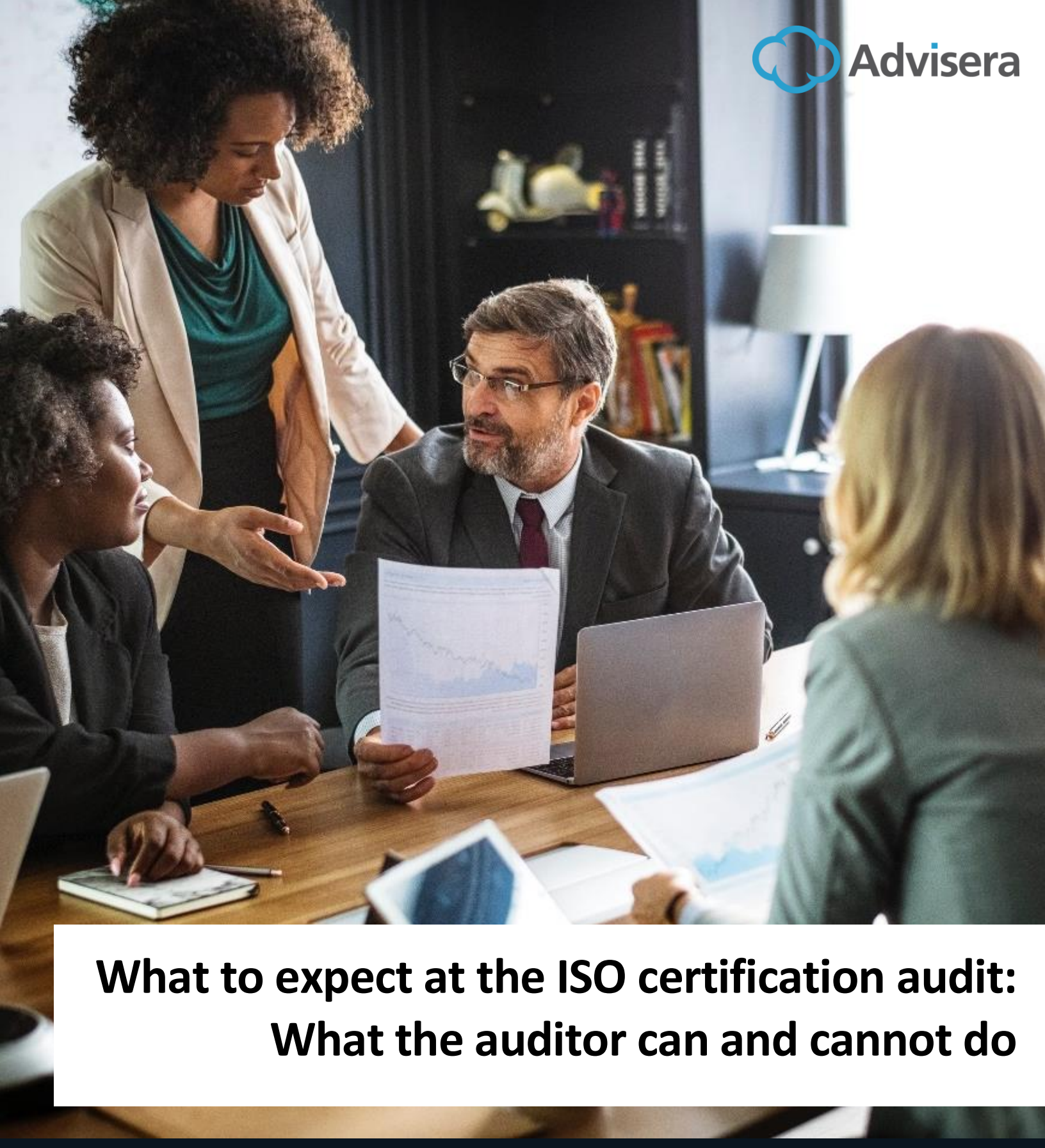


What to expect at the ISO certification audit: What the auditor can and cannot do

Advisera

Making certification simple.

Table of Contents

Introduction

With the ever-increasing popularity of implementing ISO management system standards to help focus a company's policies and procedures on a specific topic such as quality, environmental performance, occupational health & safety, or information security, companies have been taking to many different management system standards to help them ensure that they have all the processes that they need included, and that nothing is missed. These standards include ISO 9001, ISO 14001, ISO 45001, ISO 27001, ISO 20000, and ISO 13485, as well as IATF 16949 and AS9100, because they are based on ISO 9001. Many companies have seen the benefit of implementing more than one standard into one integrated management system, as they provide focus on different important aspects of the organization.

No matter what management system standard or standards you choose to implement, you will have to consider the question of certification and what this means for your company. Certification is the process that a company goes through to have a management system audited against a certain standard set of requirements, and the certification shows that the requirements have been met. This white paper shows what certification means, including why you would want to certify your management system, and what you can expect from the certification audit process.

Certification of persons vs. certification of organizations

One of the most common misunderstandings when it comes to certification is for whom it is intended. Is certification for individuals or for companies? Very often people expect personal certification related to a standard, while ISO certification is primarily intended for organizations. This kind of misunderstanding is not entirely unexpected, since many certifications in the security domain (e.g., CISSP, CISA, CISM) are focused on the certification of persons, and have nothing to do with organizations.

So, is ISO certification intended for organizations or persons? Actually, both.

Certification of organizations

ISO management system standards were initially designed for the certification of organizations. The system works like this: companies (or any other type of organization) develop their management system, which consists of policies, procedures, people, technology, etc., and then invite a certification body to check out whether their management system is compliant with the standard – this check is done during the so-called certification audit.

If the certification audit is successful, the certification body will issue a certificate stating that the organization in question is compliant with the specific ISO management system standard.

In this case, the employees working at that organization are not certified, although it has been confirmed that they behave according to the standard.

Certification of persons

However, the whole industry related to ISO standards (certification bodies, consultants, training institutions, etc.) soon realized that if there are no qualified employees who could develop and maintain the management system, the whole concept would fail.

Therefore, various trainings have been developed for individuals who need to get education for ISO management system standards. There are now dozens of different trainings for individuals lasting from a few hours to a few weeks. The most recognized trainings are the ISO Lead Auditor Course and ISO Lead Implementer Course, with many courses issuing an internationally recognized certificate (under the accreditation of institutions like IRCA or Exemplar Global).

This way, an individual who attends the training and passes the exam obtains the certificate that is issued in their own name. But, even if all the employees at a company were certified, this still doesn't mean that the company itself would get the certificate – there is quite a big difference between certification of persons and organizations.

So, ISO standards do offer various possibilities for certification. The best, of course, would be to pursue both certifications – certify your personnel so that they can help your organization develop and maintain an adequate management system, and certify your company so that the training of the individuals is done systematically and according to realistic security needs.

The rest of this white paper will discuss the process for certifying your organization.

Why go for certification?

If your company is in the process of implementing an ISO management system, you are probably wondering whether to go for the certification. And, as you probably know, certification is not mandatory for most ISO management system standards – so you have to ask yourself one important question: Do you really need it?

Many organizations have implemented the standard(s) without going for the certification – one obvious example is banks and other financial institutions. Regulations in most countries are such that they had to implement very strict information security and business continuity procedures and safeguards, and the majority of them did that by using ISO 27001 and ISO 22301. But, very few of them got certified – they concluded that there was no business reason for them to do it.

And this is exactly what you need to do – consider carefully if you need the certificate. Here are the potential reasons why you might find the certification useful:

1) **Marketing**. You can use the certificate to get some new clients (because of, e.g., tenders), or to further satisfy your current clients and stay in business (e.g., all your competitors already have the certificate).

2) **Compliance.** In rare cases, some regulations will require you to implement an ISO management system standard, but more commonly you may have cases where you will sign contracts with clients which oblige you to implement a specific management system compliant with an ISO standard. And instead of having to go through audits from all of the auditors from each of your clients who want to check whether you complied with the contract, you can have the certification auditor do the job, and then show everyone else the certificate.

3) **Internal pressure.** In some companies, these kinds of projects will never finish unless there is powerful pressure – e.g., a clear deadline. So, if you agree with the certification body on a fixed date for the certification audit, both your management and your employees will have a much stronger sense of urgency for implementation.

4) **Objective inputs.** If you want your business continuity to be at a really high level, it is good to call in people with high experience and who know how you can benchmark with the best in the industry. Certification auditors will be more than happy to audit someone who is trying really hard and will provide inputs on what you could improve.

If you didn't find yourself in any of these bullets, you probably don't need the certificate at all – you can be one of those many companies that have implemented an ISO management system standard because they understood the biggest value is in the methodology these standards provide.

To get the most benefit out of your certification, it is important to pick a good certification body to audit your management system.

There are also some helpful checklists to use when you are choosing a certification body:

- List of questions to ask an ISO 9001 certification body
- List of questions to ask an ISO 27001 or ISO 22301 certification body
- List of questions to ask an IATF 16949 certification body
- List of questions to ask an ISO 13485 certification body

What are the phases of the certification process?

The ISO management system certification process for companies starts with the decision to use an ISO standard as the basis for the management system. After this, the company will take all actions necessary to create and document their system by utilizing the standard requirements as a guideline for what needs to be done. The implementation is complete after the company has maintained the system for a length of time, and then conducted internal audits and at least one management review of the system. After this, certification auditors from a certification body (sometimes called a Registrar) will assess the system against the requirements for the particular ISO standard, and if it is deemed that the system meets the standard, a certificate will be issued showing that the company's management system is acceptable to meet the standard. The company is then considered to be certified.

The certification process after implementation is generally divided into three phases as follows:

1) **Documentation audit**. The certification auditor will come and review all of the documentation that you have created for your management system to ensure that you have everything in place to meet the requirements of the standard.

2) **Certification audit.** The certification auditors will come and audit what is happening in all of your processes to compare them to what was documented and ensure that everyone is compliant.

3) **Surveillance / maintenance audits.** Once the certificate is issued, it is valid for three years – during this time, the certification auditors will come and audit a sample of processes from the system to make sure you are maintaining the system. Over the surveillance time the entire system is intended to be audited, but not all at once.

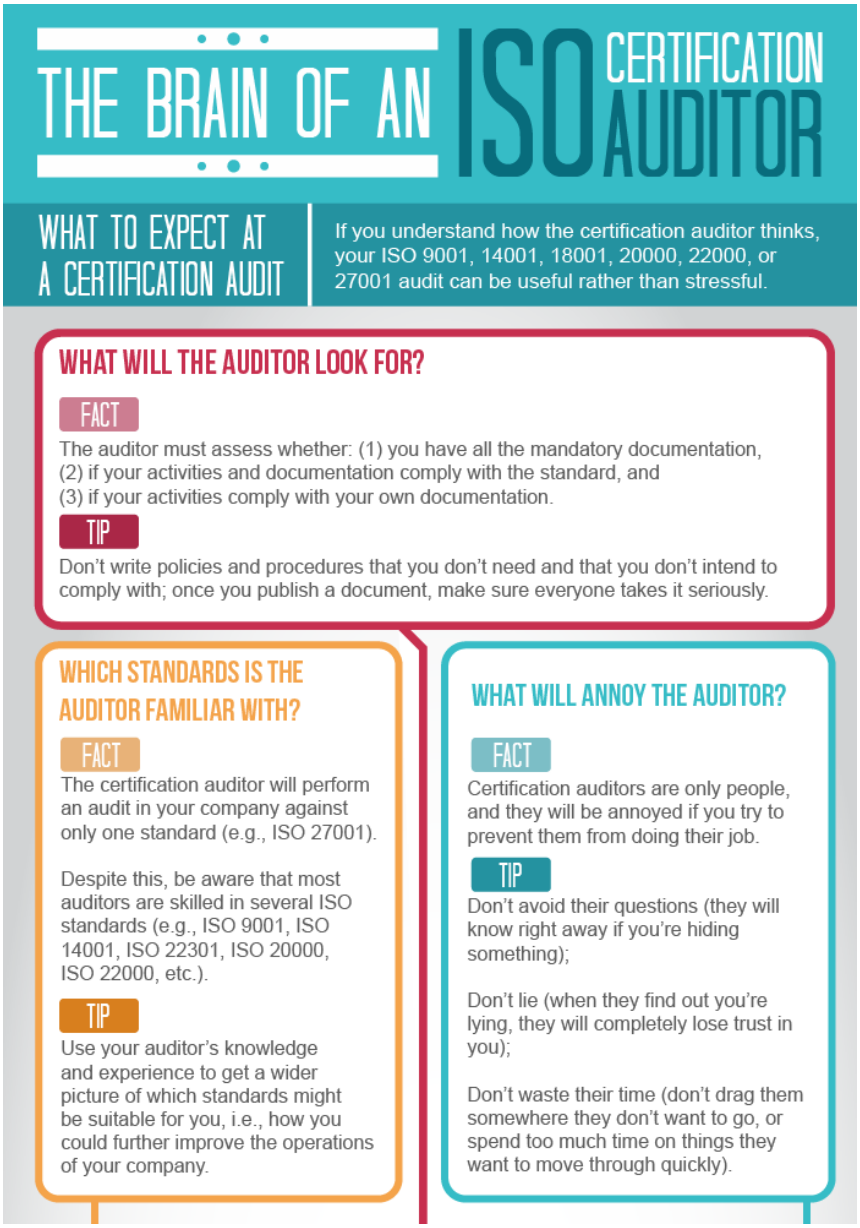
At the end of three years, the cycle will start again if the company chooses to maintain the certification and the benefits it provides. Then, a recertification audit that reviews the entire system will be done.

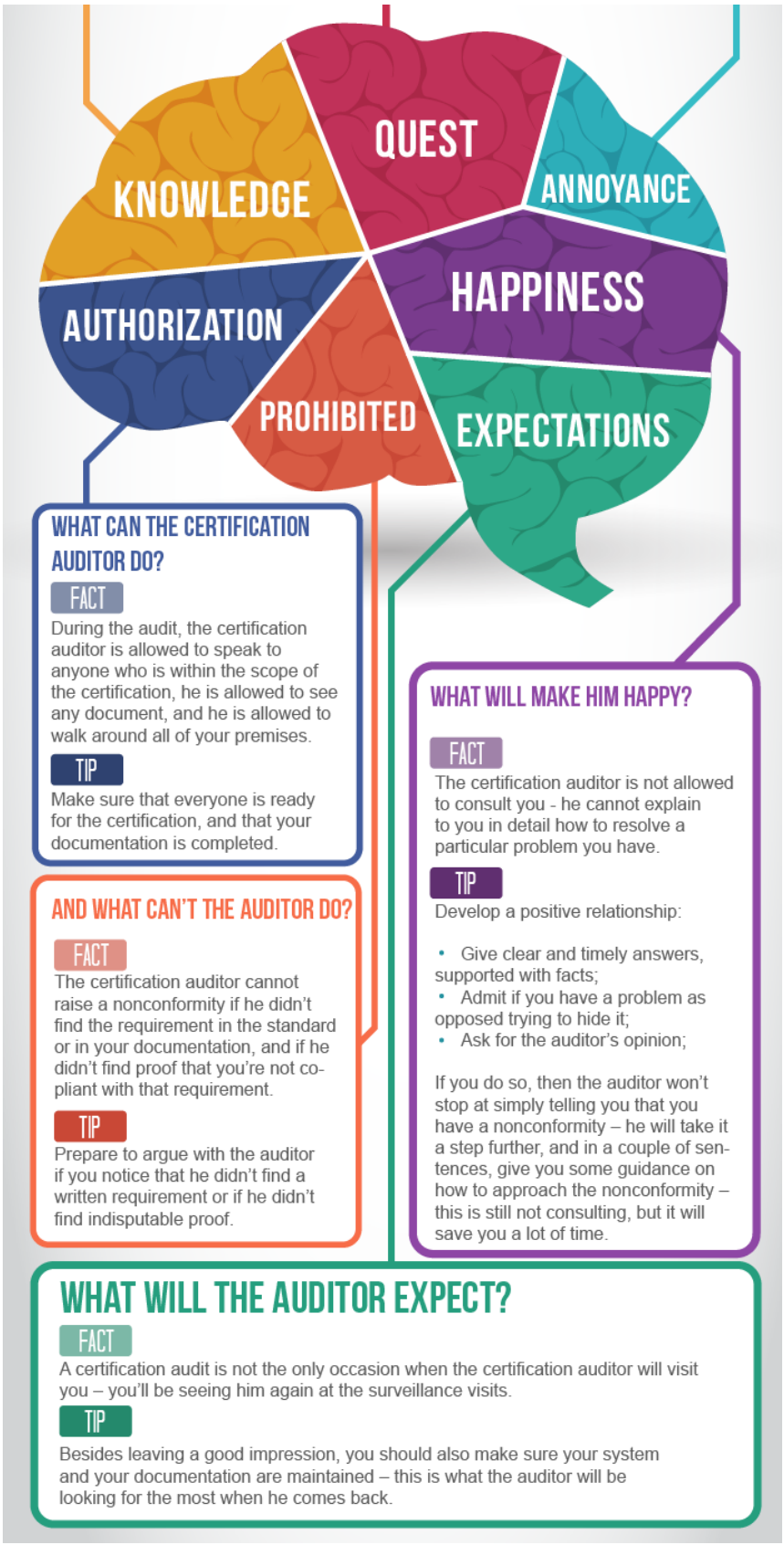
For more information, see these helpful articles:

- Checklist of ISO 9001 implementation & certification steps
- 12 steps for implementation and certification against ISO 45001
- What's needed for successful ISO 20000 certification of your company?
- ISO 27001 implementation checklist

What will the auditors look for during the certification audits?

If your company is going for the ISO certification, you may not be very happy about it – certification auditors are usually perceived as persons who are not very open minded and who will insist on a whole bunch of unnecessary details. But the truth is, it doesn't have to be this way – if you understand how the auditor thinks, your audit can turn out to be much more pleasant and useful. Here's what you need to know.





To be ready for the audit, you will have had to comply with, and in many cases provide evidence of your conformity with each of the clauses of the specific ISO standard, working carefully through each part. Technically, you may feel you are ready, but you might have that feeling there must be something you have forgotten. So, the parameters of the standard aside, what questions might the auditor actually ask you? And are you ready for them?

Preparing for questions by the auditor

The ISO management system standards are very specific and precise. Generally, the standard tells you exactly what you have to comply with and, for the most part, what you have to do to comply, but in my experience some of the most telling questions will be asked by the auditor himself. The standards talk of the "top management's commitment to comply with the requirements of the standard and to continually improve." The auditor will almost certainly ask why your organization is pursuing the accreditation. Hopefully, your organization wants the ISO certification to improve the performance of your company, and help satisfy your interested parties in the most efficient way possible. If the real reason is that you seek accreditation as a result of pressure by a customer, or you cannot enter a tendering process without certification, then that is not what your auditor will want to hear.

What, more questions?

The most recent standards update to Annex SL place extra emphasis on the commitment of top management to the management system and its ability to deliver the set objectives. Being able to show evidence of your management review and its outputs and improvement measures will be required, but it is highly unlikely that this will be enough for a good auditor – he will want to speak to your management team. Your senior team will need to illustrate that they are well informed, have a strategy for the management system, and are prepared to show commitment to ensure the correct risk management and corrective actions are undertaken, thereby ensuring that continual improvement can be achieved. It will pay to remember that your certification audit is not only a paper exercise, but you will be judged on what you say and the knowledge that you show.

In days past, certification auditors were primarily interested in how you dealt with internal issues, but as times have changed, auditors are equally (if not more) interested in the wider external impact that your performance – and your products – can have. Evidencing this to your auditor will create the positive impression that your organization is working to improve your compliance to the expectations of interested parties, for the ongoing benefit of the marketplace. Ironically, this will no doubt help you to avoid some questions from the auditor!

Deeds, actions, and questions

In summary, to prove to an auditor that your organization can pass a certification audit, you must do two things. You must prove that you comply with every clause and salient point of the standard, and secondly you must demonstrate by the knowledge of your team that you understand the ethos behind the standard. As ever, don't make anything up for the benefit of the auditor, but be honest and truthful, answering the questions as best you can. If you don't know the answer, tell him you will find out. However, display a positive attitude, have some great material, and be mindful that you want to demonstrate the impact that your organization and products have. Prepare for the probing questions as well as you prepare for developing the management system itself.

For more information, see these articles: What questions to expect on the ISO 9001 certification audit, How to prepare your company for the ISO 9001 certification audit, and Becoming ISO 27001 certified - How to prepare for certification audit.

What can the auditor *not* do?

Just as you needed to meet the requirements of the ISO management system standard for implementing your management system, the certification body auditors also have a standard that they need to follow to ensure that their audit is acceptable to the accreditation bodies that oversee their audits. This standard is called ISO 17021, and it gives the certification auditors many things to ensure when they audit your management system. One of the main items included in this standard is the requirement for certification auditors to remain free from bias regarding the management system they are auditing. This means they are not allowed to audit a management system that they have helped create, and further, they are not allowed to tell you what to do to improve your system and make it better. Certification auditors are there to verify conformance of your processes against your internal processes and the management system standard that is applicable.

Further, if they discover that what is happening in the system does not meet the requirements, then it is their duty to point out this non-conformance so that you can correct it. It is important to note that for something to be a nonconformance it needs to have a requirement that is not met fully, not just something that the certification auditor would like you to do. The auditor cannot raise a nonconformity if there is not a requirement, or if there is no evidence that a requirement is not being met. Nonconformities are not a matter of opinion; they are a statement of fact.

For more information on dealing with certification auditors, see this article: How to approach an auditor in a certification audit.

What do you do about nonconformities?

Many companies going for a certification audit wonder what will happen if the auditors find something wrong in the audit. Will they just leave in the middle of the audit? Will they refuse to grant you certification? Will they never come back? These questions run through the heads of many management system implementers as they await the certification audit, but it is not as bad as you fear. Here is a bit about how audit findings work, what nonconformities mean, and what you need to do about them.

How do audit findings work?

What happens in an audit is that the auditor takes a set of criteria, such as the ISO management system requirements, along with your policies and procedures, and gathers evidence to verify if the criteria are being met. This evidence may be records, statements of facts, or other information that is relevant to the audit criteria. For example, the ISO requirements for control of records demand that you have controls to identify, store, protect, retrieve, and retain records. During the audit, the auditors will check the records you have to make sure that they meet all of these criteria.

Once the audit evidence is gathered, the auditors will compare the evidence to the criteria and determine if the criteria were met. The hope is that this comparison will show that the process is conforming to the criteria, but it

can also show that it is non-conforming. When the audit finding is that the process is non-conforming, then an audit nonconformity is recorded in the audit report. This is not the end of the world.

What are audit nonconformities, and what do they mean?

During a registration audit, nonconformities are generally divided into two different types by certification bodies: major and minor. Both need to be addressed, but each can mean a different thing when it comes to your company certification being granted.

Major nonconformities are typically seen as a breakdown of a requirement of the management system. For instance, the ISO requirements state that you need to prevent the unintended use of obsolete documents, and to address this you may state in your procedure that employees are not to print out copies of documents to keep at their desks and must use the version available on your intranet. If the auditors found many different people across your company using printed versions of older procedures for their work, this could be seen as a major nonconformity.

A minor nonconformity is when there is a problem found that is more limited in scope throughout your company. If the evidence above for the printed versions of obsolete documents occurred only with one or two individuals in one department, then the problem would be labeled as a minor nonconformity.

To answer the earlier question of the auditors leaving in the middle of an audit, this is an extremely rare occurrence and I have only heard of it once. This was when an audit was taking place and several major nonconformities were identified early in the audit, which indicated that the company was actually not ready because the management system was not fully implemented. The termination of the audit was an agreement between the auditors and the company management, as it was seen as an unnecessary waste of resources to continue.

What do you need to do if a nonconformity is found?

It does not matter if an audit nonconformity is major or minor – you should address them in the same way, by correcting them using your corrective action process. The only real difference in this process between a corrective action raised internally in your company, and one raised due to a certification audit nonconformity, is who should review your plan's adequacy and perform the follow up. With a certification audit nonconformity, this should be done with your certification body auditor, as they will record your response to the nonconformity in their audit report and follow up on the completion of the corrective action at their next audit.

For a major audit nonconformity, the certification auditor will want you to implement the corrective action within the agreed timeline, and only then will issue the certificate once they are satisfied that the actions are completed. This may require them to perform a follow-up audit to verify the process is working.

Minor nonconformities found in an audit will need to be addressed within a certain timeline, but the certification can be granted when the corrective action plan is received, and the audit team will follow up at the next maintenance audit by the certification body.

Audit nonconformities are not the end of the world

Because the overall goal of the management system is to make improvements in the system processes, any nonconformity should be viewed as one way to identify these needed improvements. Sometimes, when you have an outside expert look at your processes, they can see things that are not easily seen by an observer internal to your company. Use these findings to improve, and you will be getting the most for your money from your certification audit.

Conclusion

Preparing for the certification audit can be as important as all of the work you have already done in implementing the ISO management system requirements, because the benefits gained by having an outside auditor review and comment on your management system processes can be a good source of improvement initiative ideas. The better prepared you are for the audit, the better you can react to the findings of the audit and make the improvements that will benefit you. The key point of a successful certification audit is to gain a better understanding of how your management system processes work, so that you can take these insights and build on them to make your management system better.

To learn more about preparing for the ISO certification audit, see this eBook: Preparing for ISO Certification Audit: A Plain English Guide.

Sample of documentation templates

The following toolkits can help you with implementing standards:

- ISO 9001 Documentation Toolkit
- ISO 14001 Documentation Toolkit
- ISO 45001 Documentation Toolkit
- ISO 27001 Documentation Toolkit
- ISO 13485 Documentation Toolkit

References

- 9001 Academy
- 14001 Academy
- 45001Academy
- 27001Academy
- 20000Academy
- 13485Academy
- 16949Academy
- 9100Academy

About the author

Mark Hammar is a Certified Manager of Quality / Organizational Excellence through the American Society for Quality, and 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**