riskza group

RISK-BASED APPROACH TO AUDITING AN ISO MANAGEMENT SYSTEM

info@riskza.com | www.riskza.com | 0861 RISK ZA

CONTENTS

Auditing in the ISO sense is a verification activity and the ISO 19011:2018 Guidelines for auditing management systems, sets out guidance on all aspects of the management systems audit. Importantly, the new standard adopts a risk-based approach to auditing and places greater focus on the competency of audit professionals. This Guide gives a general overview of the ISO 19011:2018 standard and references to the Risk-based approach under Audit Activities.

The Risk-based approach to auditing according to ISO 19011:2018, Guidelines for Auditing Management Systems, is an audit approach that considers risks and opportunities.

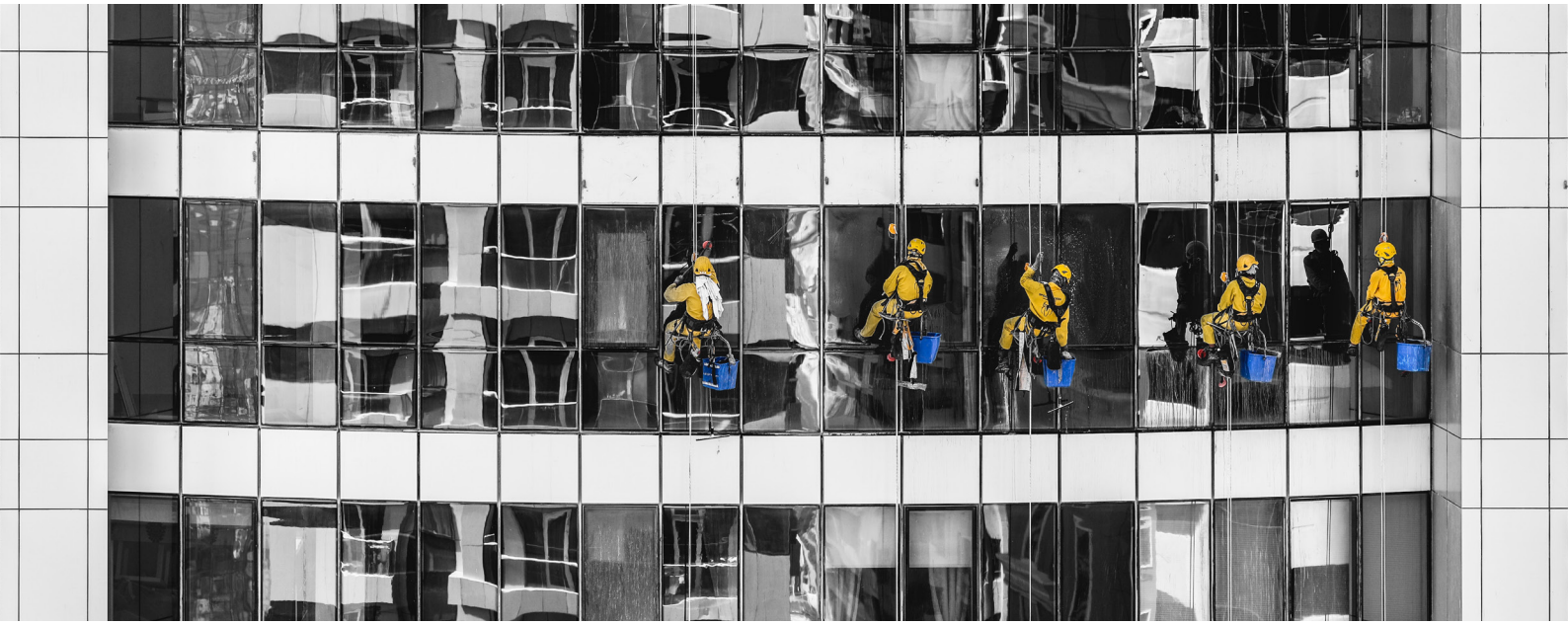
THE RISK-BASED APPROACH TO AUDITING

The risk-based approach should influence the planning, conducting, and reporting of audits to ensure that audits are focused on matters that are significant for the audit client, and for achieving the audit programme objectives.

ISO 19011:2018 DEFINITION OF RISK

Risk is defined in clause 3.19 as the "effect of uncertainty". Notes explain that an "effect" is a deviation from the expected – positive or negative and that "uncertainty" is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence and likelihood.

Additional Notes state that risk is often characterised by reference to potential events and consequences, or a combination of these. The Notes also state that risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated of occurrence.



THE 7 PRINCIPLES OF ISO AUDITING

The principles of ISO auditing contained in 19011:2018 help to ensure that audits are effective and reliable tools and support the Management Systems they are auditing by providing actionable information that organisations can use to improve performance. The principles are:

1. Integrity: the foundation of professionalism;
2. Fair presentation: the obligation to report truthfully and accurately;
3. Due professional care: the application of diligence and judgement in auditing;
4. Confidentiality: security of information;
5. Independence: the basis for the impartiality of the audit and objectivity of the audit conclusions;
6. Evidence-based approach: the rational method for reaching reliable and reproducible audit conclusions in a systematic audit process;
7. Risk-based approach: an audit approach that considers risks and opportunities.

THE KEY STAGES OF AN ISO AUDIT

CHOOSING YOUR AUDIT TEAM

You will want to have a number of trained internal auditors for your audit program. You will be auditing each area of your facility at least once a year, with an audit team of 1 to 4 auditors depending on the size of the organisation. You will want to have enough auditors to ensure they will not be auditing their own area.

Look for employees who have a strength in investigating issues and are good communicators. An audit team leader should have the competence to discuss strategic issues with top management of the auditee to determine if they have considered these strategic issues when evaluating their risks and opportunities.

AUDITOR COMPETENCE

In deciding the necessary competence for an auditor, clause 7.2 states that an auditor's knowledge and skills related to the types and levels of risks and opportunities addressed by the management system should be considered. An auditor should be able to understand the types of risks and opportunities associated with auditing and the principles of the risk-based approach to auditing.

The discipline and sector-specific competence of auditors should include the principles, methods, and techniques relevant to the discipline and sector, such that the auditor can determine and evaluate the risks and opportunities associated with the audit objectives.

PREPARING FOR AN ISO AUDIT

Broadly, an ISO audit involves a cycle of four main activities:

1. PLANNING

The audit team leader should adopt a risk-based approach to planning the audit based on the information in the audit program and the documented information provided by the auditee.

An audit plan is prepared ahead of an audit. A Lead Auditor is appointed, who prepares the plan after consulting with Management. The audit plan includes the scope of the audit, which refers to the clauses and departments that are covered, the sampling rate, the audit dates and the auditors. An auditor collects the evidence and determines the findings. The auditor should be competent and authorised to conduct the audit. When performing a review of the auditee's documented information to prepare for the audit, clause 6.3.1 states that the review should take into account the context of the auditee's organisation, including its size, nature, and complexity, and its related risks and opportunities.

2. AUDITING

The audit team starts the audit with an Opening meeting with the Management. Auditors later audit the employees as per the audit plan and schedule. Nonconformity should be recorded after collecting the objective evidence for that nonconformity. A nonconformity refers to the non-fulfilment of a requirement of the chosen ISO standard. Objective evidence is evidence that exists and is verifiable. The Auditor should help the auditee (the company/department being audited) to identify the root cause of nonconformity and suggest a suitable corrective action for the nonconformity.

OPENING MEETING

The purpose of the opening meeting, according to clause 6.4.3 is to:

1. Confirm the agreement of all participants to the audit plan
2. Introduce the audit team and their roles
3. Ensure that all planned audit activities can be performed

An important topic to introduce will be the audit methods that manage risks that the organisation faces. These might only be brought to surface through the presence of the audit team members.

AUDIT COMMUNICATION

During the audit, the audit team leader should periodically communicate the progress, any significant findings, and any concerns to the auditee and audit client. Clause 6.4.4 states that evidence collected during the audit that suggests an immediate and significant risk should be reported without delay to the auditee and, as appropriate, to the audit client.

INFORMATION VERIFICATION

Clause 6.4.7 states that information relevant to the audit objectives, scope, and criteria, including information relating to interfaces between functions, activities, and processes, should be collected by means of appropriate sampling and should be verified, as far as practicable.

If during the collection of objective evidence, the audit team becomes aware of any new or changed circumstances, or risks or opportunities, these should be addressed by the team.

3. REPORTING

The audit report should provide a complete, accurate, concise, and clear record of the audit. Clause 6.5 states the report should note that audits by nature are a sampling exercise, and therefore, there is a risk that the audit evidence examined may not be representative.

The audit team records any observed nonconformity. During the closing meeting, a summary of the audit and the audit findings are presented to Management.

AUDIT FINDING

An “audit finding” is defined at clause 3.10 as the results of evaluating the collected audit evidence against audit criteria. Notes for that definition state that audit findings indicate conformity or nonconformity, and can lead to the identification of risks, opportunities for improvement, or recording of good practices.

NONCONFORMITY GRADING

According to clause 6.4.8, nonconformities can be graded depending on the context of the organisation and its risks. This grading can be quantitative (e.g., 1 to 5) and qualitative (e.g., minor, major). They should be reviewed with the auditee to obtain acknowledgement that the audit evidence is accurate and that the nonconformities are understood.

4. CORRECTIVE ACTION

The auditees are given a time frame to correct the nonconformity and document the details of the corrective action(s). The auditor should provide suggestions for improvement and any preventive actions that can be taken. The auditor verifies whether the corrective action taken is adequate and the nonconformity has been corrected.

TIPS FOR A SMOOTH INTERNAL AUDIT

The organisation and top management need to recognise the real worth of their internal auditors, nurture and develop those people, and make use of their insight.

These are the people who are completely familiar with the business management system and can significantly impact the bottom line if you listen to what they're saying.

- Internal auditors should attend Internal Auditor training to learn good practice and how to interpret and apply the requirements of the specific ISO standard.
- Our Internal Auditor training courses have been updated for the revised guidance in ISO 19011:2018.
- It is important to educate all staff about the benefits of internal auditing and the significant impact it can have on the organisation when it's used in a constructive manner.
- An auditor must be impartial and objective and cannot audit their own work.
- Learn to plan and perform your own audit with Risk ZA Training.

HOW RISK ZA CAN ASSIST YOU

TRAINING

We offer an extensive range of training courses that are facilitated by industry experts and registered educators. We are registered with the Southern African Auditor Training Certification Authority (SAATCA) and our courses include but are not limited to:

- Awareness training (in English, Afrikaans and isiZulu)
- Introductory and intermediate courses
- Advanced exposure to developing and implementing management arrangements to foster a culture of continual improvement
- Practical application of strategic elements of local and international best-practices
- Internal and supplier auditing
- Lead auditor training

View our Auditing Training courses here.

AUDITING

Auditing is an integral function of continual improvement and of high value and importance to an organisation's ability to improve. We promote and make use of risk-based auditing in conducting performance and conformance audits both for our clients or on their behalf. We conduct our audits with influence from ISO 19011 and ISO 17021 and supply the following Auditing services:

- First party internal audits
- Second-party supplier audits
- Third-party preparation audits (pre-certification)

CONSULTING

We specialise in consulting on all policies, procedures, processes, systems and other business activities. Our risk-based approach enables our consultants to effectively advise on restraints or potential areas of risk which could or are currently affecting the consistency of business processes and/or hindering profitability.

Our expertise includes compliance with international standards, corporate governance legislation and best practices and other enterprise-wide risk contributors.

Consulting Interventions include:

- Gap Analysis and Project Planning
- Steering Committees
- Policy Development
- Process Mapping and Evaluation
- Corrective Action Systems
- System Development and Implementation
- Documentation Creation, Review and Control

ONLINE LEARNING

Risk ZA is the regional channel and technical partner for Erudio Global, an Online ISO Training and Coaching provider. We offer innovative online learning solutions at a reduced rate throughout the African continent for busy professionals and people who are based in remote locations.

Online courses currently focus on ISO 9001:2015 Quality Management and ISO 14001:2015 Environmental Management. To sign-up for an online learning course click here.

SOFTWARE

Risk ZA offers a variety of software solutions specifically designed to suit your organisation's needs and support the document requirements of the ISO standard/s that your organisation has in place.

Click here to get in touch with our team and find the best software solution for you!

For more information about our wide-range of services, please contact our expert team on +27 (0) 31 569 5900 or email info@riskza.com.