

2013 ISO 27001 Plain English Outline

Plain English outline of ISO 27001 information security standard

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.

4. Contextual requirements

- 4.1 Understand your organization and its particular context.
- 4.2 Define the needs and expectations of your interested parties.
- 4.3 Figure out what your ISMS should apply to and clarify its scope.
- 4.4 Develop an ISMS that complies with this international standard.

5. Leadership requirements

- 5.1 Provide leadership and show that you support your ISMS.
- 5.2 Establish an appropriate information security policy.
- 5.3 Assign responsibility and authority for your ISMS.

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.
 - 6.1.2 Establish an information security risk assessment process.
 - 6.1.3 Develop an information security risk treatment process.
- 6.2 Set security objectives and develop plans to achieve them.

7. Support requirements

- 7.1 Support your ISMS by providing the necessary resources.
- 7.2 Support your ISMS by making sure that people are competent.
- 7.3 Support your ISMS by making people aware of their responsibilities.
- 7.4 Support your ISMS by identifying your communication needs.
- 7.5 Support your ISMS by managing all relevant information.
 - 7.5.1 Include the information and documents that your ISMS needs.
 - 7.5.2 Manage the creation and modification of your ISMS documents.
 - 7.5.3 Control your organization's ISMS information and documents.

8. Operational requirements

- 8.1 Carry out operational planning and control your processes.
- 8.2 Conduct regular information security risk assessments.
- 8.3 Implement your information security risk treatment plan.

9. Evaluation requirements

- 9.1 Monitor, measure, analyze, and evaluate your information security.
- 9.2 Set up an internal audit program and use it to evaluate your ISMS.
- 9.3 Review performance of your organization's ISMS at planned intervals.

10. Improvement requirements

- 10.1 Identify nonconformities and take corrective actions.
- 10.2 Enhance the overall performance of your ISMS.

If you'd like to see how we've translated each of the above sections into Plain English, please consider [purchasing our detailed product](#).

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.