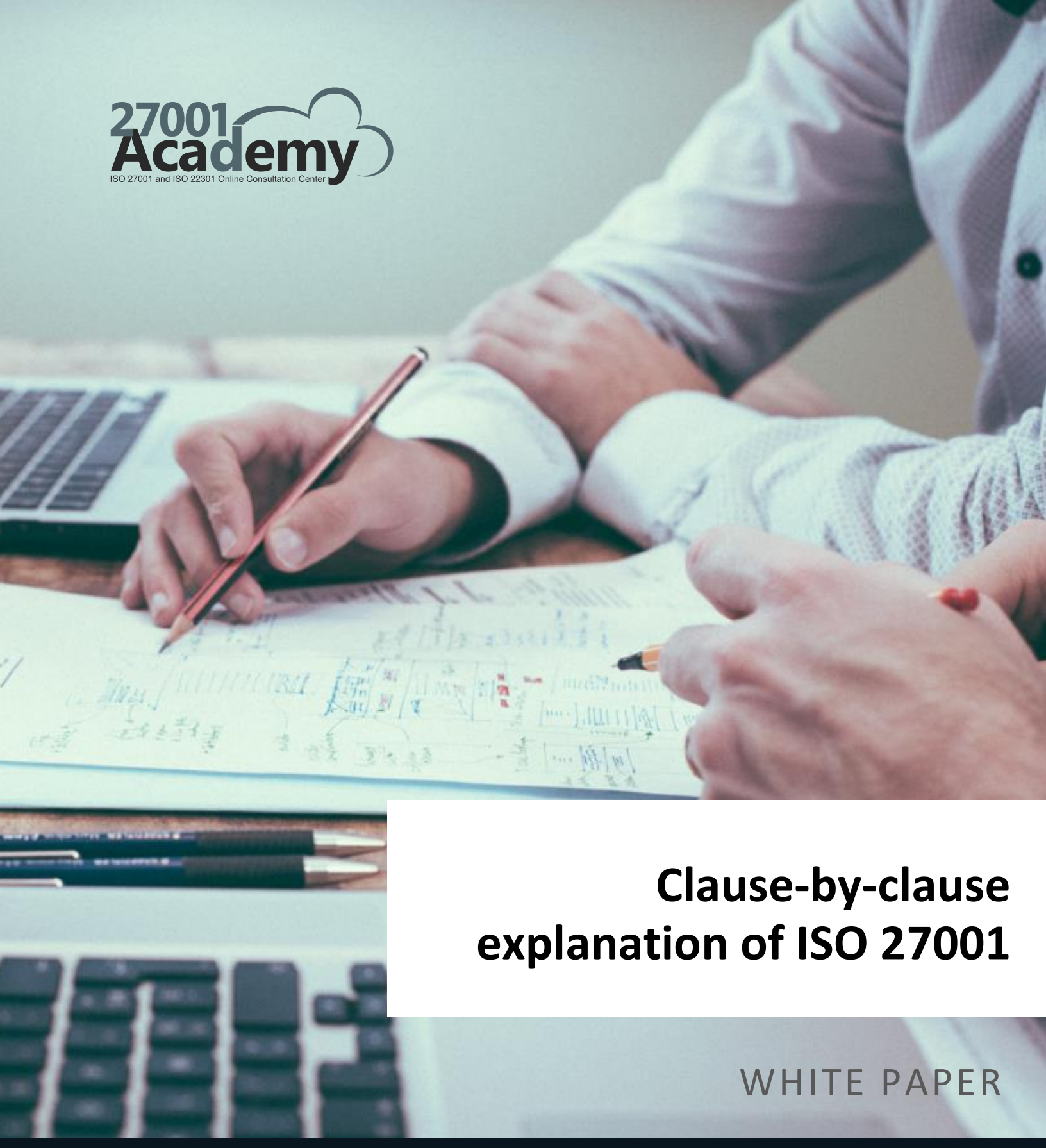
27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center



Clause-by-clause explanation of ISO 27001

WHITE PAPER

Advisera
Making certification simple.

Table of Contents

Executive summary

Addressing information security risks in order to improve an organization's results is a matter of being well prepared. This white paper is designed to assist top management and employees from organizations that have decided to properly protect information by establishing and maintaining an ISO 27001:2013-based Information Security Management System (ISMS).

In this document, you will find an explanation of each clause of ISO 27001, from sections 4 to 10, and the control objectives and security controls from Annex A, to facilitate understanding of the standard. The clauses' presentation is in the same order and number of the clauses as the ISO 27001:2013 standard itself. Furthermore, you'll find links to additional learning materials like articles and other white papers.

Please note: This white paper is not a replacement for ISO 27001 – to get the standard, visit the ISO website: http://www.iso.org

0. Introduction

Information security systems are often regarded by organizations as simple checklists or policies and procedures that deny them a lot of things, far from the way they do their normal business. By sticking to these beliefs, organizations prevent themselves from properly building an ISMS (Information Security Management System) and achieving its full potential, either in operational and financial performance, or marketing reputation.

Fortunately, there are many frameworks on the market that can help organizations to handle this situation, among them being ISO 27001:2013.

Whether standing alone or integrated with another management system, such as ISO 9001 (Quality), ISO 22301 (Information Security), ISO 14001 (Environment), or OHSAS 18001 (Operational Health and Safety), the ISO 27001:2013 standard provides guidance and direction for how an organization, regardless of its size and industry, should manage information security and address information security risks, which can bring many benefits not only to the organization itself, but also to clients, suppliers, and other interested parties.

But, for those unfamiliar with ISO standards or information security concepts, ISO 27001 may be confusing, so we developed this white paper to help you get inside this world.

Sections 1 to 3 will cover the concepts of process, process approach, and PDCA cycle applicable to ISO management standards, as well as the most important definitions a beginner in information security should know.

The main content of this white paper will follow the same order and numbering of the following clauses required to certify an ISMS against ISO 27001:2013:

4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement

Additionally, the white paper also covers the content of Annex A, control objectives and security controls (safeguards), numbered from A.5 to A.18.

Besides all this explanatory information, you will find throughout this white paper references to other learning materials.

1. Process and process approach

1.1 Terms and definitions

Process: a group of repeatable and interrelated activities performed to transform a series of inputs into defined outputs.

Process approach: management of a group of processes together as a system, where the interrelations between processes are identified and the outputs of a previous process are treated as the inputs of the following one. This approach helps ensure the results of each individual process will add business value and contribute to achieve the final desired results.

Information security: processes, methodologies, and technologies with the objective to preserve the confidentiality, integrity, and availability of information.

Confidentiality: property of the information that can be accessed or disclosed only to authorized persons, entities, or processes.

Integrity: property of something that is complete and free of error.

Availability: property of something that is accessible and usable only by an authorized person, entity, or process when demanded.

Information security management: management of processes that cover the identification of situations that may put information at risk, and the implementation of controls to address those risks and protect the interest of the business and other relevant interested parties (e.g., customers, employees, etc.).

Risk: the effect of uncertainty upon desired results.

Risk assessment (RA): a process that helps identify, analyze, and evaluate risks.

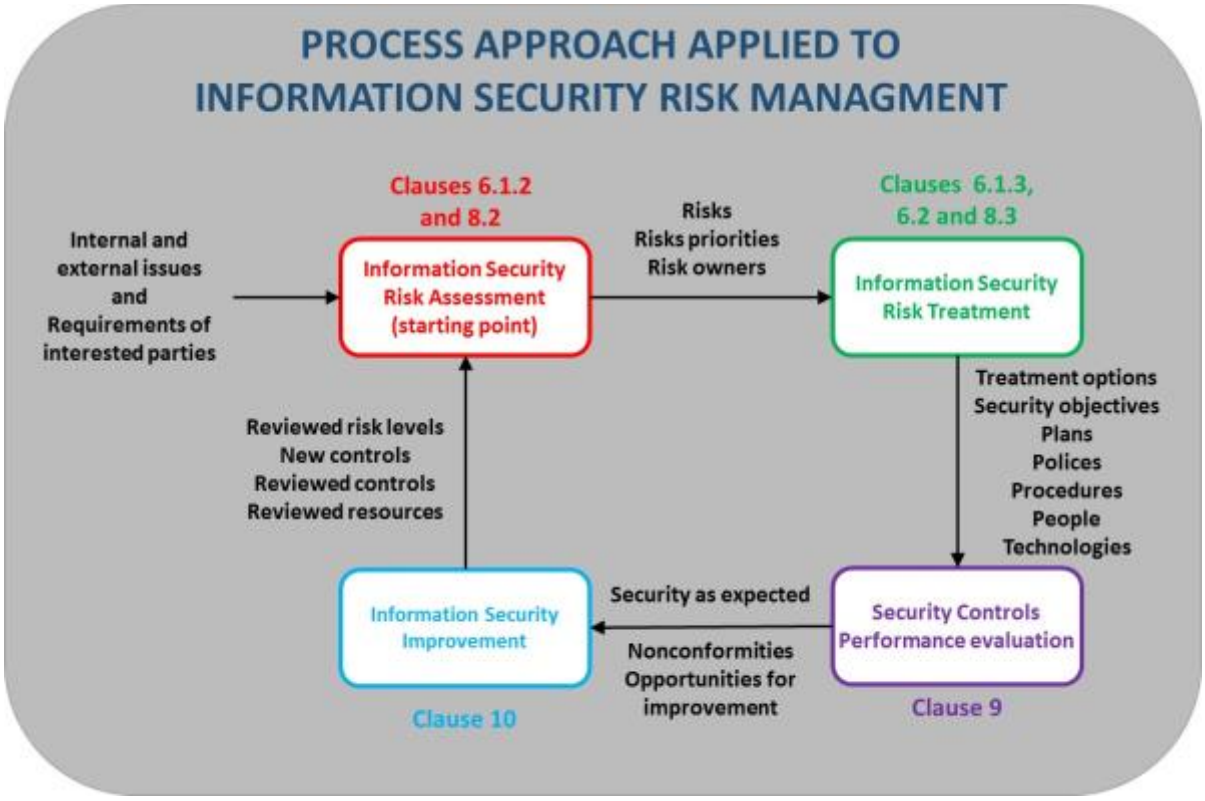
Risk treatment plan: a set of procedures, methodologies, and technologies applied to modify risks.

Residual risk: the value of a risk after risk treatment.

2. Process approach impact

Compliance with the ISO 27001:2013 standard is mandatory for certification, but compliance alone doesn't guarantee the capacity of an organization to protect information. It's necessary to create a robust link between requirements, policies, objectives, performance, and actions. And that's why a process approach, as defined in the previous section, is so useful to implementing an ISMS.

The following diagram presents some examples of inputs, outputs, and activities involved in the risk management process, a cornerstone of an ISO 27001 Information Security Management System, demonstrating how a process approach is a good way to organize and manage information security processes to create value for an organization and other interested parties.



So, by adopting a process approach for information security, an organization can have a better view of how each step contributes to the main objectives of protecting information, allowing it to quickly identify problematic points in performing the process.

3. The Plan-Do-Check-Act cycle

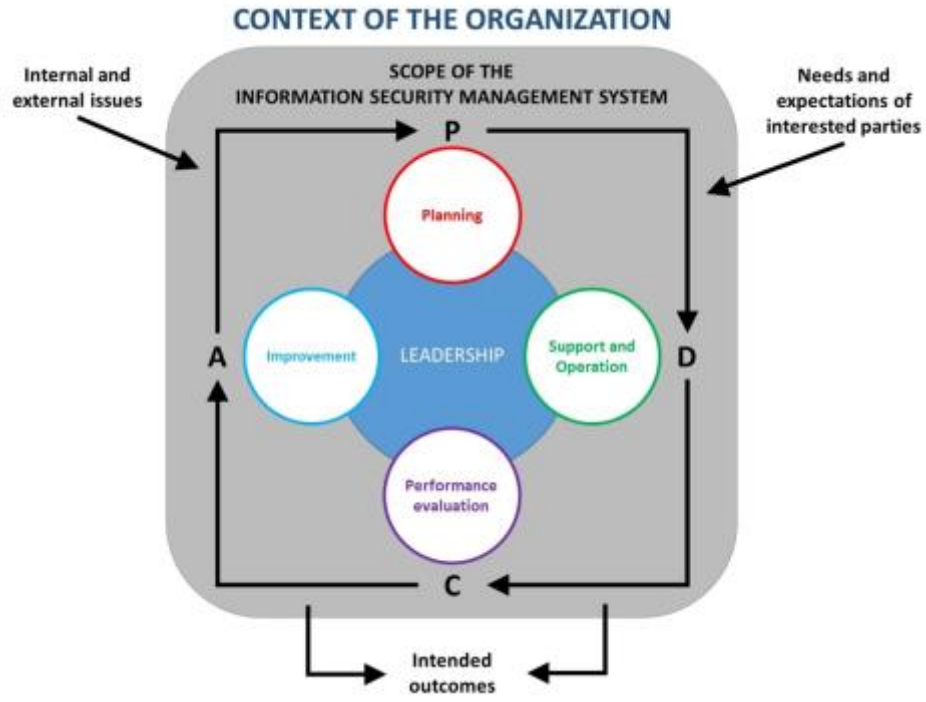
Since any business is a living thing, changing and evolving because of internal and external influences, it is necessary that the Information Security Management System also be capable of adjusting itself (e.g., objectives and procedures) to follow business changes and remain relevant and useful. The ISO 27001:2013 standard ensures this condition is achieved by adopting a "Plan-Do-Check-Act" cycle (PDCA) in its framework, which can be described as follows:

Plan: the definition of policies, objectives, targets, controls, processes, and procedures, as well as performing the risk management, which support the delivery of information security aligned with the organization's core business.

Do: the implementation and operation of the planned processes.

Check: the monitoring, measuring, evaluation, and review of results against the information security policy and objectives, so corrective and/or improvement actions can be determined and authorized.

Act: the performing of authorized actions to ensure the information security delivers its results and can be improved.



It should be noted that the PDCA cycle is a globally recognized management system methodology that is used across various business management systems, but its use is both compulsory and highly beneficial within ISO 27001:2013.

4. Context of the organization

4.1 Understanding the organization and its context

This clause requires the organization to determine all internal and external issues that may be relevant to its business purposes and to the achievement of the objectives of the ISMS itself.

4.2 Understanding the needs and expectations of interested parties

The standard requires the organization to assess who the interest parties are in terms of its ISMS, what their needs and expectations may be, which legal and regulatory requirements, as well as contractual obligations, are applicable, and consequently, if any of these should become compliance obligations.

Tip: For more information on this topic, see the article: How to identify interested parties according to ISO 27001 and ISO 22301.

4.3 Determining the scope of the Information Security Management System

The scope and boundaries and applicability of the ISMS must be examined and defined considering the internal and external issues, interested parties' requirements, as well as the existing interfaces and dependencies between the organization's activities and those performed by other organizations.

The scope must be kept as "documented information."

Tip: For more information on this topic, see the article: How to define the ISMS scope.

4.4 Information Security Management System

The standard indicates that an ISMS should be established and operated and, by using interacting processes, be controlled and continuously improved.

5. Leadership

5.1 Leadership and commitment

Top management and line managers with relevant roles in the organization must demonstrate genuine effort to engage people in the support of the ISMS.

For more information on this topic, please see the article: Roles and responsibilities of top management in ISO 27001 and ISO 22301.

This clause provides many items of top management commitment with enhanced levels of leadership, involvement, and cooperation in the operation of the ISMS, by ensuring aspects like:

- information security policy and objectives' alignment with each other, and with the strategic policies and overall direction of the business;
- information security activities' integration with other business systems where applicable;
- provision for resources so the ISMS can be operated efficiently;
- understanding of the importance of information security management and compliance with ISMS requirements;
- achievement of ISMS objectives;
- definition of information security responsibilities to people within the ISMS, and their correct support, training, and guidance to complete their tasks effectively;
- support of the ISMS during all its life cycle, considering a PCDA approach and continual improvement.

5.2 Policy

Top management has the responsibility to establish an information security policy, which is aligned with the organization's purposes and provides a framework for setting information security objectives, including a commitment to fulfill applicable requirements and the continual improvement of the ISMS. The information security policy must be maintained as documented information, be communicated within the organization, and be available to all interested parties.

For more information on this topic, please see the article: What should you write in your Information Security Policy according to ISO 27001?

5.3 Organizational roles, responsibilities and authorities

The standard states that it is the responsibility of top management to ensure that roles, responsibilities, and authorities are delegated and communicated effectively. The responsibility shall also be assigned to ensure that the ISMS meets the terms of the ISO 27001:2013 standard itself, and that the ISMS performance can be accurately reported to top management.

For more information on this topic, please see the article: What is the job of Chief Information Security Officer (CISO) in ISO 27001?

6. Planning

6.1 Actions to address risks and opportunities

6.1.1 General

This clause seeks to cover the "preventive action" stated in the old ISO 27001:2005. The organization must plan actions to handle risks and opportunities relevant to the context of the organization (section 4.1) and the needs and expectations of interested parties (section 4.2), as a way to ensure that the ISMS can achieve its intended outcomes and results, prevent or mitigate undesired consequences, and continually improve. These actions must consider their integration with ISMS activities, as well as how effectiveness should be evaluated.

For more information on this topic, please see the article: Infographic: New ISO 27001 2013 revision – What has changed?

6.1.2 Information security risk assessment

The organization must define and apply an information security risk assessment process with defined information security risk and acceptance criteria, as well as criteria to perform such assessments, so repeated assessments produce consistent, valid, and comparable results.

The risk assessment process must include risk identification, analyses, and evaluation, and the process must be kept as documented information.

For more information on this topic, please see the article: How to write ISO 27001 risk assessment methodology.

6.1.3 Information security risk treatment

The organization must define and apply an information security risk treatment process to select proper risk treatment options and controls. The selected controls must consider, but not be limited to, controls described in Annex A. The main results of the risk treatment process are the statement of applicability, and the risk treatment plan, which must be approved by the risk owners. The information security risk treatment process must be kept as documented information.

For more information on this topic, please see these articles: ISO 27001 risk assessment & treatment – 6 basic steps, 4 mitigation options in risk treatment according to ISO 27001, and The importance of Statement of Applicability for ISO 27001.

6.1.4 Information security objectives and plans to achieve them

Information security objectives should be established and communicated at appropriate levels and functions, having considered the alignment with the information security policy, the possibility of measurement, and the applicable information security requirements, and results from risk assessment and risk treatment. The objectives must be updated when deemed necessary.

They must be thought of in terms of what needs to be done, when it needs to be done by, what resources are required to achieve them, who is responsible for the objectives, and how results are to be evaluated, to ensure that objectives are being achieved and can be updated when circumstances require.

Again, it is mandatory that documented information is kept outlining the information security objectives.

For more help with information security objectives and how to plan and achieve them, please see the article: ISO 27001 control objectives – Why are they important?

7. Support

7.1 Resources

No mystery here, the standard states that resources required by the ISMS to achieve the stated objectives and show continual improvement must be defined and made available by the organization.

7.2 Competence

The competence of people given responsibility for the ISMS who work under the organization's control must meet the terms of the ISO 27001:2013 standard, to ensure that their performance does not negatively affect the ISMS. Competence can be demonstrated by experience, training, and/or education regarding the assumed tasks. When the competence is not enough, training must be identified and delivered, as well as measured to ensure that the required level of competence was achieved. This is also another aspect of the standard that must be kept as documented information for the ISMS.

For more help with information security training, please see the article: How to perform training & awareness for ISO 27001 and ISO 22301.

7.3 Awareness

Awareness is closely related to competence in the standard. People who work under the organization's control must be made aware of the information security policy and its contents, what their personal performance means to the ISMS and its objectives, and what the implications of nonconformities may be to the ISMS.

7.4 Communication

Internal and external communication deemed relevant to the ISMS must be determined, as well as the processes by which they must be effected, considering what needs to be communicated, by whom, when it should be done, and who needs to receive the communication. See also: How to create a Communication Plan according to ISO 27001.

7.5 Documented information

7.5.1 General

"Documented information," which you will see mentioned several times during this white paper, now covers both the "documents" and "records" concepts seen in the previous revision of the ISO 27001 standard.

This change was designed to facilitate the management of documents and records required by the standard, as well as those viewed as critical by the organization to the ISMS and its operation. It should also be noted that the amount and coverage of documented information that an organization requires will differ, according to its size, activities, products, services, complexity of processes and their interrelations, and people's competence.

To learn more about this topic, please see the article: List of mandatory documents required by ISO 27001 (2013 revision).

7.5.2 Creating and updating

The standard requires that documented information created or updated in the scope of the ISMS must be properly identified and described, also considering its content presentation, and media used. All documented information must go under proper review and approval procedures to ensure they are fit for purpose.

7.5.3 Control of documented information

The standard states that documented information required by the ISMS, and the standard itself, either from internal or external origin, must be available and fit for use where and when needed, and reasonably protected against damage or loss of integrity and identity.

For the proper control of documented information, the organization must consider the provision of processes regarding the distribution, retention, access, usage, retrieval, preservation and storage, control, and disposition.

See also: Document management in ISO 27001 & BS 25999-2 and Records management in ISO 27001 and ISO 22301.

8. Operation

8.1 Operational planning and control

To ensure that risks and opportunities are treated properly (clause 6.1), security objectives are achieved (clause 6.2), and information security requirements are met, an ISMS must plan, implement, and control its processes, as well as identify and control any relevant outsourced processes, and retain documented information deemed as necessary to provide confidence that the process are being performed and achieving their results as planned.

Being focused on keeping the information secure, the ISMS also should consider in its planning and control the monitoring of planned changes, and impact analysis of unexpected changes, to be able to take actions to mitigate adverse effects if necessary.

8.2 Information security risk assessment

The standard requires risk assessments to be performed at planned intervals or according to the criteria defined in clause 6.1.2 a).

The resulting information must be kept as documented information.

For more information on this topic, please see the article: ISO 27001 risk assessment: How to match assets, threats and vulnerabilities.

8.3 Information security risk treatment

The standard requires risk treatment plans to be implemented, retaining the resulting information as documented information.

For more information on this topic, please see the article: Risk Treatment Plan and risk treatment process – What's the difference?

9. Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

The organization not only has to establish and evaluate performance metrics regarding the effectiveness and efficiency of processes, procedures, and functions that protect information, but should also consider metrics for the ISMS performance, regarding compliance with the standard, preventive actions in response to adverse trends, and the degree by which the information security policy, objectives, and goals are being achieved.

The methods established should take into consideration what needs to be monitored and measured, how to ensure the accuracy of results, and at what frequency to perform the monitoring, measurement, analysis, and evaluation of ISMS data and results. It should also be noted that performance results should be properly retained as evidence of compliance and as a source to facilitate subsequent corrective actions.

9.2 Internal audit

Internal audits should be performed at planned intervals, considering the processes' relevance and results of previous audits, to ensure effective implementation and maintenance, as well as compliance with the standard's requirements and any requirements defined by the organization itself. Criteria and scope for each audit must be defined.

Auditors should be independent and have no conflict of interest over the audit subject. Auditors also must report the audit results to relevant management, and ensure that non-conformities are subject to the responsible managers, who in turn must ensure that any corrective measures needed are implemented in a timely manner. Finally, the auditor must also verify the effectiveness of corrective actions taken.

To learn more about this topic, please see the article: How to make an Internal Audit checklist for ISO 27001 / ISO 22301.

9.3 Management review

The management review exists so that the ISMS can be kept continuously suitable, adequate, and effective to support the information security.

It must be performed at planned intervals, in a strategic manner and at the top management level, covering the required aspects all at once or by parts, in a way that is best suitable to business needs.

The status of actions defined in previous reviews, significant internal and external factors that may impact the ISMS, information security performance, and opportunities for improvement should be reviewed by top management, so relevant adjustments and improvement opportunities can be implemented.

The management review is the most relevant function to the continuity of an ISMS, because of the top management's direct involvement, and all details and data from the management review must be documented and recorded to ensure that the ISMS can follow the specific requirements and general strategic direction for the organization detailed there.

Tip: For more details on this topic, please see the article: Why is management review important for ISO 27001 and ISO 22301?

10. Improvement

10.1 Nonconformity and corrective action

Outputs from management reviews, internal audits, and compliance and performance evaluation should all be used to form the basis for nonconformities and corrective actions. Once identified, a nonconformity or corrective action should trigger, if considered relevant, proper and systematic responses to mitigate its consequences and eliminate root causes, by updating processes and procedures, to avoid recurrence.

The effectiveness of actions taken must be evaluated and documented, along with the originally reported information about the nonconformity / corrective action and the results achieved.

For more detail on this subject, please take a look at the article: Practical use of corrective actions for ISO 27001 and ISO 22301.

10.2 Continual improvement

Continual improvement is a key aspect of the ISMS in the effort to achieve and maintain the suitability, adequacy, and effectiveness of the information security as it relates to the organizations' objectives.

For more detail on this subject, please take a look at the article: Achieving continual improvement through the use of maturity models.

Annex A – Reference control objectives and controls

A.5. Information security policies

The controls in this section aim to provide direction and support to the ISMS by the implementation, communication, and controlled review of information security policies.

For more detail on this subject, please take a look at the article: One Information Security Policy, or several policies?

A.6. Organization of information security

The controls in this section aim to provide the basic framework for the implementation and operation of information security by defining its internal organization (e.g., roles, responsibilities, etc.), and through the consideration of organizational aspects of information security, like project management, use of mobile devices, and teleworking.

For more detail on this subject, please take a look at these articles:

- How to document roles and responsibilities according to ISO 27001
- How to write an easy-to-use BYOD policy compliant with ISO 27001
- Special interest groups: A useful resource to support your ISMS
- How to manage security in project management according to ISO 27001 A.6.1.5

A.7. Human resource security

The controls in this section aim to ensure that those people who are under the organization's control and can affect information security are fit for working and know their responsibilities, and that any changes in employment conditions will not affect information security.

For more detail on this subject, please take a look at these articles: What to look for when hiring a security professional, and 8 Security Practices to Use in Your Employee Training and Awareness Program.

A.8. Asset management

The controls in this section aim to ensure information security assets (e.g., information, processing devices, storage devices, etc.) are identified, that responsibilities for their security are designated, and that people know how to handle them according to predefined classification levels.

For more detail on this subject, please take a look at these articles:

- How to handle Asset register (Asset inventory) according to ISO 27001
- Secure equipment and media disposal according to ISO 27001
- Information classification according to ISO 27001
- Risk owners vs. asset owners in ISO 27001:2013

A.9. Access control

The controls in this section aim to limit access to information and information assets considering business needs, by means of formal processes to grant or revoke access rights. The controls consider either physical or logical access, as well as access made by people and by information systems.

For more detail on this subject, please take a look at these articles: How to handle access control according to ISO 27001, and How two-factor authentication enables compliance with ISO 27001 access controls.

A.10. Cryptography

The controls in this section aim to provide the basis for proper use of cryptographic solutions to protect the confidentiality, authenticity, and/or integrity of information.

For more detail on this subject, please take a look at the article: How to use the cryptography according to ISO 27001 control A.10.

A.11. Physical and environmental security

The controls in this section aim to prevent unauthorized access to physical areas, as well as to protect equipment and facilities that if compromised, by human or natural intervention, could affect information assets or business operations.

For more detail on this subject, please take a look at these articles:

- How to implement equipment physical protection according to ISO 27001 A.11.2 – Part 1
- How to implement equipment physical protection according to ISO 27001 A.11.2 – Part 2
- Physical security in ISO 27001: How to protect the secure areas
- How to protect against external and environmental threats according to ISO 27001 A.11.1.4
- Secure equipment and media disposal according to ISO 27001
- Clear desk and clear screen policy – What does ISO 27001 require?

A.12. Operations security

The controls in this section aim to ensure that the operation of information processing facilities, including operating systems, are secure and protected against malware and data loss. Additionally, controls in this section require the means to record events and generate evidence, periodic verification of vulnerabilities, and the establishment of precautions to prevent audit activities from affecting operations.

For more detail on this subject, please take a look at these articles:

- Implementing capacity management according to ISO 27001:2013 control A.12.1.3
- Logging and monitoring according to ISO 27001 A.12.4
- Implementing restrictions on software installation using ISO 27001 control A.12.6.2
- How can ISO 27001 help protect your company against ransomware?
- How to manage changes in an ISMS according to ISO 27001 A.12.1.2
- Backup policy – How to determine backup frequency
- How to manage technical vulnerabilities according to ISO 27001 control A.12.6.1
- How to use penetration testing for ISO 27001 A.12.6.1

A.13. Communications security

The controls in this section aim to protect the network infrastructure and services, as well as the information that travels on them.

For more detail on this subject, please take a look at these articles:

- Requirements to implement network segregation according to ISO 27001 control A.13.1.3
- How to manage network security according to ISO 27001 A.13.1
- How to use firewalls in ISO 27001 and ISO 27002 implementation

A.14. System acquisition, development and maintenance

The controls in this section aim to ensure that information security is considered in the system development life cycle.

For more detail on this subject, please take a look at these articles: How to set security requirements and test systems according to ISO 27001, and What are secure engineering principles in ISO 27001:2013 control A.14.2.5?

A.15. Supplier relationships

The controls in this section aim to ensure that outsourced activities performed by suppliers also consider information security controls, and that they are properly managed by the organization.

For more detail on this subject, please take a look at the article: 6-step process for handling supplier security according to ISO 27001.

A.16. Information security incident management

The controls in this section aim to provide a framework to ensure the proper communication and handling of security events and incidents, so that they can be resolved in a timely manner and consider the preservation of evidence as required, as well as the improvement of processes to avoid recurrence.

For more detail on this subject, please take a look at these articles: How to handle incidents according to ISO 27001 A.16, and Using ITIL to implement ISO 27001 incident management.

A.17. Information security aspects of business continuity management

The controls in this section aim to ensure the continuity of information security management during adverse situations, as well as the availability of information systems.

For more detail on this subject, please take a look at these articles:

- How to use ISO 22301 for the implementation of business continuity in ISO 27001
- How to implement business impact analysis (BIA) according to ISO 22301
- Business continuity plan: How to structure it according to ISO 22301
- How to perform business continuity exercising and testing according to ISO 22301
- Understanding IT disaster recovery according to ISO 27031

A.18. Compliance

The controls in this section aim to provide a framework to prevent legal, statutory, regulatory, and contractual breaches, and to ensure independent confirmation that information security is implemented and is effective according to the defined policies, procedures, and requirements of the ISO 27001 standard.

For more detail on this subject, please take a look at this list of Laws and regulations on information security and business continuity.

Conclusion

ISO 27001:2013 provides organizations with guidance on how to manage information security risks, with the ultimate goal being to preserve the confidentiality, integrity, and availability of information by applying a risk management process and give confidence to interested parties that risks are adequately managed. And, by implementing all the clauses of the standard and truly understanding their impacts, your organization can achieve many other benefits.

Certification and compliance can bring reputational, motivational, and financial benefits to your organization through customers that have greater confidence that you can protect their information at agreed security levels, along with improvements in your supply chain security. All of these elements are closely related to your organization's ability to deliver satisfaction to your customers, and fulfill the expectations and wishes of your stakeholders, while protecting the organization's capacity for doing business in the long run. Bearing all this in mind, can your organization afford not to have ISO 27001:2013?

Sample of documentation templates or toolkits

You can download a free preview of our ISO 27001 Documentation Toolkit, which will allow you to view samples of the documents available to help you to implement ISO 27001:2013 without the assistance and cost of external consultancy.

References

27001 Academy

International Organization for Standardization

27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

Advisera Expert Solutions Ltd
for electronic business and business consulting
Zavizanska 12, 10000 Zagreb
Croatia, European Union

Email: support@advisera.com
Phone: +1 (646) 759 9933
Toll-Free (U.S. and Canada): 1-888-553-2256
Toll-Free (United Kingdom): 0800 808 5485
Fax: +385 1 556 0711

EXPLORE **ADVISERA**

27001 Academy · 9001 Academy · 14001 Academy · 18001 Academy · 20000 Academy

Conformio · eTraining · AdviseraBooks

Advisera
Making certification simple.