PAPER PRESENTED AT THE 2011 SAATCA CONFERENCE
BY D.I. MUIR, PRINCIPAL, MANAGEMENT SYSTEM FACILITATORS

FDIS ISO 19011

GUIDELINES FOR AUDITING MANAGEMENT SYSTEMS

The drafting of the FDIS of ISO 19011 was undertaken by a joint working group of ISO TC176/SC3 and ISO TC207/SC2 although it was under the administration of ISO TC176/SC3/WG16 with the secretariat being AFNOR based in France. The writer had the pleasure to be the co-convenor of this project with a colleague, Mr Alister Dalrymple from France. It was quite significant that in one case we had a Scotsman representing South Africa and in the other an Irishman representing France on this project.

Members of working group 16 included representatives of other technical committees, for example ISO/TC207, ISO/JTC1/SC7, ISO/TC8, ISO/TC223 and for the first time the OHSAS group (the group concerned with occupational health and safety) and other interested parties for management systems were included within the technical committee who were drafting this international standard.

Looking at the major changes from the 2002 edition, the scope of the standard is widened from quality and environmental management systems auditing to auditing of any management systems. The relationship between ISO 19011 and ISO/IEC 17021 is clarified. Remote audit methods and the concept of risk are introduced. Confidentiality is added as a new principle. Clauses 5, 6 and 7 have been reorganised and additional information is contained in a new annex and this has resulted in the removal of the help boxes from the original text. Competence determination and an evaluation process is strengthened. Illustrative examples of discipline specific knowledge and skills are presented in a new annex. More information is intended to be available on an ISO public website, but as yet this has not come to fruition.

Turning now to ISO 19011 and ISO 17021 we could actually call these a consistent pair of standards. The revision of ISO 19011 provides guidance for all users including small and medium size organisations and concentrates on what are commonly termed internal audits (first party) and audits conducted by customers on their suppliers (second party).

While those involved in management system certification audits follow the requirements of ISO/IEC 17021: 2011, they may also find the guidance in ISO 19011 useful. There is a small table in ISO 19011 that is intended to provide guidance for internal auditing, supplier auditing and third party auditing in a non-certification environment and also with a reference to ISO/IEC 17021.

Like its predecessor, the new standard does not state requirements but provides guidance on the management of an audit programme, on the planning and conducting of an audit of the management system as well as on the competence and evaluation of an auditor and an audit team.

The international standard is intended to apply to a broad range of potential users including auditors, organisations implementing management systems and organisations needing to conduct audits of management systems for contractual or regulatory reasons. Users of the standard can, however, apply this guidance in developing their own audit related requirements. The guidance in the standard may also be used for the purpose of self-declaration and be useful to organisations involved in auditor training or personnel certification. The guidance in the standard is intended to be flexible. As indicated at various points in the text, the use of the guidance can differ according to the size and level of maturity of an organisation's management system and to the nature and complexity of the organisation to be audited as well as the objectives and scope of the audits to be conducted.

The new standard also introduces the concept of risk to management systems auditing. The approach adopted relates both to the risk of the audit process not achieving its objectives and to the potential of the audit to interfere with the auditee's activities and processes. It does not provide specific guidance on the organisation's risk management process, but recognises that organisations may focus audit effort on matters of significance to the management system.

The new standard deals, in part, with the complex problem known as integrated management system audits. FDIS 19011 takes the approach that when two or more management systems of different disciplines are audited together, this is termed a combined audit. Where these systems are integrated into a single management system, the principles and processes of auditing are the same as for a combined audit. This is a different definition from that in the new version of ISO/IEC 17021: 2011 where that standard actually has a definition of an integrated audit – albeit in a note.

The scope of ISO 19011: 2011 states: "This standard provides guidance on auditing management systems including the principles of auditing, managing an audit programme and conducting management system audits as well as guidance on the evaluation of competence of individuals involved in the audit process including the person managing the audit programme, auditors and audit teams. It is applicable to all organisations needing to conduct internal or external audits of management systems or manage an audit programme".

"The application of the international standard to other types of audits is possible, provided that special consideration is given to the specific competence needed".

The standard is still principles based. The principle of ethical conduct in the 2002 version has been reworded as: "Integrity: the foundation of professionalism". Auditors and the person managing an audit programme should:

- perform their work with honesty, diligence and responsibility;
- observe and comply with any applicable legal requirements;
- demonstrate their competence while performing their work;
- perform their work in an impartial manner, i.e. remain fair and unbiased in all their dealings; and
- be sensitive to any influences that may be exerted on their judgment while carry out an audit.

A new principle was added: "Confidentiality; which is the security of information. Auditors should exercise discretion in the use and protection of information acquired in the course of their duties. Audit information should not be used inappropriately for personal gain by the auditor or the audit client or in a manner detrimental to the legitimate interest of the auditee. This concept includes the proper handling of sensitive or confidential information".

In managing an audit programme, priority should be given to allocating audit programme resources to audit those matters of significance within the management system. These may include the key characteristics of product quality or hazards related to health and safety or significant environmental aspects and their control. There is a note to this general clause – "this concept is commonly know as risk based auditing", but the standard does not give any further guidance on risk. This clause begins the introduction of risk to the audit process in ISO 19011.

In evaluating audit programme risks, there are many different risks associated with an audit programme that may affect the achievement of the audit objectives. These risks may be associated with:

- planning, for example failing to set relevant objectives and determining the extent of the audit programme;
- resources, for example allowing insufficient time for developing the audit programme or conducting an audit;
- selection of the audit team, for example the team does not have the collective competence to conduct audits effectively;

These are some of the examples of risk in the new standard.

There are some others:

- implementation risks, for example ineffective communication of the audit programme;

- records and their controls, for example failure to adequately protect audit records to demonstrate audit programme effectiveness;
- monitoring, reviewing and improving the audit programme, for example ineffective monitor of audit programme outcomes.

The process of auditing has not radically changed since the 2002 version and the diagram and the process remains the same. When we come to preparing the audit plan, however, the standard has some new advice. For combined audits, particular attention should be given to the interactions between operational processes and the competing objectives and priorities of the different management systems. The scale and content of the audit plan may differ, for example between initial and subsequent audits and also between internal and external audits. The audit plan should be sufficiently flexible to permit changes which can become necessary as the audit activities progress.

Opening meeting: The purpose of the opening meeting is to confirm the agreement of all parties (for example auditee, audit team) to the audit plan, introduce the audit team and ensure that all planned audit activities can be performed. The degree of detail should be consistent with the familiarity of the auditee with the audit process. In many instances, for example internal audits in a small organisation, the opening meeting may simply consist of communicating that an audit is being conducted and explaining the nature of the audit. For other audit situations the meeting may be formal and records of attendance should be kept. The meeting should be chaired by the audit team leader. This is where recognition of small business and more informal auditing takes us away from the more formal stereotype checklist type of auditing that we have been used to especially in conducting opening and closing meetings.

A further example in the guidance is communication during an audit: "Where the available audit evidence indicates that the audit objectives are unattainable, the audit team leader should report the reasons to the audit client and the auditee to determine appropriate action. Such action may include reconfirmation or modification of the audit plan, changes to the audit objectives or audit scope or even termination of the audit. Any need for changes to the audit plan which may become apparent as auditing activities progress should be reviewed with and approved as appropriate by the person managing the audit programme and the auditee". Similarly when audit conclusions are being prepared they can address such issues as:

- "the extent of conformity and acknowledgement of strength of the management system with the audit criteria, including the effectiveness of the management system in meeting the stated objectives;
- the effect of implementation, maintenance and improvement of the management system;
- the capability of the management review process to ensure the continuing suitability, adequacy, effectiveness and improvement of the management system;
- achievement of audit objectives, coverage of audit scope and fulfilment of audit criteria".

The most radical change in the new standard is related to competence and evaluation of auditors. Confidence in the audit process and the ability to achieve its objectives depends on the competence of those individuals who are involved in planning and conducting audits including auditors and audit team leaders. Competence should be evaluated through a process that considers personal behaviour and the ability to apply the knowledge and skills gained through education, work experience, auditor training and audit experience. Some of the knowledge and skills described in the standard are common to auditors of any management system discipline, others are specific to individual management system disciples. Each auditor in the audit team does not need to have the same competence, however, the overall competence of the audit team needs to be sufficient to achieve the audit objectives". This introduces now the concept of team competence. In the old version of the standard, each auditor in the team had to be fully competent for every aspect of the audit. The new version now highlights the concept of team competence.

"The evaluation of auditor competence: The evaluation of auditor competence should be planned, implemented and documented in accordance with the audit programme including its procedures to provide an outcome that is objective, consistent, fair and reliable. The evaluation process should include four main steps:

- determine the competence of audit personnel to fulfil the needs of the audit programme;
- establish the evaluation criteria;
- select the appropriate evaluation method; and
- conduct the evaluation".

"Personal behaviour: Auditors should possess the necessary qualities to enable them to act in accordance with the principles of auditing as described in clause 4 of the standard. New behaviours added in the 2011 version include being:

- self-reliant, i.e. able to act and function independently whilst interacting effectively with others;
- able to act responsibly and ethically even though those actions may not always be popular and may sometime result in disagreement or confrontation;
- open to improvement, i.e. willing to learn from situations, striving for better audit results;
- culture sensitive, i.e. observant and respectful to the culture of the auditee;
- collaborative, i.e. effectively interacting with others including audit team members and the auditee's personnel.

Discipline and sector specific knowledge and skills of management system auditors

Auditors should have the discipline and sector specific knowledge and skills that are appropriate for auditing a particular type of management system sector. Each auditor in a team does not need to have the same competence, however, the overall competence of the audit team needs to be sufficient to achieve the audit objectives.

Discipline specific knowledge related to the particular sector, nature of operations or workplace being audited sufficient for the auditor to evaluate the auditee's activities, process and products (goods and services).

Risk management principles, methods and techniques relevant to the discipline and sector to enable the auditor to evaluate and control the risks associated with the audit programme".

Guidance and illustrated examples of discipline specific knowledge and skills of auditors is provided in an annex in the new standard. This is new information that was not in the 2002 version.

"Knowledge and skills for auditing management systems addressing multiple disciplines

Auditors who intend to participate as an audit team member in auditing management systems addressing multiple disciplines should have the competence necessary to audit at least one of the management system disciplines and an understanding of the interaction and synergy between the different management systems. Audit team leaders conducting audits of management systems addressing multiple disciplines should understand the requirements of each of the management system standards and recognise the limits of their knowledge and skills in each of the disciples. Again this is new guidance that was not in the 2002 version.

"Achieving auditor competence

Auditor knowledge and skills can be acquired using a combination of the following:

- formal education or training and experience that contributed to the development of knowledge and skills in the management system discipline and sector the auditor intends to audit;
- training programmes that cover generic auditor knowledge and skills;

- experience in a relevant technical managerial or professional position involving the exercise of judgment, decision making, problem solving and communication of managers, professionals, peers, customers and other interested parties;
- audit experience acquired under the supervision of an auditor in the same discipline".

It will be seen in the new standard that there is no more table 1. However, when it comes to establishing the auditor evaluation criteria, note must be taken of the following: "The criteria should be qualitative (such as having demonstrated personal behaviour, knowledge or the performance of the skills in training or in the workplace) and quantitative (such as years of work experience and education, number of audits conducted and hours of audit training). The person managing the audit programme should establish one or more procedures assuring the competence of auditors and audit team leaders. The evaluation of auditor competence should be planned, implemented and documented in accordance with the appropriate as you were with the audit programme, including its procedures, to provide an outcome as objective, consistent, fair and reliable". Although there is no more table 1 the guidance that was in the original table 1 has manifested itself again in the new standard, except this time the equivalent of table 1 is required to be implemented and demonstrated by the person managing the audit programme.

"Maintaining and improving auditor competence

Auditors and audit team leaders should continually improve their competence. Auditors should maintain their auditing competence through regular participation in management system audits and continual professional development. Continual professional development involves the maintenance and improvement of competence. This may be achieved through means such as additional work experience, training, private study, coaching, attendance at meetings, seminars and conferences or other relevant activities. The continual professional development activities should take into account the changes in the needs of the individual and the organisation responsible for the conduct of the audit, the practise or auditing, relevant standards and other requirements".

There is a new appendix as an informative annex in ISO 19011 and this is guidance and illustrative examples of discipline specific knowledge and skills of auditors. Appendix A in the standard gives generic examples of discipline specific knowledge and skills for auditors of management systems and are intended as guidance to assist the person managing the audit programme to select or evaluate auditors. Other examples of discipline specific knowledge and skills for auditors may be developed for management systems other than these examples. It is suggested that such examples follow the same general structure where possible in order to ensure comparability.

Guidance and illustrative examples of discipline specific knowledge and skills of auditors:

- transportation safety management;
- environmental management;
- quality management;
- records management;
- resilience, security, preparedness and continuity management;
- information security;
- occupational health and safety management.

Annexure B which is also informative gives additional guidance for auditors for planning and conducting audits:

- applying audit methods;
- selecting sources of information;
- conducting document review;
- preparing work documents;
- sampling;
- guidance for visiting an auditee's location;

- conducting interviews;
- audit findings.

To assist with competence challenges in third party certification auditing, there is a joint programme by RABQSA and IRCA based on ISO/IEC 17021: 2011. These two organisations are auditor certification/registration bodies and they plan to offer competence based certification of auditors for specific technical areas. The working group concerned with ISO 17021 were quite pleased with that approach, but could not allow it to happen fully exclusively for the registration of auditors only. It has been agreed that the tools to be used by these auditor registration bodies will also be made available to certification and accreditation bodies. At present there are no similar plans for first, second or third party non-certification auditing and perhaps SAATCA will have to decide if there is a need to make any changes to the current SAATCA criteria for the registration of auditors of management systems.

Publication of the new standard

The international ballot on FDIS 19011 for two months started on 28 July 2011. The vote closes on 4 October 2011 and it is expected that the standard will be published before the end of 2011 or early 2012. The South African national standard is following a parallel course and therefore should also be published within days of the publication of the ISO standard.