D 44v22

ISO 27001 internal audit

Goal of the module: To conduct an internal audit according to ISO 19011 in order to:

- identify improvement opportunities
- increase the satisfaction of interested parties
- evaluate the performance of the ISO 27001 information security management system

1 Scope

The word audit comes from Latin "audire" = to listen.

Audit: *a systematic and independent survey to determine whether activities and results comply with pre-established measures and are capable of achieving the objectives*

Audits are mostly internal or external.

Internal audits, also called first party audits, are a requirement of the ISO 27001 standard (cf. sub-clause 9.2).

External, customer (or supplier) and certification audits, also called second and third party audits, are not within the scope of this module.

Internal audits are the most widespread tool for checking and evaluating the effectiveness of an information security management system (ISMS). It is never intended to find the weak points in personnel. The internal audit has entered many company's daily lives as it has become inseparable from:

- any management system
- internal communication
- daily improvement
- corporate culture

It's only through other people's eyes that one can really see one's weakness. Chinese proverb

An internal audit is of (cf. figure 1-1):

- the information security management system
- a process
- a product (service, project)

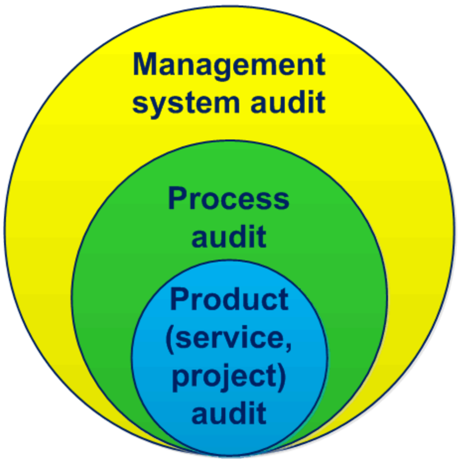


Figure 1-1. Internal audit types

Process: *activities that transform inputs into outputs*

The internal audit results are part of the inputs of the management review and allow the identification of fields in which to improve the information security management system (ISMS) as:

No system is perfect

As shown in figure 1-2, for the process “Perform an audit”, top management (via the management review) is considered as an audit client with needs and expectations, which are themselves related to processes and various requirements.

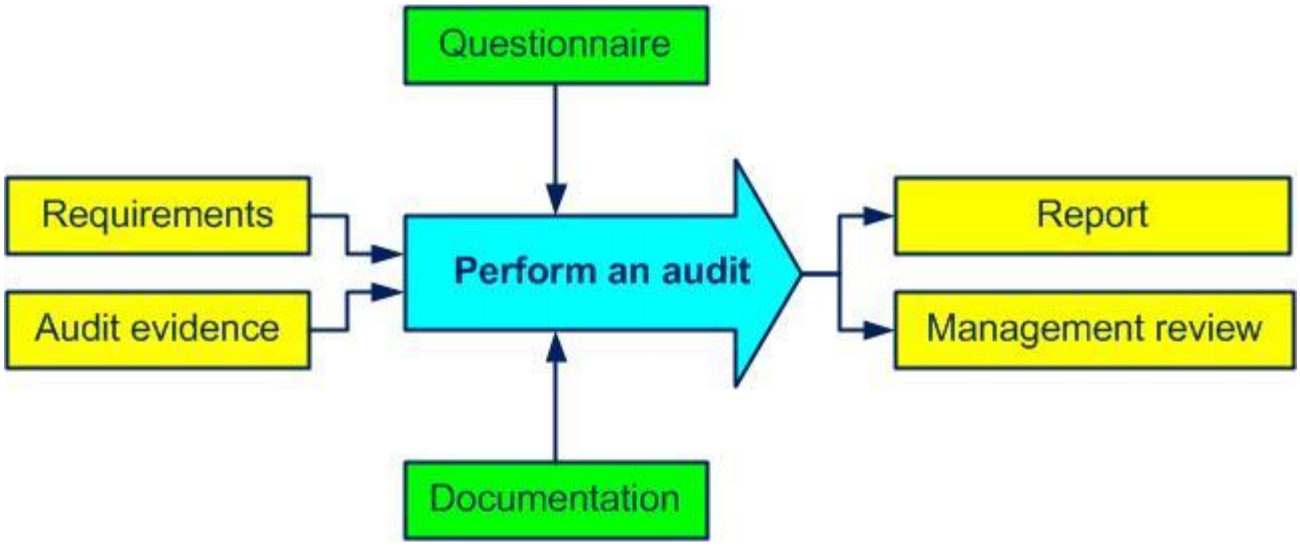


Figure 1-2. Perform an audit process

In the 1980s internal audits were mostly documentary - did you write down what you do?

Later, in the early 2000s, internal audits were more about conformity - does what you do meet the requirements of the standard?

Now internal audits are essentially about effectiveness - how do you improve your performance?

2 Normative references

The advice given by the ISO 19011 document can be summarized in the following fields:

- audit principles - clause 4
- audit program - clause 5
- audit activities - clause 6
- auditor competence - clause 7

A good knowledge of the ISO 27001 standard is required to understand and follow this module.

This module is based on the following generic and international standards:

- **ISO 19011 (2018): Guidelines for auditing management systems**
- **ISO 27000 (2018): Information technology – Security techniques – Information security management systems – Overview and vocabulary**
- **ISO 27001 (2022): Information security, cybersecurity and privacy protection – Information security management system – Requirements**

All of these standards and many more can be ordered in electronic or paper format on the ISO site.

More than 28,000 standards (in English and other languages) are available on the Public.Resource.Org site.

3 Definitions

The beginning of wisdom is the definition of terms. Socrates

Some terms and definitions currently used in management systems and audits:

Accident: *undesired event causing death or health*
Asset: *any element of value for the organization*
Audit client: *everyone requesting an audit*
Audit conclusions: *outcome of an audit*
Audit criteria: *everything against which audit evidence is compared*
Audit findings: *every deviation from audit criteria*
Auditee: *everyone who is audited*
Auditor: *everyone who is trained to conduct audits*
Competence: *personal skills, knowledge and experiences*
Conformity: *fulfillment of a specified requirement*
Continual improvement: *permanent process allowing the improvement of the global performance of the organization*
Control: *ensure compliance with the specified criteria*
Corrective action: *action to eliminate the causes of nonconformity or any other undesirable event and to prevent their recurrence*
Customer: *anyone who receives a product*
Document (documented information): *any support allowing the treatment of information*
Deviation: *failure to meet a given threshold*
Hazard: *situation that could lead to a potential incident*
Incident (information security): *unwanted ad unexpected event that can compromise information security*
Information security: *controls to protect the confidentiality, integrity and availability of information*
Interested party: *person, group or company affected by the impacts from an organization*
ISMS: *Information security management system*
Nonconformity: *non-fulfillment of a specified requirement*
Organization: *a structure that satisfies a need*
Product (or service): *every result of a process or activity*
Quality: *aptitude to fulfill requirements*
Quality objective: *quality related, measurable goal that must be achieved*
Problem: *the distance that has to be overcome between real and desired situation*
Procedure: *set of actions to carry out a process*
Record: *document providing objective evidence of achieved results*
Requirement: *explicit or implicit need or expectation*
Review: *survey of a file, product, process so as to verify if pre-set objectives are achieved*
Risk: *likelihood of occurrence of a threat or an opportunity*
Stakeholder: *person, group or company that can affect or be affected by an organization*
Statement of Applicability (SoA): *document describing the objectives and security controls*
Supplier (external provider): *an entity that provides a product*
Top management: *group or persons in charge of the organizational control at the highest level*
Work environment: *set of human and physical factors in which work is carried out*

Examples of interested parties: investors, customers, suppliers, employees and social, public or political organizations

In the terminology of information security management systems, do not confuse the following:

- anomaly, defect, dysfunction, failure, nonconformity, reject and waste:
    - an anomaly is a deviation from what is expected
    - a defect is the non-fulfillment of a requirement related to an intended use
    - a dysfunction is a degraded function that can lead to a failure
    - a failure is when a function has become unfit
    - a nonconformity is the non-fulfillment of a requirement in production
    - a reject is a nonconforming product that will be destroyed
    - a waste is when there are added costs but not value
- audit and inspect
    - to audit is to improve the ISMS
    - to inspect is to verify the conformity of a process or product
- audit, auditee and auditor
    - an audit is a process of evaluating and improving the ISMS
    - an auditee is the one who is audited
    - an auditor is the one who conducts the audit
- audit program and plan
    - an audit program is the annual planning of the audits
    - an audit plan is the description of the audit activities
- communicate and inform
    - to communicate is to pass on a message, listen to the reaction and discuss
    - to inform is to give someone meaningful data
- control and optimization
    - control is meeting the objectives
    - optimization is the search for the best possible results
- customer, supplier and subcontractor
    - a customer receives a product
    - a supplier provides a product
    - a subcontractor provides a service or a product on which a specific work is done
- effectiveness and efficiency
    - effectiveness is the level of achievement of planned results
    - efficiency is the ratio between results and resources
- follow-up and review
    - follow-up is the verification of the obtained results of an action
    - review is the analysis of the effectiveness in achieving objectives
- indicator and objective
    - an indicator is the information on the difference between the achieved result and the pre-set objective
    - an objective is a sought after commitment
- organization and enterprise, society, company
    - organization is the term used in the standard ISO 27001 as the entity between the supplier and the customer
    - an enterprise, society and company are examples of organizations
- organizational chart and process map
    - the organizational chart is the graphic display of departments and their links
    - the process map is the graphic display of processes and their interaction
- process, procedure, product, activity and task
    - a process is how we satisfy the customer using people to achieve the objectives
    - a procedure is the description of how we should conform to the rules
    - a product is the result of a process
    - an activity is a set of tasks
    - a task is a sequence of simple operations

Remark 1: each time you use the term "improvement opportunity" instead of nonconformity, malfunction or failure, the auditee will gain a little more confidence in you.

Remark 2: the use of ISO 19011 and ISO 27000 definitions is recommended. The most important thing is to determine a common and unequivocal vocabulary for everyone in the company.

Remark 3: the customer can also be the user, the beneficiary, the initiator, the client, the prime contractor, the consumer.

Remark 4: ISO 19011 version 2018 uses the terms procedure (📄), record (🗋) and documented information together. We also use the terms procedure and record together with the term documented information.

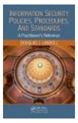
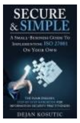
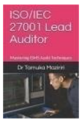
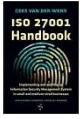
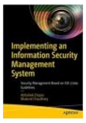
For other definitions, comments, explanations and interpretations that you won't find in this module and annex 06, you can consult:

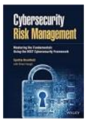
- Online Browsing Platform, ISO
- Electropedia, IEC

When I think of all the books still left for me to read, I am certain of further happiness. Jules Renard

Books for further reading on internal audits:

- Denis Provonost, Internal Quality Auditing, ASQ Quality Press, 2000
- J. P. Russel, The Internal Auditing Pocket Guide, ASQ Quality Press, 2002
- Dennis Arter and al, How to Audit the Process Based QMS, Quality Press, 2003
- Spencer Pickett, The Essential Handbook of Internal Auditing, John Wiley & Sons, 2005
- Karen Welch, The Process Approach Audit Checklist for Manufacturing, ASQ Quality Press, 2005
- Paul Palmes, Process Driven Comprehensive Auditing, ASQ Quality Press, 2009
- David Hoyle, John Thompson, ISO 9000 Auditor Questions, Transition Support, 2009

- J. P. Russel, The Process Auditing and Techniques Guide, ASQ Quality Press, 2010
- Janet Smith, Auditing Beyond Compliance, ASQ Quality Press, 2012
- Edward Humphreys, Implementing the ISO/IEC 27001 2013 ISMS Standard, Artech House, 2016
-  Douglas Landoll, Information security policies, procedures, and standards, Auerbach Publications, 2016
-  Dejan Kosutic, Secure & simple, A small-business guide to implementing iso 27001 on your own, Advisera Expert Solutions, 2016
- Dejan Kosutic, ISO 27001 Risk management in plain english, step-by-step handbook for information security practitioners in small businesses, Advisera Expert Solutions, 2016
- Dejan Kosutic, ISO 27001 annex A controls in plain english, Step-by-step handbook for information security practitioners in small businesses, Advisera Expert Solutions, 2016
- Raphaël Hertzog et al, Kali Linux Revealed: Mastering the Penetration Testing Distribution, OFFSEC Press, 2017
- Bridget Kenyon, Iso 27001 Controls: A Guide to Implementing and Auditing, IT Governance Publishing, 2019
-  Tamuka Maziriri, ISO/IEC 27001 Lead Auditor: Mastering ISMS Audit Techniques, Independently Published, 2019
-  Cees van der Wens, ISO 27001 handbook: Implementing and auditing an 'Information Security Management System' in small and medium-sized businesses, Brave New Books, 2020
-  Abhishek Chopra, Mukund Chaudary, Implementing an Information Security Management System, Apress, 2020

-  Cynthia Brumfield , Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework, Wiley, 2021
- Cesare Gallotti, Information security - 2022 Edition. Risk management. Management systems. The ISO/IEC 27001:2022 standard. The ISO/IEC 27002:2022 controls, Youcanprint, 2022
- Dr David Brewer, ISO/IEC 27001:2022 – Mastering Risk Assessment and the Statement of Applicability, Independently published, 2022

4 Principles

4.1 Management principles

The seven quality management principles (cf. figure 4-1) will help us achieve sustained success (ISO 9001, sub-clause 0.2).

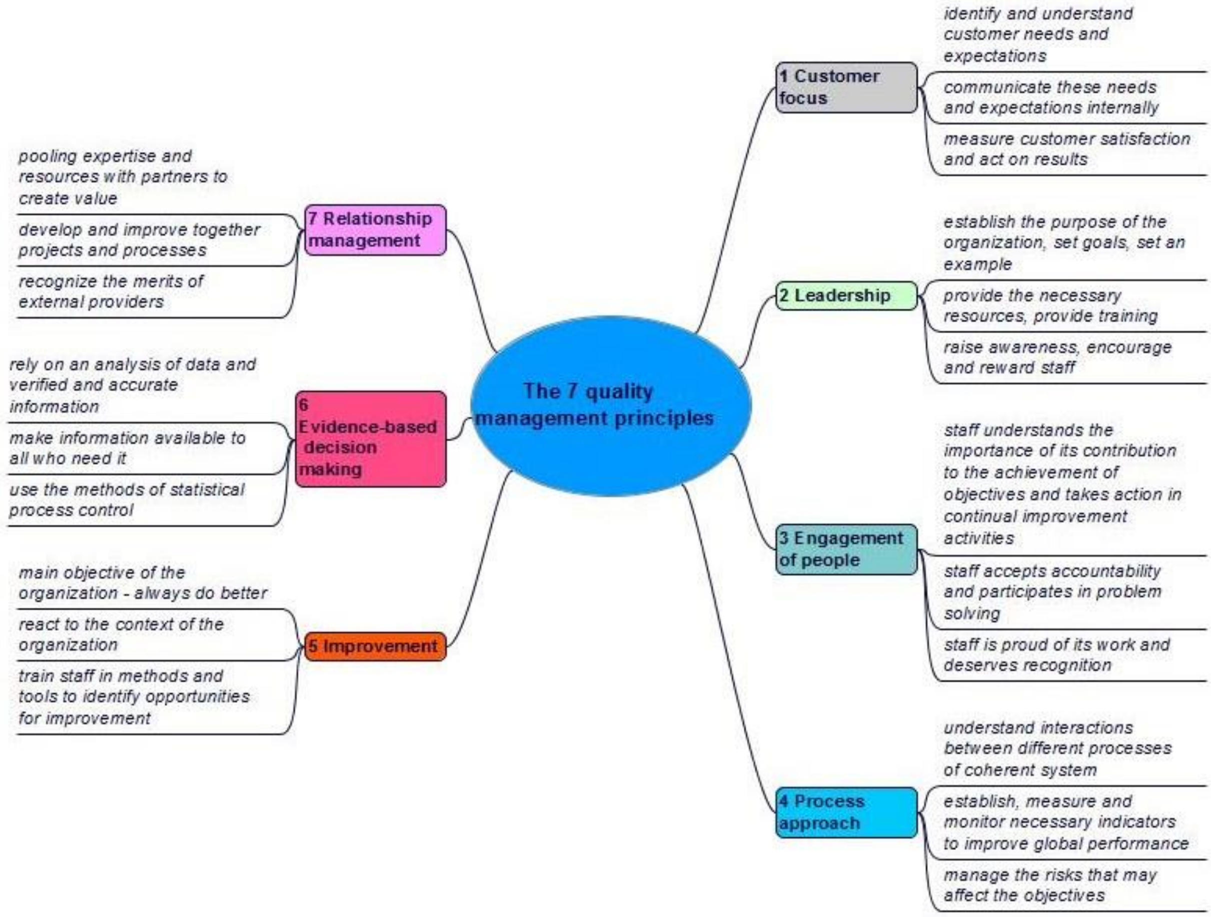

The 7 quality management principles
1 Customer focus
identify and understand customer needs and expectations
communicate these needs and expectations internally
measure customer satisfaction and act on results
2 Leadership
establish the purpose of the organization, set goals, set an example
provide the necessary resources, provide training
raise awareness, encourage and reward staff
3 Engagement of people
staff understands the importance of its contribution to the achievement of objectives and takes action in continual improvement activities
staff accepts accountability and participates in problem solving
staff is proud of its work and deserves recognition
4 Process approach
understand interactions between different processes of coherent system
establish, measure and monitor necessary indicators to improve global performance
manage the risks that may affect the objectives
5 Improvement
main objective of the organization - always do better
react to the context of the organization
train staff in methods and tools to identify opportunities for improvement
6 Evidence-based decision making
rely on an analysis of data and verified and accurate information
make information available to all who need it
use the methods of statistical process control
7 Relationship management
pooling expertise and resources with partners to create value
develop and improve together projects and processes
recognize the merits of external providers

Figure 4-1. The 7 quality management principles

4.2 Audit principles

Certain principles must be followed for an audit to be a value added tool.

For the auditor:

- professional ethics, to guarantee:
  - mutual trust
  - compliance with legal requirements
- impartial presentation, to ensure:
  - honest and precise audit conclusions
  - detailed findings and audit reports
- professional integrity, to guarantee:
  - the importance of the task
  - the trust given
- confidentiality, to treat with care information which is:
  - sensitive
  - confidential

- independence, to:
    - conduct an impartial audit
    - write objective conclusions
- the evidence-based approach, to reach conclusions that are:
    - reliable, verifiable and
    - reproducible
- risk-based thinking, to achieve the objectives of the audit by:
    - identifying and decreasing threats
    - seizing opportunities

But also:

- common sense - always the best tool
- curiosity, to learn and succeed
- goodwill to help the auditee identify improvement opportunities
- understandable language
- positive attitude is gratifying for the auditee

For the audit:

- independence (the auditor and audited activity do not have conflicts of interest), to guarantee:
    - objective conclusions
    - findings based on objective evidence
- a factual approach, to ensure:
    - the audit evidence is verifiable
    - the audit conclusions are repeatable

For the auditee:

- remain available
- do not try to hide the truth
- do not be afraid of the answers
- objectively accept the nonconformities found
- be aware of participating in the improvement of the ISMS by being:
    - benevolent and
    - cooperative

An auditor cannot audit their own department as:

No-one should be a judge in his own case. Latin proverb

Minute of relaxation. Cf. joke "The engineer and the shepherd"

4.3 Performance of the ISMS

For an information security management system what is of interest is the degree of achievement of objectives or, in other words, performance. The performance of an ISMS is measured by its effectiveness and, above all, by its efficiency (see figure 4-2).

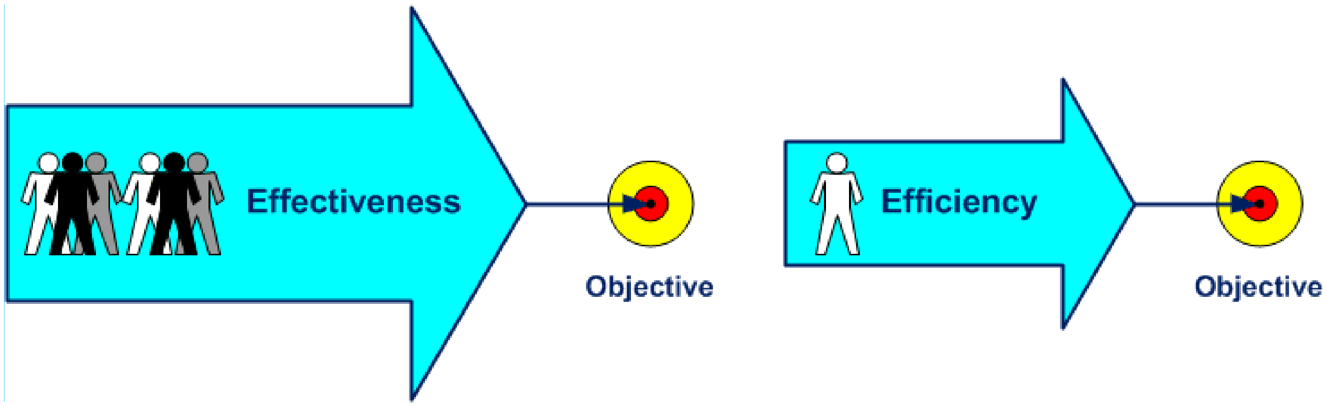


Figure 4-2. Performance of an ISMS

Effectiveness: *capacity to perform planned activities with minimum effort*
Efficiency: *financial relationship between achieved results and resources used*

⚠ N.B. We can be effective because we achieved our objective, but are not efficient if we used too many resources or tolerated and produced too much waste!