



How to perform an internal audit using ISO 19011

Table of Contents

- Introduction 3
- Why ISO 19011?..... 3
- What’s new in ISO 19011:2018? 4
- ISO 19011 principles of auditing 5
- ISO 19011 auditor characteristics 6
- Steps for internal auditing using ISO 19011..... 7
- Conclusion 9
- Sample of documentation templates 10
- References 10
- About the author 10

Introduction

In all management system standards issued by the International Organization for Standardization (ISO), and standards that are related to them, there is a requirement to perform internal auditing of the company's processes. These requirements are found in each of the standards, i.e., [ISO 27001](#), [ISO 20000](#), [ISO 9001](#), [ISO 14001](#), [ISO 45001](#), [ISO 13485](#), [IATF 16949](#), and [AS9100](#), and are relatively the same no matter which standard you read. These requirements for internal audit provide a method of checking that the system you have implemented is working as you planned.

The internal audit process is intended to help you maintain your processes by looking at what is happening in the process and ensuring that this meets the planned arrangements - both those of the ISO standard and the policies and procedures implemented by the organization. In addition, the internal audits provide information on the effective implementation and maintenance of the management system. Each standard requires that you perform internal audits, but they do not give details on how to implement one, as there may be different ways to audit depending on the organization's needs.

For a more detailed process for conducting audits, there is the [ISO 19011:2018](#) standard: guidelines for auditing management systems. This standard is issued by the ISO as the premier method for carrying out audits of a management system, and it is the standard used to train certification auditors. So, using ISO 19011 allows you to understand how the certification auditor will look at your management system when he/she conducts the certification audit.

Why ISO 19011?

As said, ISO 19011 is the standard that defines how to perform an audit for a management system. This is the document according to which certification auditors are trained, and expected to align, but it is also a helpful guide for how to do any management system audits, including internal audits.

This standard says that an internal audit is an audit performed by, or on behalf of, the organization to review the management system. This basically means that you can use your own employees to perform an internal audit, or you can hire someone from the outside to perform the internal audit. On the other hand, the external audit is an audit done by a third party on their own behalf – in the ISO world, the most common third-party audit is the certification audit performed by the certification bodies.

You can also understand the difference between internal and external audits in the following way: the results of the internal audit will be used only internally in your company, while the results of the external audit or third-party audit can be used publicly as well – for instance, if your company goes for the certification audit and if your company gets the certificate, this certificate is a public document, which means it will often be presented to others.

Also, the main purpose of the internal audit is to improve the management system in your company, whereas the purpose of the certification audit is actually different; its purpose is to find out if your company is compliant with the standard, which automatically leads to issuing the certificate. However, because one of the outcomes of the internal audit is to prepare employees for the certification audit, using the same format and guidelines for the internal audit will help to do this.

Some people confuse the ISO 19011 standard with other standards due to the numbering convention. For help with resolving this confusion, see the article: [ISO 9011: Don't confuse it with ISO 9001 or ISO 19011](#).

What's new in ISO 19011:2018?

The biggest change in ISO 19011:2018 is the introduction of risk-based auditing to the principles of the management system audit. This change aligns with the updates to the ISO standards to align with Annex SL, which brings the assessment of risk, and making plans to address risk, into the management systems. This same thinking about risk is now part of how we think about auditing the processes of the management system. Risk, as defined in the ISO documents, is the effect of uncertainty, and planning to deal with the uncertainty in auditing is a helpful addition to the auditing principles. When planning for the audit process, we need to understand the uncertainty that is part of the process, the potential consequences and likelihood of occurrences of events, and how these will impact the audit.

So, when planning an audit, you need to look at the processes to be audited and understand what could go wrong, including the two types of risk: risk that the audit objectives will not be achieved and risk that the audit will adversely affect the process. For instance, if the process owner is in the process of making major changes to a sub-process (such as the supplier approval of a sub-process that is part of the purchasing process), this might mean that you will not be able to adequately audit this part of the process, as the records will not match the new process. In fact, conducting this audit when the process is being changed could waste resources that would be better used to help verify the new process after implementation, something that could greatly benefit the process owner. This all needs to be considered when planning the audit.

Another change to the ISO 19011 standard is the process flow chart included in the standard. In the previous versions of the standard there were separate figures to show the flow of the audit program and the flow of the process audits. While these flow charts were good, the new figure now shows both processes in the same flow chart so that you can easily see the interaction between the two processes: when the process audits are part of implementing the audit program, and where the information from process audits flows into the monitoring of the audit program.

For more on Annex SL, what it is about, and how it relates to management system requirements, see the article: [ISO 45001:2018 compliant with Annex SL?](#)

ISO 19011 principles of auditing

In order to make the audit an effective tool for the organization, and to make the data collected accurate and useful, there are seven principles that need to be included in the audit program. These principles help you to provide audit conclusions that are relevant, consistent, and useful, and all members of the audit are expected to follow these principles during the audit activity.

Integrity – Auditors need to be ethical, honest, and responsible. If you are not competent to audit a process, due to a lack of understanding, then you need to stop. Audits need to be done impartially to make them fair and unbiased. Remember, you are auditing to confirm conformity - you are not digging for errors.

Fair presentation – The audit needs to report the truth, accurately and objectively. Any audit statements need to be based on verifiable facts, and not on the opinion of the auditor. Audit reporting needs to be timely, clear, and complete so that the facts can be acted upon if necessary. If there is a problem in a process, this needs to be stated clearly throughout the audit process, not ignored during the audit and only reported in the audit report.

Due professional care – Making reasonable judgements based on the importance of the task is essential. If you are auditing a critical function, looking deeper and taking more samples is a good way of ensuring that you check thoroughly.

Confidentiality – Auditors may look at information that is not intended to be widely known, such as financial information or personnel records. This information needs to be used appropriately for the audit, and not disclosed or used inappropriately.

Independence – Auditors should not audit their own work and, where possible, should not audit activities that they are significantly involved in. It is noted in the ISO 19011 standard that this can be difficult in smaller organizations, but that every effort to remove bias needs to be made.

Evidence-based approach – Similar to fair presentation, the auditor needs to have verifiable facts to back up their audit findings and conclusions. These facts mostly come from records of the process, but they can also be statements of fact by knowledgeable personnel or observations of activities. If there is no evidence of a nonconformity, then a nonconformity should not be raised.

Risk-based approach – Considering risks and opportunities in the audit is important to ensure that you focus on significant matters. Remember the two types of risks that need to be addressed: the risks that the audit objectives will not be met, and the risk that the audit will adversely affect the process being audited.

ISO 19011 auditor characteristics

As with all processes in your management system, you need to identify the competencies required to perform the process, and then ensure that the people meet these requirements. Part of the competence of the ISO 19011:2018 standard includes a set of auditor characteristics, or personal behaviors, that auditors need to be successful in. To support audits that meet the seven principles, the ISO 19011:2018 standard lists 13 attributes that you should look for in an auditor.

These professional behaviors will help the auditor to ensure that the findings and report of their audit is unbiased and beneficial to the organization, as is the intent of the ISO 19011:2018 standard. These behaviors include the following characteristics:

Ethical – Is the auditor fair, truthful, honest, discreet, and sincere?

Open-minded – Can the auditor consider alternate ideas or points of view so that they can assess these ideas?

Diplomatic – Tact in dealing with individuals can be critical for a successful audit outcome.

Observant – Not every audit question is answered by records or interviews. Sometimes, observation of the activities taking place is important (e.g., are people wearing the required safety equipment in the area?).

Perceptive – Can the auditor understand different situations, including processes that are not designed as they would expect? Are they aware of what is going on in order to assess how it is affecting the process being audited?

Versatile – You may need to adapt to certain situations during an audit, and you need an auditor who can do this. Is an auditee sick? Do you need to change the times of auditing? Do you need to switch processes to audit with another auditor? What are you going to do about these challenges?

Tenacious – Sometimes the audit can get off track if the auditor is not focused on meeting the objectives of the audit. A tenacious auditor will prevent this from happening.

Decisive – The auditor will need to make decisions on whether the information presented meets the intent of the planned process, and this will need to happen in a timely fashion.

Self-reliant – While audits are often done as a team, the individual process audits are often done by a sole auditor, so this person will need to be able to act independently.

Act with fortitude – Not every audit finding will be popular, and the auditor will need to be able to stick to the conclusion that the evidence supports, even if this makes people unhappy. This does not mean that the auditor should never change their mind if additional data is presented, but it does mean that the auditor should not just change the audit finding because the auditee doesn't like it.

Open to improvement – Being an auditor means continually trying to learn how to audit better. Using their auditing skill is helpful, but they will also need to look for ways to improve their skills, such as using online training or seminars.

Culturally sensitive – Respect for the culture of the auditee is imperative for an auditor to successfully find out the information they need to determine if the planned arrangements for the process are met.

Collaborative – Even though individual process audits are done independently, the overall audit is often done as a team, and the auditor will need to collaborate with that team, and the auditee’s personnel, to get the job done.

To learn how to perform an internal audit, see this list of free online [ISO internal auditor courses](#).

Steps for internal auditing using ISO 19011

The steps for auditing in ISO 19011 are separated into two distinct parts: managing the audit program and conducting an audit. Each of these two parts has six individual steps within it, and conducting an audit is part of the overall audit program.

The audit program

The audit program includes all of the activities you undertake to plan all of the audits for the management system. This will include decisions such as having an audit schedule with process audits spread over the entire year, or having all processes audited together as the certification auditors would in a certification audit. Who will your auditors be, and what are the competencies required? Will you combine the audits of several management systems, or audit them separately? In short, the audit program is everything you need to do to prepare for actually conducting an audit. Below are the six steps included in the audit program as described by ISO 19011:2018:

- 1) **Set audit program objectives** – What are the objectives of the audit program? What management systems are included? How mature is the management system, and how well are performance indicators used? What processes, products and services, and projects need to be included? For instance, will the audit objectives focus strictly on conformance of the processes, or will it also focus on opportunities for improvement?
- 2) **Determine risks and opportunities** – What are the risks and opportunities that need to be addressed by the audit program? Are there risks that need to be addressed, or opportunities to capitalize on, related to planning, resources, auditors, communication, coordination, documents, monitoring, or auditee availability? If so, what plans need to be put in place to address the risks or capture the opportunity? For a critical process, you may need to speak to key people who are hard to connect with, so planning for this can help ensure audit success.
- 3) **Establish the program** – What are the roles and responsibilities for managing the audit program? How will you ensure auditor competence and audit resources? What is the extent of the audits you will do, and what processes need to be included in the audits? For example, does the audit of the purchasing process consider all of the sub-processes of supplier approval, supplier maintenance, and placing purchase orders, or only some of these sub-processes?

- 4) **Implement the program** – You implement the program by planning and performing each process audit. What are the objective, scope, criteria, and audit methods for each individual audit? Who will be the auditors for each audit, and what will their responsibilities be? How do you manage audit reports and records? This is where the link is made to conducting an audit, where this information is used to initiate the audit.
- 5) **Monitor the program** – You will monitor if the audit program is occurring as planned, or if changes are needed. Are schedules being met, and are audit plans being completed? Is documented information adequate, and are auditor skills sufficient? Are there any changes that need to be made to correct or improve the audit program? This information comes from the process audit step of completing the audit.
- 6) **Review and improve the program** – As with all processes, the audit process needs to look for ways to make the process better. Do we need to increase the number of any specific process audits? Are we auditing certain processes too often? How does the audit program need to change?

For more on the management of the internal audit process, see the article: [How to prepare for an ISO 27001 internal audit](#).

Conducting an audit

As part of implementing the audit program, one or several audits will be conducted. Each audit will be tailored to the scope and objectives planned for the audit, but the general process described below is followed to ensure that the audit is successful:

Initiate the audit – The auditor needs to initiate contact with the auditee and ensure that the audit is feasible. When will the audit be, and what is the audit schedule? If you find out that a major sub-process is in the process of change, you may need to modify the audit objectives, as that part of the process may not be easily assessed. Here is where you make agreements with the auditees on what will happen and who to talk to.

Prepare the audit – Audit preparation is critical for an effective audit, and the internal audit plan needs to be created to guide the audit activities. Auditors need to review documentation and plan for risks associated with the audit. Audit checklists are necessary to help guide the audit, including enough information so that another auditor could take over if necessary, but they also need to be flexible enough to allow the auditor to follow an audit trail. The audit checklist becomes the backbone of what will be asked during the audit.

For more information on audit preparation, see the article: [ISO 9001: How to prepare for an internal audit](#). For information on creating audit checklists, see the articles: [How to create a checklist for an ISO 9001 internal audit for your QMS](#) and [How to create a checklist for an ISO 13485 internal audit for your QMS](#).

Conduct the audit – After preparation, the audit is conducted. The audit process starts with an opening meeting where information about the audit is confirmed and the audit plan reviewed to ensure that it can be completed. Auditors then need to gather and verify information, which is done through the process of interviews, observing activities, and reviewing documents. The auditor then compares this information to the planned arrangements and generates the audit findings. When all audit findings are gathered, the final audit conclusions are reached, and the closing meeting is conducted to present a verbal report of the audit.

For more insight on asking questions during an audit, see the article: [Questions to successfully perform ISO 14001 top management audit](#).

Prepare the audit report – The audit report is not only a method of delivering the audit findings and associated audit evidence to the audit client - it is also the record to show how the audit was performed. A good audit report will demonstrate that all the principles of auditing were followed, and that the audit conclusions are sound. The audit report should give all the information necessary for the auditees to not only know what was looked at, but also what needs to be investigated to take corrective action.

For more information on audit reporting, see the article: [Writing a good QMS internal audit report](#).

Complete the audit – The audit is considered complete when the planned audit activities are done, or otherwise agreed to be left incomplete. Audit reports are filed, and necessary feedback is given to monitor the audit program, such as lessons learned during the audit.

Conduct follow-up activities – Although not always part of an audit, some follow-up activities may be identified. They will include the auditors in the corrective action process for nonconformities. Verification of corrective actions may be done, but it is not mandatory that this becomes part of all audits and is only done when agreed in the closing meeting.

For more on improving internal audits, see the article: [7 ways to improve the internal audits of your ISO 27001 ISMS](#).

Conclusion

While an internal audit process is mandatory for all ISO management systems, utilizing the formalized approach prescribed in ISO 19011 is not a requirement. However, this is a well thought-out, world-class format for planning and performing process audits and, as such, can help you to ensure that the process you implement for your internal audits gives you the most consistent and effective outcome.

If you are looking for a way to improve the success of your internal audit program and make it more useful for the continual improvement of your organization, it would be beneficial to turn to the requirements of ISO 19011:2018 to find better ways to audit.

Sample of documentation templates

The following toolkits can help you with the processes for auditing various standards:

- [ISO 27001/ISO 22301 Internal Audit Toolkit](#)
- [ISO 9001 Internal Audit Toolkit](#)
- [ISO 14001 Internal Audit Toolkit](#)
- [ISO 45001 Internal Audit Toolkit](#)
- [ISO 13485 Internal Audit Toolkit](#)
- [IATF 16949 Internal Audit Toolkit](#)
- [AS9100 Internal Audit Toolkit](#)

References

- [27001Academy](#)
- [9001Academy](#)
- [14001Academy](#)
- [45001Academy](#)
- [20000Academy](#)
- [13485Academy](#)
- [16949Academy](#)
- [9100Academy](#)

About the author

Mark Hammar is a Certified Manager of Quality / Organizational Excellence through the American Society for Quality, and he has been a Quality Professional since 1994. Mark has experience in auditing, improving processes, and writing procedures for Quality, Environmental, and Occupational Health & Safety Management Systems, and is certified as a Lead Auditor for ISO 9001, AS9100, and ISO 14001.



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

Email: support@advisera.com
U.S. (international): +1 (646) 759 9933
United Kingdom (international): +44 1502 449001
Toll-Free (U.S. and Canada): 1-888-553-2256
Toll-Free (United Kingdom): 0800 808 5485
Australia: +61 3 4000 0020

EXPLORE **ADVISERA**

