IRCA Briefing note: ISO/FDIS 19011:2011 – Guidelines for auditing management systems

Introduction

The International Register of Certificated Auditors (IRCA) has prepared this briefing note to communicate to IRCA Certificated Auditors, IRCA Approved Training Organisations and other interested parties our understanding of ISO/FDIS 19011:2011.

The content of this briefing note is provided in good faith and is the opinion of the IRCA. It should not be reproduced nor used for commercial purposes. IRCA Certificated Auditors and IRCA Approved Training Organizations are advised to familiarise themselves with ISO 19011:2011 when it is published.

- FDIS released to the National Standards bodies July 2011
- ISO 19011:2011 expected to be issued October 2011

Since initial publication in 2002 a number of new management system standards have been published. This has resulted in a need to consider a broader scope of management system auditing as well as providing guidance that is more generic. This is reflected in the revised title "Guidelines for auditing management systems" and in the content.

ISO 19011:2011 provides guidance for all users, including small and medium sized organizations and concentrates on what are commonly termed internal (first party) and second party audits as often conducted by customers on their suppliers.

Relationship between ISO/IEC 17021:2011 and ISO 19011:2011

<table>
<tr><th colspan="3">ISO 19011 is intended to provide useful guidance in:</th></tr>
<tr><th>Internal auditing</th><th colspan="2">External auditing</th></tr>
<tr><td rowspan="2">Commonly called 1st party audit</td><td rowspan="2">Supplier auditing
commonly called 2nd party audit</td><td>3rd party auditing
e.g. legal, certification and similar purposes</td></tr>
<tr><td>ISO/IEC 17021:2011
Conformity assessment-Requirements for bodies providing audit and certification of management systems</td></tr>
</table>

2nd Floor North
Chancery Exchange
10 Furnival Street
London
EC4A 1AB
Tel +44 (0)20 7245 6833
Fax +44 (0)20 7245 6755
Email irca@irca.org
Website www.irca.org

With the publication of ISO 17021:2011 we now have two independent standards:

- ISO 19011:2011 - Guidelines for auditing management systems.

And

- ISO 17021:2011 - Conformity assessment - Requirements for bodies providing audit and certification of management systems.

Some may view the guidance in ISO 19011:2011 as a substantial change. Others may think it largely captures good practices already implemented. The IRCA's view is that publication of ISO 19011:2011 provides auditors, organizations implementing management systems and organizations needing to conduct audits of management systems an opportunity to re-assess their own practices and identify improvement opportunities.

Summary of the changes within ISO 19011:2011

Overview

ISO 19011 has been revised to provide persons involved in management system auditing with good audit practice guidance relevant to today's environment where many organizations operate a management system covering multiple disciplines, for example quality, environment, occupational health and safety and information security etc.

The **Principles of auditing** on which the guidance is based have been revised and expanded to include the new principle of 'Confidentiality – security of information'. A principle that requires auditors to be prudent in the use and protection of information acquired in the course of their duties.

The main body of ISO 19011:2011 sets out good practice for **Managing an Audit Programme** and **Performing an Audit**. Updated to reflect current thinking and in parts expanded significantly. These sections provide detailed guidance; intended to be used flexibly according to the size, level of maturity of an organization's management system, the nature and complexity of the organization to be audited. The concept of risk in auditing is introduced. Some guidance is given on combined audits, where two or more management systems of different disciplines are audited together (e.g. EMS and OHSAS). Also, the use of technology in remote auditing is acknowledged. For example conducting remote interviews and reviewing records remotely. Although significantly rewritten, the overall approach to managing an audit programme and planning and conducting audits described in these two sections is consistent with the previous issue and with requirements of ISO 17021:2011.

2nd Floor North
Chancery Exchange
10 Furnival Street
London
EC4A 1AB
Tel +44 (0)20 7245 6833
Fax +44 (0)20 7245 6755
Email irca@irca.org
Website www.irca.org

Changes have been introduced in the guidance on **Competence and evaluation of auditors**. As would be expected given that ISO 19011:2011 addresses auditing management system covering multiple disciplines some of these are wide ranging. The significant changes include:

- ISO 19011:2011 identifies that necessary auditor competence comprises generic knowledge and skills of management systems, plus discipline (e.g. EMS) and sector (e.g. aerospace) knowledge and skills. Annex A (informative) gives examples of discipline-specific knowledge and skills of auditors, including:
    - Transportation safety management
    - Environmental management
    - Quality management
    - Records management
    - Resilience, security, preparedness and continuity management
    - Information security
    - Occupational health and safety

  No guidance is given on sector specific knowledge and skills of auditor. These may be developed later and published separately.

- ISO 19011:2002 gave guidance on education, work experience, auditor training and audit experience that contribute to development of the knowledge and skills needed to perform audits and lead audit teams. ISO 19011:2011 also gives guidance on knowledge and skills of management system auditors and an audit team leader but no longer makes reference to auditors having completed education, work experience, auditor training and audit experience.

This change recognises that education, work experience, training and audit experience are enablers to competence, which ISO 19001:2011 and ISO 17021:2011 define as 'ability to apply knowledge and skills to achieve intended results'. Also, ISO 19011:2011 and ISO 17021:2011 recognise that competence needs to be evaluated, which can be done in a variety of ways, for example a combination of testing and examination, interview and observed audits.

2nd Floor North
Chancery Exchange
10 Furnival Street
London
EC4A 1AB
Tel +44 (0)20 7245 6833
Fax +44 (0)20 7245 6755
Email irca@irca.org
Website www.irca.org

Headquarters and Registered Office:
2nd Floor North
Chancery Exchange
10 Furnival Street
London
EC4A 1AB

Detail review

1. **Scope** – no significant changes.
2. **Informative references** – previous reference to terms and definitions given in ISO 9000 (QMS) and ISO 14050 (EMS) deleted.
3. **Terms and definitions** – definitions for Observer and Guide introduced and also for Risk. The term risk is used in ISO 19011:2011 in context of "risk-based auditing" and also "audit programme risks". The definition of competence is revised and although the change in wording appears slight it requires organisations to determine competence to achieve intended results. The starting point for which is to define the intended results for the various activities involved in managing an audit programme and performing audits. This change is consistent with ISO 17021:2011.
4. **Principles of auditing** – expanded from five to six. Principles (a) – (d) relate to auditors and the person managing the audit programme. Principles (e) and (f) relate to the audit.
    - **Integrity** - *the foundation of professionalism*. Replaces and expands the previous principle of Ethical conduct.
    - **Fair presentation –** *the obligation to report truthfully and accurately*. Minor expansion.
    - **Due professional care** – *the application of diligence and judgement in auditing*. 'Having the necessary competence is an important factor' is replaced with 'An important factor in carrying out their work with due professional care is having the ability to make reasoned judgement in all audit situations'.
    - **Confidentiality** – *security of information*. A new principle that addresses the need for auditors to exercise discretion in the use and protection of information acquired in the course of their duties. The principle refers to inappropriate use of such information for personal gain or in a manner detrimental to the legitimate interests of the auditee.
    - **Independence** – *the basis for the impartiality of the audit and objectivity of audit conclusions*. Provides more specific guidance on the extent of independence that needs to be achieved, whilst recognising that in small organizations it may be difficult for internal auditors to be fully independent. Now refers to internal auditors being independent from the operating managers of the function being audited. Reflects the interpretation of independence that certification bodies generally apply.
    - **Evidence-based approach** – *the rational method for reaching reliable and reproducible audit conclusions in a systematic way*. Minor rewording.

2nd Floor North
Chancery Exchange
10 Furnival Street
London
EC4A 1AB
Tel +44 (0)20 7245 6833
Fax +44 (0)20 7245 6755
Email irca@irca.org
Website www.irca.org

5. **Managing an audit programme –** Considerable revision. Clarity of the guidance has been improved, structuring the section to follow a process flow:
   - 5.1 - General
   - 5.2 – Establishing the audit programme objectives
   - 5.3 – Establishing the audit programme
   - 5.4 – Implementing the audit programme
   - 5.5 – Monitoring the audit programme
   - 5.6 – Reviewing and improving the audit programme

   General – this section recognises that an organization may implement a number of management system standards. Where the previous issue of ISO 19011 referred to an organization establishing one or more audit programmes ISO/FDIS 19011:2011 refers to an audit programme that can include audits considering one or more management system standards. In practical terms this makes little difference.

   This section refers to allocating audit resources to audit those matters of significance within the management system. It notes that this concept is commonly known as risk-based auditing. This reflects the requirements of many management system standards, for example ISO 9001:2008, although the term risk is not always used.

   Establishing the audit programme objectives – section title revised; otherwise little practical change although the list of considerations to take account of when establishing audit programme objectives has been extended; now includes for example results of previous audits and maturity of the management system being audited. Also, for clarity in structuring the content to follow the process flow guidance on the ***extent of an audit programme*** has been transferred to section 5.3.3.

   Establishing the audit programme – revision of what was previously titled 'Audit programme responsibilities, resources and procedures'. New to this issue is guidance on 'Competence of the person managing the audit programme'. Also new is guidance on 'Identifying and evaluating audit programme risks'. For example risks associated with ineffective communication of the audit programme.

   Implementing the audit programme – more extensive guidance is given, including describing more clearly what the person managing the audit programme should do to implement it.

   The need to 'Define the objectives, scope and criteria for an individual audit' is a sub-section. This identifies that each audit should have a clear objective, for example 'identification of areas for potential improvement of a management system'. This addresses weakness often found in audit systems where audits are scheduled and carried out with no clearly defined purpose or objective.

2nd Floor North
Chancery Exchange
10 Furnival Street
London
EC4A 1AB
Tel +44 (0)20 7245 6833
Fax +44 (0)20 7245 6755
Email irca@irca.org
Website www.irca.org

This section also highlights issues to consider when two or more management systems of different disciplines are audited together.

There is a new sub-section '**Selecting the audit methods'** and additional guidance on this is given in Annex B. The previous simplistic approach to audit methods of on-site or off-site has been revised to take account of the use of technology in remote auditing. For example conducting remote interviews and accessing records remotely.

Other sub-sections include:

- Selecting the audit team members
- Assigning responsibilities for an individual audit to the team leader
- Managing the audit programme outcome
- Managing and maintaining audit programme records

In summary, section 5.4 of ISO 19011:2002 has been extensively rewritten to provide comprehensive guidance to what was previously a list of headline topics that needed to be addressed when implementing the audit programme. Section 5.5 of ISO 19011:2002 – Audit programme records is now part of section 5.4

Monitoring the audit programme and **Reviewing and improving the audit programme** - These two sections replace what previously was one, Audit programme monitoring and reviewing. Minor expansion and reference to consider the need to:

- evaluate the performance of audit team members
- consider as part of a review, alternative or new auditing methods
- review the effectiveness of the measures to address the risks associated with the audit programme
- review confidentiality and information security issues relating to the programme

6. **Performing an audit** – As with section 5, the guidance has been improved and in parts more detail is given. The section is structured to follow the audit process flow, which is largely as it was presented in ISO 19011:2002.

- 6.1 General
- 6.2 Initiating the audit
- 6.3 Preparing audit activities
- 6.4 Conducting the audit activities
- 6.5 Preparing and distributing the audit report
- 6.6 Completing the audit
- 6.7 Conducting audit follow-up

Some, but not all, of the changes are described below to illustrate the extent and nature of the revisions.

2nd Floor North
Chancery Exchange
10 Furnival Street
London
EC4A 1AB
Tel +44 (0)20 7245 6833
Fax +44 (0)20 7245 6755
Email irca@irca.org
Website www.irca.org

Initiating the audit – no longer refers to appointing the team leader or defining audit objectives, scope and criteria as these are dealt with under Managing an audit programme. Now focuses on 'Establishing initial contact with the auditee' and 'Determining the feasibility of the audit'.

Preparing audit activities – combines what were previously two sections 'Conducting document review' and 'Preparing for the on-site audit activities'. Now covers:

- Performing document review in preparation for the audit
- Preparing the audit plan
- Assigning work to the audit team
- Preparing work documents

As described in ISO 19011:2011, the purpose of performing document review for preparation is to gather information to prepare audit activities and applicable work documents. Also to establish an overview of the extent of the system documentation to detect possible gaps.

What some have previously referred to as a documentation review - reviewing documentation to determine conformity of the system with audit criteria - is now dealt with as part of conducting audit activities.

Conducting audit activities – now covers:

- Conducting the opening meeting
- Performing document review while conducting the audit
- Communicating during the audit
- Assigning roles and responsibilities of guides and observers
- Collecting and verifying information
- Generating audit findings
- Preparing audit conclusions
- Conducting the closing meeting

Preparing and distributing the audit report – no substantial changes.

Completing the audit – no substantial changes.

Conducting audit follow-up – no substantial change. Text clarifies that post audit actions may be corrections, corrective action, and preventive or improvement actions. Reference to corrections added.

7. **Competence and evaluation of auditors** – Some significant changes have been introduced, as would be expected given that ISO 19011:2011 addresses auditing management system covering multiple disciplines. New guidance includes:

   Determining auditor competence to fulfil the needs of the audit programme – a section that identifies factors to consider when deciding appropriate knowledge and skills, for example the management system disciplines to be audited. This section then goes on to describe:

2nd Floor North
Chancery Exchange
10 Furnival Street
London
EC4A 1AB
Tel +44 (0)20 7245 6833
Fax +44 (0)20 7245 6755
Email irca@irca.org
Website www.irca.org

Personal behaviour – behaviours auditors should display during the performance of audit activities, for example observant, perceptive, open to improvement, culturally sensitive and collaborative. Some expansion on ISO 19011:2002.

Knowledge and skills – section comprises:

- **Generic knowledge and skills of management system auditors** – a section expanded to incorporate knowledge and skills needed to audit multiple discipline management systems and implement other parts of ISO 19011:2011. For example, understand the types of risk associated with auditing, have knowledge of organizational types, general business and management concepts, processes and related terminology, including budgeting and management of personnel. Many of the additions in this section address the need for auditors to be able to position discipline and sector requirements and audit findings in the wider context of the organization's business activities, governing agencies, business environment, legal and contractual requirements and management's policies and intentions for the organization.
- **Discipline and sector specific knowledge and skills of management system auditor** – (discipline, for example EMS and sector, for example aerospace). ISO 19011:2002 provided guidance for quality management system auditors and environmental management system auditors, each having its own section providing guidance on auditor knowledge and skill requirements. In ISO 19011:2011 these two sections are replaced by one that identifies knowledge and skills that need to be applied to all management systems. For example, knowledge of:
  - Legal requirements relevant to the specific discipline.
  - Fundamentals of the discipline and the application of business and technical discipline-specific methods, techniques, processes and practices sufficient to enable the auditor to examine the management system and generate appropriate audit findings and conclusions.
  - 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.

  ISO 19011:2011 **Annex A** provides guidance on discipline-specific knowledge and skills of auditors for:
  - Transportation safety management
  - Environmental management
  - Quality management
  - Records management
  - Resilience, security, preparedness and continuity management
  - Information security
  - Occupational health and safety

2nd Floor North
Chancery Exchange
10 Furnival Street
London
EC4A 1AB
Tel +44 (0)20 7245 6833
Fax +44 (0)20 7245 6755
Email irca@irca.org
Website www.irca.org

No guidance is given on sector specific knowledge and skills. These could be developed later and published separately.

- **Generic knowledge and skills of an audit team leader** – now includes knowledge and skills to:
  - Balance the strengths and weaknesses of the individual audit team members
  - Develop a harmonious working relationship among the audit team members
  - Manage the uncertainty of achieving audit objectives
- **Knowledge and skills for auditing management systems addressing multiple disciplines** – previously limited to auditors who audit both quality and environmental management systems and quite prescriptive. Now describes in principle the knowledge and skill requirements. For example, understanding of the interaction and synergy between the different management systems.

Achieving auditor competence – a section that largely replaces previous quite prescriptive guidance. For example ISO 19011:2002 refers to five years work experience and twenty days of audit experience etc. Now acknowledges that auditor knowledge and skills can be acquired using a combination education, auditor training programmes, experience in relevant technical, managerial or professional positions and audit experience without detailing specific guidance.

Auditor evaluation – ISO 19011:2011 gives guidance on:

- **Establishing the auditor evaluation criteria** – as previous, these should be qualitative, for example having demonstrated audit skills, and quantative, for example number of audits conducted.
- **Selecting the appropriate auditor evaluation method** – as previous, guidance is given on evaluation methods, for example review of records, feedback, interview etc.
- **Conducting auditor evaluation –** a simple statement that information collected about the person should e compared against criteria set. And when the criteria set are not met additional training, work or audit experience and subsequent re-evaluation should be performed.

Overall the guidance given is largely unchanged; however its presentation has been simplified and ease of understanding improved.

Maintaining and improving auditor competence – largely unchanged in stating that auditors and team leaders should continually improve their competence through participation in management system audits and continual professional development.

The guidance makes it clear that the person managing the audit programme should establish suitable mechanisms for the continual evaluation of the performance of the auditors, and team leaders.

2nd Floor North
Chancery Exchange
10 Furnival Street
London
EC4A 1AB
Tel +44 (0)20 7245 6833
Fax +44 (0)20 7245 6755
Email irca@irca.org
Website www.irca.org

Annex A (informative) **– Illustrative examples of discipline-specific knowledge and skills of auditors.**

Provides guidance that organizations may choose use to support the development of their own auditor competence criteria and selection of auditors.

Annex B (informative) **– Additional guidance for auditors planning and conducting audits.**

More practical guidance, of a type often given in Auditor/Lead Auditor training courses. Extracts from Annex B include for example:

- **Selecting sources of information** – a list of sources of information to select from, e.g. interviews, observation of activities, databases and websites.
- **Conducting document review** – a list of things auditors should consider, e.g. if the information in the documents is complete, correct, consistent and current.
- **Preparing working documents** – considerations for each document, e.g. who will be the user of this work document?
- **Sampling** – guidance on selecting sampling methods, judgement-based sampling, statistical sampling.
- **Guidance for visiting auditee's location** – practical guidance on planning and conducting on-site activities, e.g. confirm with the auditee that any required PPE will be available, if taking photographs ask for authorisation from management in advance and consider security and confidentiality matters.

Other guidance covers conducting interviews, audit findings (determining audit findings, recording conformities and recording nonconformities) and dealing with findings related to multiple criteria.

END

2nd Floor North
Chancery Exchange
10 Furnival Street
London
EC4A 1AB
Tel +44 (0)20 7245 6833
Fax +44 (0)20 7245 6755
Email irca@irca.org
Website www.irca.org