, precise, and easy to understand.

Praxiom Research Group Limited
First Edmonton Place 14 Floor 10665 Jasper Ave
Edmonton, Alberta, Canada, T5J 3S9 780-461-4514
info@praxiom.com info@praxiom.org praxiom@gmail.com
We ship worldwide. Our products are used in over 100 countries.