SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Antonio **Belli**

M11 Audit techniques and approach examples

Contents

M11.1 Audit techniques and approach examples

- Management Systems audit. Definitions.
- ISO 17021 and 19011
- Use case

Definitions

AUDIT AND CERTIFICATION

audit
systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

management system
set of interrelated or interacting elements of an organization to establish policies and objectives, and processes to achieve those objectives

[SOURCE:ISO 9000:2015]

Definitions

AUDIT AND CERTIFICATION

combined audit
audit carried out together at a single auditee on two or more management systems

joint audit
audit carried out at a single auditee by two or more auditing organizations

audit programme
arrangements for a set of one or more audits planned for a specific time frame and directed towards a specific purpose

[SOURCE:ISO 9000:2015]

Definitions

AUDIT AND CERTIFICATION

audit client
organization or person *requesting* an audit

audit team
one or more persons conducting an audit, supported if needed by technical experts

auditor
person who *conducts* an audit

[SOURCE:ISO 9000:2015]

Definitions

AUDIT AND CERTIFICATION

performance
measurable result

process
set of interrelated or interacting activities that use inputs to deliver an intended result

effectiveness
extent to which planned activities are *realized* and planned results achieved

[SOURCE:ISO 9000:2015]

Process and definitions

audit criteria
set of requirements used as a reference against which objective evidence is compared

objective evidence
data supporting the existence or verity of something

audit evidence
records, statements of fact or other information, which are relevant to the audit criteria and verifiable

AUDIT AND CERTIFICATION

audit scope
extent and boundaries of an audit

audit plan
description of the activities and arrangements for an audit

audit findings
results of the evaluation of the collected audit evidence against audit criteria

audit conclusion
outcome of an audit, after consideration of the audit objectives and all audit findings

[Definitions are taken from ISO 9000:2015]

Audit report

nonconformity
non-fulfilment of a requirement
If **major**, no certification is possible.
If **minor**…

…Certification is still possible, but nonconformity will have to be dealt with by the following year

conformity
fulfilment of a requirement

Certification

Purpose of a certification

ENSURE SECURE INFORMATION ON AN ORGANIZATION

The auditor ("evaluator") is the professional who collects this information.

- Please remember that certification can also be a mandatory requirement in certain circumstances (e.g. calls for tender).

Audit can be:

- *first party*: internal, auditors and audited are in the same organization)

- *second party*: carried out by an interested external party (e.g. a Customer)

- *third party*: carried out by an independent body (e.g. a Certification Body)

Certification and ISO Standards

FOR AN MANAGEMENT SYSTEMS

ISO 17021
Accreditation standard

It is addressed to the Certification Body

Contains information on third party audits

The first part deals with the general requirements for all system certifications

A series of subsequent parts supplement the text with specific requirements for the individual Management Systems

ISO 19011
Guideline for management system audits

It is aimed at **anyone who carries out audits**

Focused on first and second party audits

Provides **guidance** on managing an *audit program*, *planning* and *conducting* audits of management systems, as well as the competence and evaluation of an auditor and audit team.

Purpose of a certification

ENSURE SECURE INFORMATION ON AN ORGANIZATION

An audit can be conducted against a range of audit criteria, separately or in combination, including but not limited to:

— requirements defined in one or more management system standards;
— policies and requirements specified by relevant interested parties;
— statutory and regulatory requirements;
— one or more management system processes defined by the organization or other parties;
— management system plan(s) relating to the provision of specific outputs of a management system (e.g. quality plan, project plan).

[Source: ISO 19011:2018]

Purpose of a certification

ENSURE SECURE INFORMATION ON AN ORGANIZATION

The certification audit consists of two phases

Audit stage 1

Audit stage 2

The pre-audit is optional, but adds value:

1 - Preparation of documentation and implementation audit

2 - Helps the organization familiarize itself with the audit approach of certification

3 - Address all regulatory requirements

4 - Optional, at the request of the organization

Purpose of a certification

ENSURE SECURE INFORMATION ON AN ORGANIZATION

Stage 1 – '*Preparation Audit*'

- It is recommended to do it in the **field**
- **Documentation** review
- Evaluation of the **structure** and specific conditions of the site
- Review of key **performance** parameters
- Validation of the **scope**

Purpose of a certification

ENSURE SECURE INFORMATION ON AN ORGANIZATION

Stage 1 – '*Preparation Audit*'

- Collection of information on **mandatory** (legal and regulatory) requirements and their compliance
- Reviewing the availability of **resources** for phase 2 audit, agreeing with the client and planning phase 2
- Assessment of **overall** preparation for the phase 2 audit
- Report the **findings**, including critical aspects, to the customer / audited entity.

Purpose of a certification

ENSURE SECURE INFORMATION ON AN ORGANIZATION

Stage 2 – '*Implementation audit*'

The purpose is to evaluate the **implementation** and **effectiveness** of the system

- It must be conducted on place

Purpose of a certification

ENSURE SECURE INFORMATION ON AN ORGANIZATION

Stage 2 – '*Implementation audit*'

- **Compliance** with all audit criteria requirements
- Performance versus **goals**
- Performance against **legal** requirements
- **Operational** control of the audited processes
- Results, actions and effectiveness in the field of **internal audits** and the **management review**
- Management's responsibility towards its own **policies**

Purpose of a certification

ENSURE SECURE INFORMATION ON AN ORGANIZATION

Stage 2 – '*Implementation audit*'

- Interrelationship between **mandatory** requirements, quality policy, objectives and performance targets

- Evaluate the *effectiveness* of the system with regard to:
  - Achieve *goals* and *objectives*
  - Implement policy *commitments* (e.g. compliance, achievement of requirements, continuous improvement, etc.)
  -*Operational* controls in all areas of the system
  -*Corrective* actions

- Evaluate the organization's **implementation** and overall **effectiveness** of the Management System

Purpose of a certification

ENSURE SECURE INFORMATION ON AN ORGANIZATION

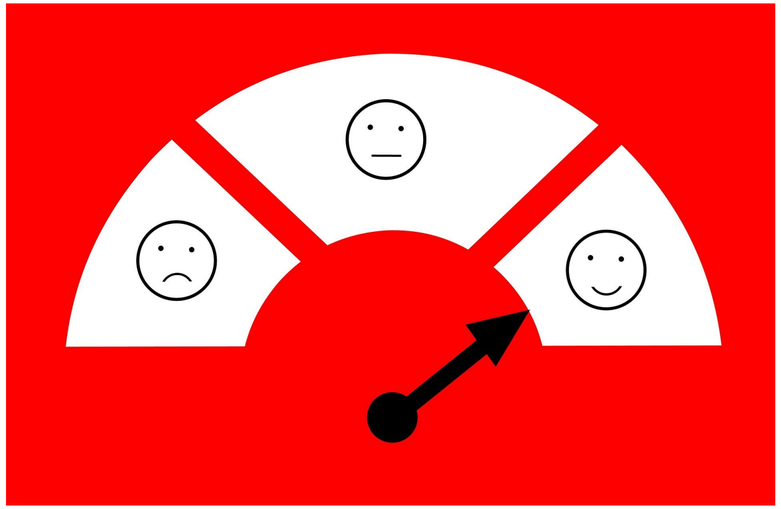
STAGE 2 - Complete system audit

The complete Management System audit covers:

- EVERY requirement: intent, implementation and effectiveness.
- Interrelationships between the elements of the MS (Management System).

3 Key questions:

1. Is the system **adequate**?
2. 2. Is the system **suitable**?
3. 3. Is the system **effective**?



Purpose of a certification

ENSURE SECURE INFORMATION ON AN ORGANIZATION

Audit **conclusion** is

Based on the results of STAGE 1 and STAGE 2

Decision to issue the certificate based on the findings of the Audit Team

Certification, surveillance and recertification

FOR AN ISMS

Surveillance audit

► Conducted in the field at least every year (sometimes every semester)

They cover all processes / functions over a three year period following certification / renewal

►The audit program is based on the results of *previous* audits and on the importance and status of the processes

► They can take into account internal audits

► Evaluate the organization's continued compliance with the requirements of the certification standard

Certification, surveillance and recertification

FOR AN ISMS

Audit plan

FOR MANAGEMENT SYSTEMS

6 phases of the audit (ISO 19011):

- **Initiating** audit
- Preparing audit **activities**
- **Conducting** audit activities
- Preparing and distributing audit **report**
- **Completing** audit
- Conducting audit **follow-up**

Audit plan

FOR MANAGEMENT SYSTEMS

Remember (from 1st lesson)

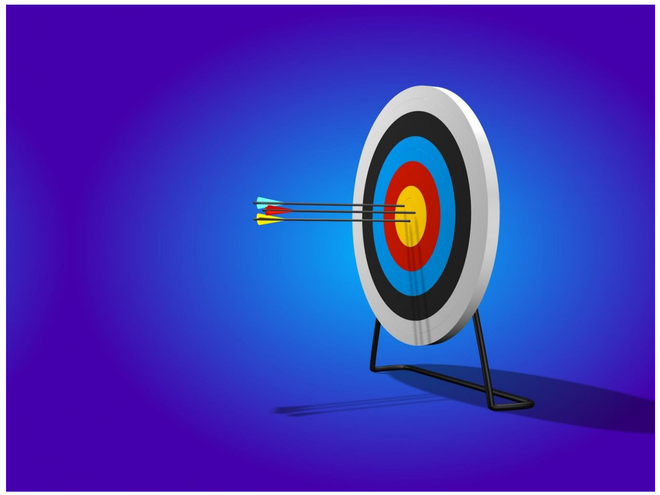
That management systems (such as ISMS or Quality MS) are based on the Hihg level structure, which is founded on the Deming Cycle «**Plan Do Check Act**».

Audit plan

FOR MANAGEMENT SYSTEMS

Conducting a single audit includes:

- Targets;
- Criteria;
- extension (including processes and / or functions);
- dates and sites;
- start and end times of activities;
- roles and responsibilities of auditors and accompanying persons.



Audit initiation and preparation

FOR MANAGEMENT SYSTEMS

► Establish communication channels and prepare the audit client to cooperate in all the aspects of its competence

► Review of *relevant* documented information relating to the management system of the audited organization

► Documented information should include, but are not limited to: management system documents and records, as well as previous audit reports. The review should consider the context of the audited organization, including size, type and complexity, as well as related risks and opportunities. The review should also consider the scope, criteria and objectives of the audit.

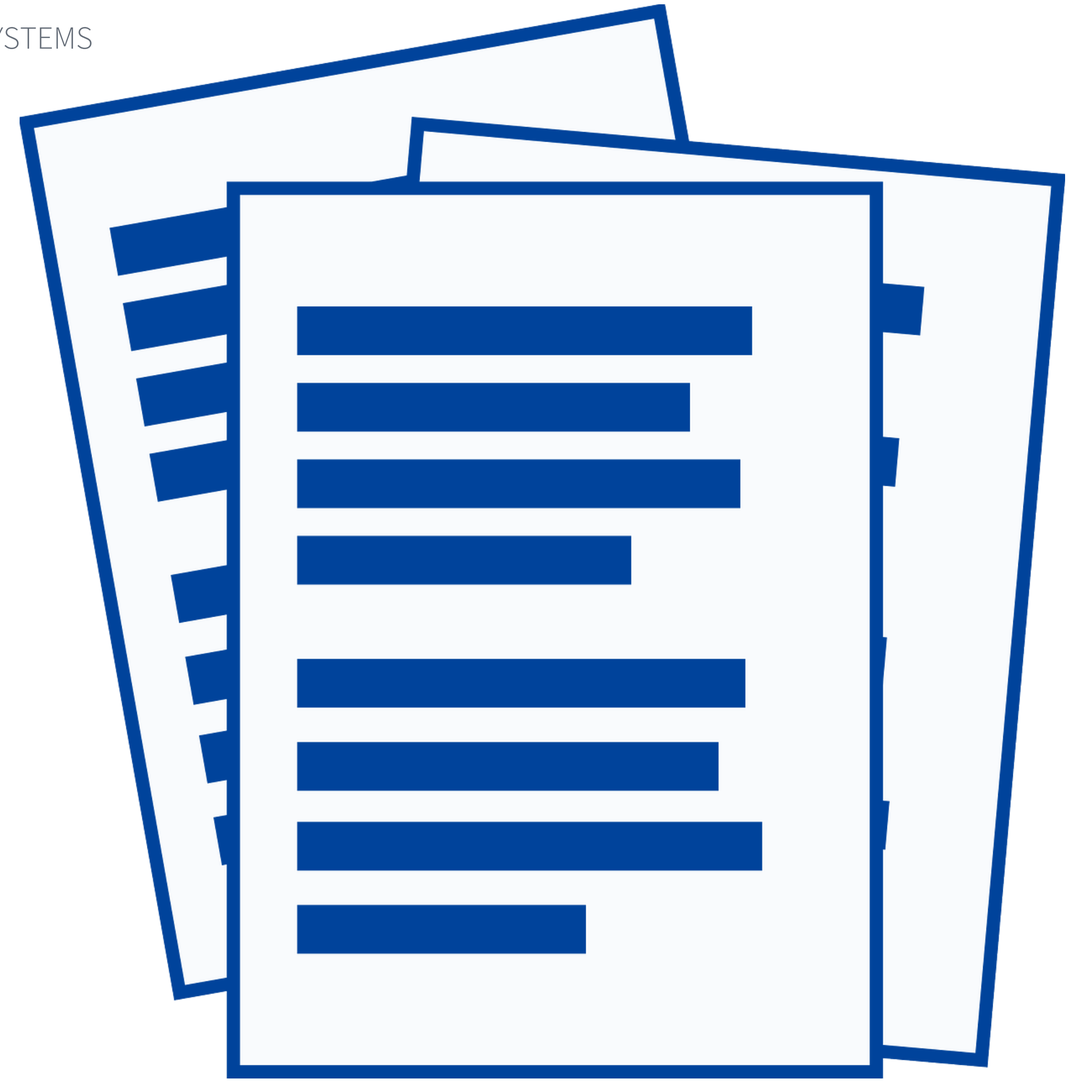
► The review is generally conducted personally by the Lead Auditor

Audit preparation

FOR MANAGEMENT SYSTEMS

Phase 1 - Documentary evidence

- Normally it is performed in the field
- Validation of the scope of the management system
- Gathering information on the legal framework
- Examination of documents
- Evaluation of the structure and specific conditions
- Review of *indicators* and *parameters*
- Establish general preparation for phase 2
- Define the plan for phase 2
- Report the findings, including areas for improvement



Preparing audit activities

FOR MANAGEMENT SYSTEMS

- *Audit plan*

  - Field of application
  - CriteriaDates and & duration
  - Group of auditors
  - Detailed timetable
  - Planning matrix
  - Auditor requests
  - (Remember to cover shifts)

- *Working documents*

  - Checklist
  - Standard
  - Guidelines

Preparing audit activities

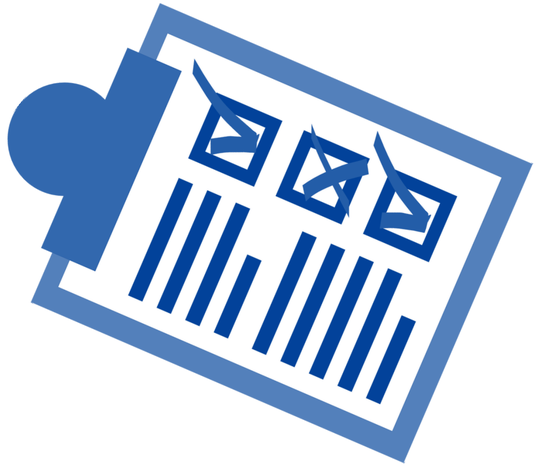
FOR MANAGEMENT SYSTEMS

Audit on the whole system

A full system audit covers:

- *<u>EVERY</u> point of the reference standard*
- *Links between elements of the system.*

1. is the system **adequate**?
2. does the system **work**?
3. Is the system **effective**?



Preparing audit activities

FOR MANAGEMENT SYSTEMS

The opening meeting is important for introducing the audit team, discussing the objectives, scope and criteria of the audit, confirming the plan and methods, sampling for evidence acquisition and other important details for the execution of the audit.

Intermediate meetings will also be planned. with the management system contact person and other managers to review the findings, discuss non-conformities, manage the proposals for corrective actions and corrections.

Preparing audit activities

FOR MANAGEMENT SYSTEMS

The auditor finds evidence by checking **documents**, looking at **records**, interviewing people at all levels, and observing practices and the physical environment.

✓ production / service lines, activities, controls, inspections, audits, monitoring management of non-compliant products / services maintenance systems

✓ product segregation

✓ conditions of the warehouses

✓ handling, identification, packaging

✓ data entry activity

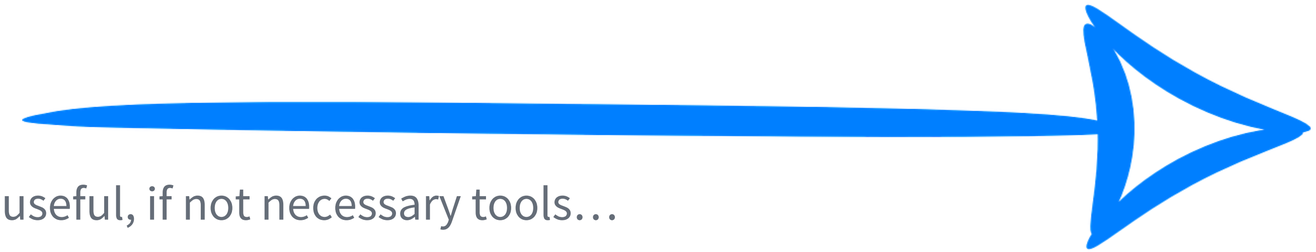
- Talk to the people on the field, if you can hear and understand them
- Ask what the dials and hands indicate about monitoring and measuring processes
- look at the processes in place at the moment, check what is happening and check the documented description of events and processes

Auditing a process

FOR MANAGEMENT SYSTEMS

How to proceed

1. process
2. input
3. output
4. resources
5. who is involved (competence, ability, training)
6. how (methods, procedures and techniques)
7. effectiveness (measurable goals)



Checklists (physical or digital) are useful, if not necessary tools…

[Source: ISO 19011]

Auditing a process

FOR MANAGEMENT SYSTEMS

How to proceed

- Leave space for your **notes**
- The Checklist must become an audit **diary**
- Reference to the audit **criteria**
- Reference to system **documents** (procedures)
- Reference to documents checked (records)

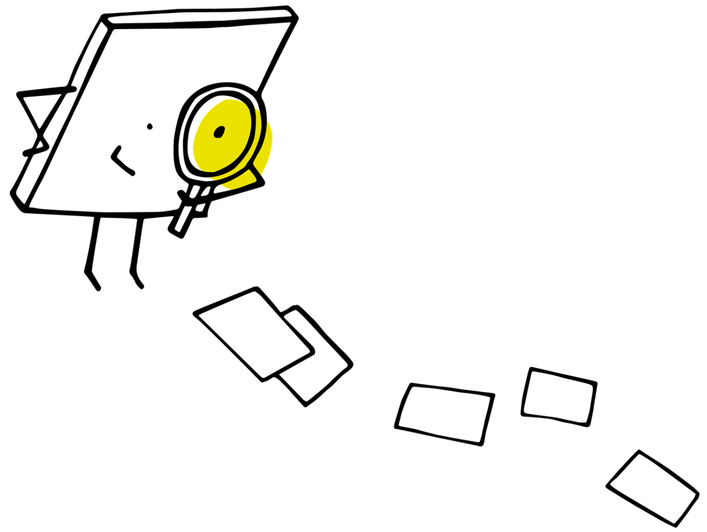
[Source: ISO 19011]

Sampling

FOR MANAGEMENT SYSTEMS

How to proceed

- An auditor always or almost always works on a sample basis
- Judgment-based sampling
- Statistical Sampling
- Consider the time since the last audit
- Consider the extension of the scope



[Source: ISO 19011]

Nonconformities

FOR MANAGEMENT SYSTEMS

What are nonconformities

Product nonconformities

- emerge during the daily work
- they are usually identified by the operators
- they are physiological in processes
- must be correct
- must be registered
- records must be analyzed
- possibly they must be improved with corrective actions

System nonconformities

- emerge during audits or other external controls
- they are identified by external bodies and not during normal control operations
- they are pathological in the processes
- the immediate effect must be corrected
- the causes must be analyzed

Nonconformities

FOR MANAGEMENT SYSTEMS

What are nonconformities

- non-conformities are not to be intended in a negative way
- a discovered nonconformity is a previously hidden opportunity for improvement

[Source: ISO 19011]

Nonconformities

FOR MANAGEMENT SYSTEMS

What are nonconformities

- the auditors do not provide suggestions on how to resolve the nonconformities.
- Nonconformity reports must be very **clear** and **objective**.

[Source: ISO 19011]

Nonconformities

FOR MANAGEMENT SYSTEMS

What are nonconformities

- Nonconformity reports have 3 elements:

1. the **declaration** of non-conformity (description of the element of the system that is incorrect)

2. the **evidence** (what has currently been found)

3. the **requirement** (what should have been)

[Source: ISO 19011]

Nonconformities

FOR MANAGEMENT SYSTEMS

What are nonconformities

- ISO 27021 requires that only non-conformities that involve failures in complying with one or more requirements and / or the system's inability to achieve the desired results, must be closed with an effective correction and corrective action before certification (*major non-conformities*).
- Please note that the *opportunities for improvement* **are not** *non-conformities*.
- It is good practice to consider opportunities for improvement, even though recommendations are not binding.

[Source: ISO 19011]

Corrective and preventive actions

MANAGEMENT SYSTEMS

What are **corrective** and **preventive** actions

Corrective action is needed to eliminate the cause of a detected non-compliance.

Preventive action is to eliminate the cause of a potential non-compliance.

Closing meeting

MANAGEMENT SYSTEMS AUDITS

What are its charateristics?

- It must be preceded by an internal meeting of the audit team;
- presence of the **management** and the heads of the audited processes
- there must be **no surprises** (non-conformities must be communicated or anticipated when they are discovered)
- discussion of corrective actions must occur first

Closing meeting

MANAGEMENT SYSTEMS AUDITS

Contents of the **final report**:

- objectives of the scope of the audit itself
- dates and places of the audit
- identification of the customer, auditor and people audited
- audit criteria
- auditor's judgment on compliance with the specified criteria
- non-conformities and observations
- confidentiality
- attachments: *complete* checklists and notes, non-compliance reports, planning of *corrective* and *preventive* actions.

Use case

EXAMPLE OF FINDINGS IN AN ISMS AUDIT

Case 1:

Beta company intends to certify its information security management system by declaring the insurance services it provides as the scope of the management system (and therefore of the certificate). Beta also provides financial services, which are not included in the scope.
The needs and expectations of interested parties are not included in the scope.

In the role of the auditor, in your opinion, what are the points of the ISO 27001 standard that have been disregarded, which may lead to non-compliance?

Use case

EXAMPLE OF FINDINGS IN AN ISMS AUDIT

Case 2

The Gamma company submits an application for certification of its ISMS to the certification body. When analyzing documented information from the management system, the company does not have a written information security policy.

In the role of the auditor, in your opinion, what are the points of the ISO 27001 standard that have been disregarded, which may lead to non-compliance?

SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Antonio **Belli**
Simone **Soderi**
antonio.belli@unipd.it
simone.soderi@unipd.it

Thanks for your attention!

M11 Audit techniques and approach examples