



How to be Audit Ready, Always

Simplifying Internal Audits & Enhancing Team Performance

The Internal Audit process is all too often seen as an unnecessary task designed to waste time and halt workers from their ‘business as usual’. Savvy organizations, however, see the internal audit process as a way to ensure continual improvement and mitigate risks – the key is figuring out how to establish a process that isn’t time consuming and allows you to audit your systems and compliance initiatives in a timely and efficient manner.

Internal Audits provide information on the effective implementation and maintenance of an organization’s management system. The ISO 19011:2018 standard provides guidance on auditing management systems and is the standard that is used to train certification auditors.

This document aims to provide further insights into this guidance, and show how Diligent Compliance eases the headache that is internal compliance and makes the process even easier to manage.


People, Process and Technology

Like with any organizational activity, consideration needs to be given to 3 basic elements: people, process and tools. The right people, an effective system and well-planned processes are key to a successful outcome. In many cases, a supporting technology solution ensures effective and ongoing reporting, enabling the organization to bring the auditing function in to business as usual rather than seen as a separate activity.



People

The ISO 19011:2018 standard outlines some key attributes required of internal auditors. They include:

- ▶ **INTEGRITY:** Audits must be impartial, and also ethical and honest
 - ▶ **FAIR PRESENTATION:** Report the truth - facts only. Statements need to be backed up by evidence, not simply opinion
 - ▶ **DUE PROFESSIONAL CARE:** Consider the importance of what you are auditing. Critical processes will require more evidence to check they are working properly compared to a lesser process
 - ▶ **CONFIDENTIALITY:** Auditors may see more information than others would in an organization. It is important to use this information only for the purposes of the audit and never disclose or use it improperly
 - ▶ **INDEPENDENCE:** Auditors should not audit their own work or any activities that they have some involvement in. Sometimes this is difficult, particularly in small organizations
- 
- ▶ **EVIDENCE-BASED APPROACH:** Use records to verify audit findings and conclusions where possible
 - ▶ **RISK-BASED APPROACH:** Focus on what matters and ask two questions: “Are there any risks that the audit objectives may not be met?”, and Are there any risks in conducting the audit that will adversely affect the process being audited?

The standard also outlines the characteristics of an effective auditor that should be inherent in individuals if they are to conduct audits.

These characteristics are:

- | | | |
|-----------------|---------------|------------------------|
| • Ethical | • Perspective | • Self-Reliant |
| • Open-Minded | • Versatile | • Act with Fortitude |
| • Diplomatic | • Tenacious | • Open to Improvement |
| • Collaborative | • Decisive | • Culturally Sensitive |
| • Observant | | |

If organizations don't have the right people, then it may make sense to outsource the internal audit activity. It does help, however, to have a good understanding of the organization and its people, objectives and culture, as this can help in making the audit process less confrontational for those being audited. It is also helpful to know where most documents are stored, thus being able to ask questions such as “can you show me where on SharePoint this process would be located?”

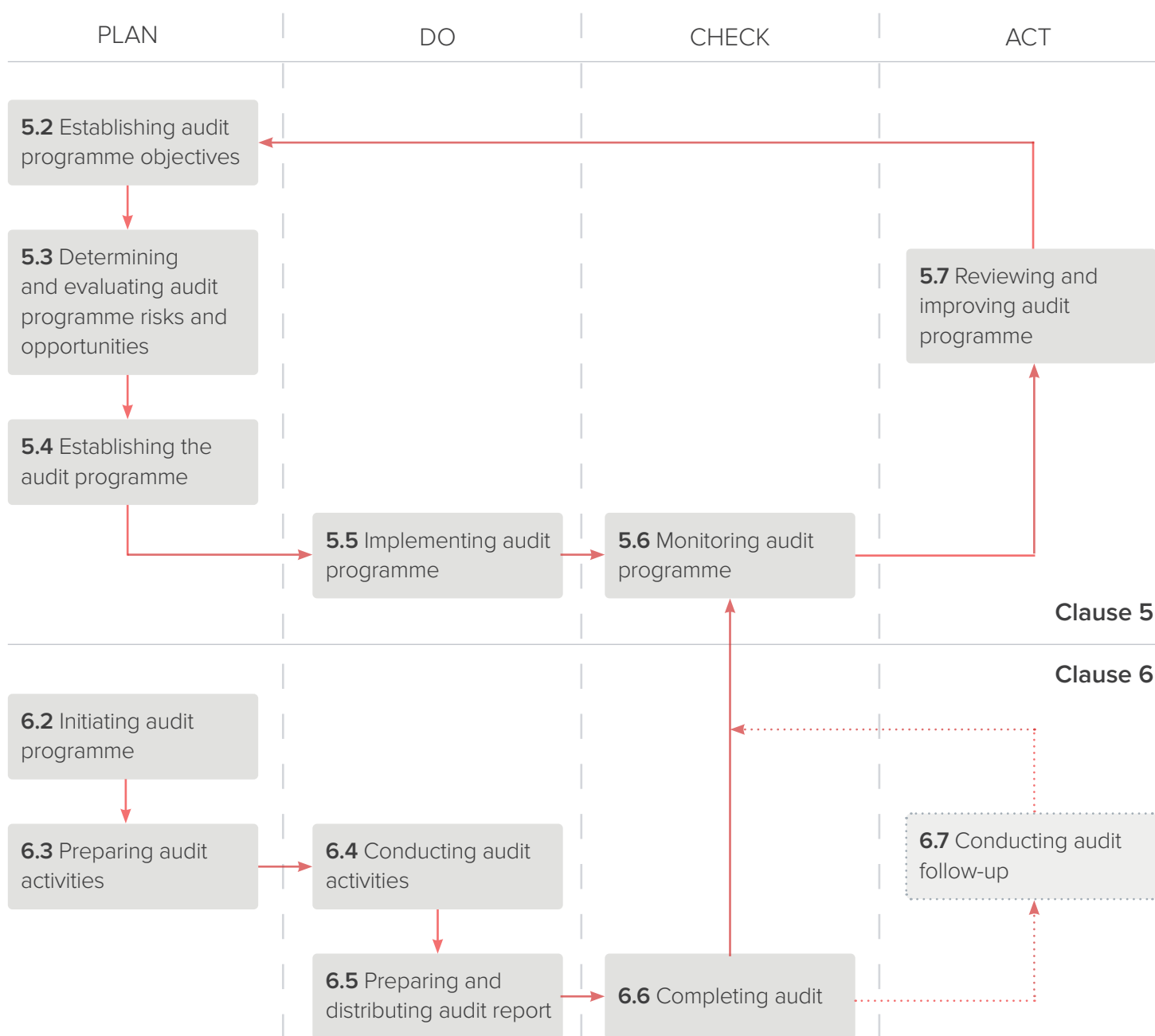
Process

The ISO 19011:2018 standard identifies 2 key clauses in the process of conducting an internal audit. Each of these parts has 6 steps within it, and all follow the standard PLAN, DO, CHECK, ACT cycle.

The two parts are:

- ▶ The Audit Program
- ▶ Conducting an Audit

The following diagram shows how these parts relate:





Technology

The standard itself does not set out any rules or recommendations for using a technology solution as part of the 'Conducting an Audit' section. However, some of the steps in particular would be better managed by implementing the right technology for your organization.

That's where Diligent Compliance fits in. It helps businesses to:

- ▶ Ensure visibility into the myriad compliance-related obligations based on their business priorities, business type and jurisdiction
- ▶ Leverage best practice frameworks and standards to improve enterprise performance
- ▶ Highlight and identify gaps in compliance, policies, and reporting across the entire organization
- ▶ Reduce risk exposure across the organization



Using a cloud-based solution provides organizations with a way to audit a range of standards and frameworks across departments. Audit tools should provide an easy dashboard to show both internal and external auditors the organization's progress against any relevant standard.

Managing the Audit Program

Section 5 of the standard identifies all the activities that must be undertaken to plan an audit.

5.2 Establishing audit program objectives

It is important to establish objectives at the commencement of the audit program to ensure that it is implemented effectively and to ensure that the objectives are consistent with the organization's strategic direction. The audit process should support the management system policy and objectives.

Audit objectives should be based on the following:

- ▶ Needs and expectations of all stakeholders - both internal and external
- ▶ Characteristics of, and requirements for processes, products, services and projects
- ▶ Requirements of the management systems
- ▶ External provider evaluation
- ▶ The level of performance and level of maturity based on KPIs, non-conformities or incidents and complaints
- ▶ Identified risks and opportunities
- ▶ Results of previous audits

5.3 Determining and evaluating audit program risks and opportunities

Consider what may impact the achievement of the audit program's objectives. Identifying risks and opportunities at the outset ensures they can be addressed early and not impede the progress of the audit. Some examples of risks include:

- ▶ Failure to plan effectively
- ▶ Not having adequate resources (insufficient time, equipment and/or training) to conduct an audit
- ▶ Ineffective communication processes and channels
- ▶ Availability and cooperation of auditee and availability of evidence to be sample

Some examples of opportunities include:

- ▶ Allowing multiple audits to be conducted in a single visit
 - ▶ Matching the level of competence of the audit team to the level of competence needed to achieve the audit objectives
 - ▶ Aligning audit dates with the availability of key staff
-

5.4 Establishing the audit program

Roles and responsibilities should be set for the individual(s) managing the audit program. This includes responsibility for the selection of audit teams and the overall competence for the auditing activities and ensuring that appropriate documented information is prepared and maintained, including audit program records.

The individual(s) managing the audit program should have the necessary competence to manage the program. This includes having sufficient knowledge of audit principles, management system standards, information regarding the Organization and its context, plus any applicable statutory and regulatory requirements. It is also useful to have some risk management, project and process management and ICT knowledge.

The extent of the audit program also needs to be determined. Sometimes the program may involve a single audit, but others may be more complex. Factors impacting the extent of an audit program include:

- ▶ The number and method of audits to be conducted
- ▶ Results of previous internal or external audits
- ▶ Language, cultural and social issues
- ▶ Concerns of interested parties, such as customer compliance or non-compliance with regulatory requirements

Finally, the program should include what resources are required. This include considering the type of method used to audit the organization, the financial and time resources necessary (including the impact of any time zone differences) the availability of technology, for example a conferencing facilities or access to a software program, and finally the security clearances and equipment required.

5.5 Implementing audit program

The key to successful audit programs is communication. It is important to communicate the relevant parts of the audit program, including risks and opportunities, to all stakeholders taking part in the program. As the program progresses, progress updates and any issues should be communicated on a regular basis.

Each individual audit should be based on defined audit objectives, scope and criteria. This helps to structure the audit and give those being audited an understanding of what is expected to be accomplished. This may include how well the organization, department or area is conforming to the management system, or identify opportunities for potential improvement of the management system. It is also important to determine how the audit will take place. Audits can be performed on-site, remotely or as a combination.

The selection of individuals appointed to the audit team need to have the right competence based on the complexity of the audit itself. Consideration should also be given to the process should a conflict of interest or competency issue arise. A team leader should be appointed for each audit being undertaken as early as possible to ensure they have enough time to plan.

The standard describes the activities that should be performed during the audit program:

- ▶ Evolution of the achievement of objectives
- ▶ Review and approval of audit reports
- ▶ Review of effectiveness of actions taken to address audit findings
- ▶ Distribution of audit reports
- ▶ Determination of the necessity for any follow up audit

Audit records are necessary to demonstrate that the audit program has been implemented. Part of this involves ensuring that processes are established to ensure that any information security and confidentiality needs associated with the audit records are addressed.

Records can include records related to the audit program (schedules, objectives, risks and opportunities), records related to each audit (audit plans, objective evidence, non-conformance reports, corrective actions, follow up reports), and records related to the audit team (criteria for the selection of audit teams, performance evaluation of audit team members). Records do not have to be exhaustive, but simply demonstrate that the objectives of the audit program have been achieved.

5.6 Monitoring audit program

Just like any other program or project it must be monitored. It is the responsibility of the manager of the audit program to check the following:

- ▶ Are schedules being met?
- ▶ Are program objectives being achieved?
- ▶ How are the audit team members performing?
- ▶ Are the audit teams able to implement the plan?
- ▶ What is the feedback from audit clients, auditees, auditors and others?
- ▶ Is the documented information across the audit process sufficient and adequate?

5.7 Reviewing and improving audit program

The lead auditor should review the audit program to assess whether it is meeting its' objectives. These 'lessons learned' can then be used as inputs to improve the program. This review should also factor in alternative or new auditing methods, any changes that are relevant to the areas being audited, the effectiveness of the actions to address any risks, opportunities and issues associated with the program, and any confidentiality and information security issues relating to the program.

Conducting an Audit

Section 6 of the standard provides guidance on preparing and conducting audits.

6.2 Initiating audit

The audit team leader is responsible for communicating with the audit to confirm authority to conduct the audit and provide relevant information on the objectives, scope, criteria, methods and individuals required to complete the audit. They must also request access to any information they require to plan for the audit. This might include any statutory and regulatory requirements, or any Current risks or opportunities the organization has identified.

It is also important to confirm appropriate time and resources to be available for the audit - this also includes any security access that may be required. If it is considered there is not enough time or the right resources to effectively conduct the audit, then the team leader should propose a new time.

6.3 Preparing audit activities

Prior to the audit, the auditor should gather information to understand the audit's operations. This aids in preparing audit activities and determining which work documents will need to be sighted to assess compliance. This also gives the auditor some advance understanding of the documentation and detect any possible areas of concern.

The documented information could include management system documents and records and any previous audit reports.

The standard recommends that the audit team leaders would adopt a 'risk-based approach' to planning the audit. This approach considers any issues that may arise due to an audit taking place. Examples the Standard provides are where the presence of the audit team members might adversely influence health and safety, security or infrastructure, for example contamination in clean room facilities.

Other details to consider when it comes to preparing for audit activities may be the physical location and timeframes. For example, does the audit team need to take a tour around the facilities, or view the IT set up? How long does it take to get through security checks? Does any IT need to be set up for the audit meeting? Planning for these prior to arrival will ensure that the audit keeps to the timeframes and there are no surprises when it comes time to audit.

6.4 Conducting audit activities

It is often good practice to assign guides and observers to accompany the audit team. Guides should assign the audit team, providing introductions to individuals to be audited, arranging access to specific locations, ensuring that security and confidentiality processes are known to the audit team and providing any clarification or assisting in providing further information as required.

An opening meeting is suggested to confirm that all participants agree on the audit plan to be followed. It also provides a simple way to introduce the audit team and their roles, and give those being audited time to ask any questions.

During the audit, it is also important to ensure a constant stream of information between audit team members, but also between the team leader and the auditee. If a significant risk is found, this should be reported without delay. As the audit progresses, it may be necessary to reassign work between team members, exchange information or make changes to the audit plan, so it is imperative that the lines of communication remain open at all times.

The collection and verification of information is an extremely important part of the audit process. Only information that can be subject to some degree of verification should be accepted as audit evidence. All evidence sighted should be recorded. Methods of collecting information can include:

- ▶ Interviews
- ▶ Observations
- ▶ Review of documented information

The evidence should show that requirements are being met. For example, are they:

- ▶ Interviews
- ▶ Observations
- ▶ Review of documented information

Audit evidence should include conformity and good practices, including their supporting evidence, any opportunities for improvement, and any recommendations to the auditee. Any non-conformities should be graded (this could be as simple as defining each nonconformance as major or minor, or be more complex, such as following a number scale).

The audit team should meet prior to the closing meeting in order to review the audit findings against the audit objectives, agree on the conclusions, prepare recommendations and discuss any follow up that may be required.

The conclusions should address the following issues:

- ▶ Extent of conformity with audit criteria
- ▶ Effective implementation, maintenance and improvement of the management system
- ▶ Whether the audit objective have been achieved
- ▶ Any findings made in more than one area, or in a previous audit in order to identify any trends

The closing meeting should be chaired by the audit team leader and attended by all those responsible for the functions and processes that were audited and the management of the organization being audited. Other stakeholders, as determined by the organization can also attend if deemed relevant. The closing meeting summarizes the audit, advising how the audit findings were collected and explaining the audit findings. If there are any diverging opinions regarding the findings, these should be resolved, if possible, at this meeting, but if not, this should be recorded.

6.5 Preparing and distributing audit report

The auditor in charge is typically responsible for preparing and distributing the final audit report. Although reports often vary by the nature and difficulty of the audit, they usually follow a standard format. Contents typically include the defined scope, objectives, interview participants/locations/dates/times, findings, recommendations and any follow-up actions if appropriate. The report should be dated, reviewed and approved in line with the audit program procedures, and should be issued within the agreed time period; the sooner results are distributed and received, the more accurate they are. The audit report should then be distributed to the intended recipients, as defined in the audit plan, ensuring that appropriate confidentiality is maintained at all times.

6.6 Completing audit

The audit is completed when all planned audit activities have been carried out. Care should be taken to ensure that all evidence gathered during the audit is securely archived and/or destroyed in accordance with defined security procedures. Finally, any lessons learned and opportunities for improvement should be captured and shared to drive continual improvement of the audit program (refer to sections 5.6 and 5.7). Diligent Compliance provides the means by which this can be done efficiently and effectively.

6.7 Conducting audit follow up

If any nonconformities or corrective actions were recorded, then an audit follow up will be required. Usually the actions to be taken are decided by the auditee and a timeframe agreed. The auditee must keep the individuals managing the audit program informed of the status of these actions.

Conclusion

The formal approach outlined in ISO 19011 represents an excellent format for planning and performing audits. Whilst it is not requirement, it will ensure that internal audits within your organization are well planned and focused on providing a consistent and effective outcome.

Ensuring you have the right people and the right process is imperative in the success of the audit program. The question of whether you need technology to help can be debated, however there is no question that a solution such as Diligent Compliance provides organizations with an easy way to conduct audits.

Diligent Compliance helps organizations confidently create, manage, and report on the obligations relevant to their business. They will be audit ready, always.

- ▶ Real-time insight into how the compliance program stacks up against internal and external obligations, gives you confidence you've got the right programs in place
- ▶ Dashboards and reports save time by reducing dependency on manual methods of pulling business-critical information around compliance and policies
- ▶ Customizable library of obligations to reflect your unique business needs and priorities allows you to measure continual improvement in what matters



Be Audit Ready, Always.

Diligent Compliance helps companies manage their compliance with both internal and external obligations, identify gaps, and suggests remedial tasks that will help drive continual improvement.

REQUEST DEMO

Find out why over 16,000 companies and 650,000 users trust Diligent.

Ask about our Governance Cloud.

Begin your journey with Diligent Entities.

Grow with Governance Cloud™.



For more information or to request a demo, contact us today:

Email: compliancesales@diligent.com

Call: +1-866-877-5865

Visit: <https://learn.diligent.com/compliance>