Running an Effective Internal Audit Program

Paul Cartlidge, BSc
QMS Lead Auditor

GHEST Symposium
September 28, 2013
Disclosures

- QMS Lead Auditor performing audits for a registrar
- Owns and operates consulting company providing auditing and quality management consulting services
Registrar Activities

- SAI Global is an accredited registrar by the Standards Council Of Canada
- Provides registration/certification services to international standards in numerous industries:
  - ISO 9001 (applicable in many industries)
  - Automotive (ISO 16949)
  - Medical Devices (ISO 13485)
  - Environmental Management System (ISO 14001)
  - Occupational Health and Safety (ISO 18001)
  - And more…
Internal Audits ... Why?

- Requirement of most quality management standards and regulations including:
  - ISO 9001
  - Z902 Blood and Blood Components
  - Cells, Tissues and Organs Regulations
  - Ontario Laboratory Accreditation Standards
  - FACT Standards
  - AABB Standards
Internal Audits ... REALLY Why?

- Opportunity to review operations and evaluate compliance against standard requirements
- Opportunity to review and improve operational processes
Internal Audits ... HELP!!!

- How do I...
  - Get started?
  - Determine the structure of the internal audit program?
  - Decide who performs the audits?
  - Establish audit criteria?
  - Develop tools for performing the audits?
  - Report the findings?
Quest for a holy grail??
There is HOPE....

INTERNATIONAL STANDARD
ISO 19011

Guidelines for auditing management systems
Lignes directrices pour l’audit des systèmes de management
Scope of ISO 19011

- Provides guidance on auditing management systems, including:
  - the principles of auditing
  - managing an audit program and conducting management system audits
  - guidance on the evaluation of competence of individuals involved in the audit process, including the person managing the audit program, auditors and audit teams.

- It is applicable to all organizations that need to conduct internal or external audits of management systems or manage an audit program.
Application of ISO 19011

- Can be used as guidance or followed in full for establishing an audit program
- Well adapted for both internal audits and external audits
- Excellent terms and definitions, overall audit program structure and considerations
Principles of Auditing – the 6 Commandments

- Integrity
- Fair Presentation
- Due Professional Care
- Confidentiality
- Independence
- Evidence-based Approach
**Integrity: the foundation of professionalism**

- Auditors and the person managing an audit program 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;
  - be sensitive to any influences that may be exerted on their judgement while carrying out an audit.
Principle of Auditing # 2

**Fair presentation:** the obligation to report truthfully and accurately

- Audit findings, audit conclusions and audit reports should reflect truthfully and accurately the audit activities.
- Significant obstacles encountered during the audit and unresolved diverging opinions between the audit team and the auditee should be reported.
- The communication should be truthful, accurate, objective, timely, clear and complete.
Principle of Auditing #3

Due professional care: the application of diligence and judgement in auditing

- Auditors should exercise due care in accordance with the importance of the task they perform and the confidence placed in them by the audit client and other interested parties.
- An important factor in carrying out their work with due professional care is having the ability to make reasoned judgements in all audit situations.
Confidentiality: 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 interests of the auditee.
- This concept includes the proper handling of sensitive or confidential information.
Principle of Auditing #5

Independence: the basis for the impartiality of the audit and objectivity of the audit conclusions

- Auditors should be independent of the activity being audited wherever practicable, and should in all cases act in a manner that is free from bias and conflict of interest.
- For internal audits, auditors should be independent from the operating managers of the function being audited.
- Auditors should maintain objectivity throughout the audit process to ensure that the audit findings and conclusions are based only on the audit evidence.
- For small organizations, it may not be possible for internal auditors to be fully independent of the activity being audited, but every effort should be made to remove bias and encourage objectivity.
Evidence-based approach: the rational method for reaching reliable and reproducible audit conclusions in a systematic audit process

- Audit evidence should be verifiable.
- It will in general be based on samples of the information available, since an audit is conducted during a finite period of time and with finite resources.
- An appropriate use of sampling should be applied, since this is closely related to the confidence that can be placed in the audit conclusions.
Managing an Audit Program

- General Considerations:
  - Standards to be audited
  - Resources to support audit program
  - Responsibility for management of the audit program
  - Audit criteria and methods
  - Monitoring the effectiveness of the audit program
Establishing the audit program objectives

- The top management should ensure that the audit program objectives are established to direct the planning and conduct of audits and should ensure the audit program is implemented effectively.
- Audit program objectives should be consistent with and support management system policy and objectives.
Considerations for audit program objectives

- management priorities
- commercial and other business intentions
- characteristics of processes, products and projects
- management system requirements
- legal and contractual requirements
- supplier evaluations
- needs and expectations of interested parties, including customers
- auditee’s level of performance
- results of previous audits
- level of maturity of the management system being audited
Establishing the audit program

Roles and responsibilities of the person managing the audit program:

- establish the extent of the audit program;
- identify and evaluate the risks for the audit program;
- establish audit responsibilities;
- establish procedures for audit programs;
- determine necessary resources;
- ensure the implementation of the audit program, including the establishment of audit objectives, scope and criteria of the individual audits, determining audit methods and selecting the audit team and evaluating auditors;
- ensure that appropriate audit program records are managed and maintained;
- monitor, review and improve the audit program.
Establishing the audit program

Competence of the person managing the audit program:

- Need appropriate competence to manage the audit program and its associated risks effectively and efficiently, as well as knowledge and skills in the following areas:
  - audit principles, procedures and methods;
  - management system standards and reference documents;
  - activities, products and processes of the auditee;
  - applicable legal and other requirements relevant to the activities and products of the auditee;
  - customers, suppliers and other interested parties of the auditee, where applicable.

- Engage in appropriate continual professional development activities to maintain the necessary knowledge and skills to manage the audit program.
Establishing the extent of the audit program:

- The person managing the audit program should determine the extent of the audit program, which can vary depending on the size and nature of the auditee.
- Evaluate the nature, functionality, complexity and the level of maturity of, and matters of significance to, the management system to be audited.
Establishing the audit program

Identifying and evaluating audit program risks:

- The person managing the program should consider risks in its development, including:
  - planning, e.g. failure to set relevant audit objectives and determine the extent of the audit program;
  - resources, e.g. allowing insufficient time for developing the audit program or conducting an audit;
  - selection of the audit team, e.g. the team does not have the collective competence to conduct audits effectively;
  - implementation, e.g. ineffective communication of the audit program;
  - records and their controls, e.g. failure to adequately protect audit records to demonstrate audit program effectiveness;
  - monitoring, reviewing and improving the audit program, e.g. ineffective monitoring of audit program outcomes.
Establishing the audit program

Establish procedures for the audit program, including:

- planning and scheduling audits considering audit program risks;
- ensuring information security and confidentiality;
- assuring the competence of auditors and audit team leaders;
- selecting appropriate audit teams and assigning their roles and responsibilities;
- conducting audits, including the use of appropriate sampling methods;
- conducting audit follow-up, if applicable;
- reporting to the top management on the overall achievements of the audit program;
- maintaining audit program records;
- monitoring and reviewing the performance and risks, and improving the effectiveness of the audit program.
Establishing the audit program

Identifying audit program resources:

- When identifying resources for the audit program, consider:
  - the financial resources necessary to develop, implement, manage and improve audit activities
  - audit methods
  - the availability of auditors and technical experts having competence appropriate to the particular audit program objectives
  - the extent of the audit program and audit program risks
  - travelling time and cost, accommodation and other auditing needs
  - the availability of information and communication technologies
Implementing the audit program

**General Considerations:**

- communicating the audit program to relevant parties (e.g. management and auditees) and informing them periodically of its progress;
- defining objectives, scope and criteria for each individual audit;
- coordinating and scheduling audits and other activities relevant to the audit program;
- ensuring the selection of audit teams with the necessary competence;
- providing necessary resources to the audit teams;
- ensuring the conduct of audits in accordance with the audit program and within the agreed time frame;
- ensuring that audit activities are recorded and records are properly managed and maintained.
Implementing the audit program

Defining the objectives, scope and criteria for an individual audit:

- The audit objectives define what is to be accomplished by the individual audit and may include the following:
  - Level of compliance of the management system to be audited, or parts of it, with audit criteria;
  - evaluation of activities, processes and products with the requirements and procedures of the management system;
  - evaluation of the capability of the management system to ensure compliance with legal and contractual requirements and other requirements to which the organization is committed;
  - evaluation of the effectiveness of the management system in meeting its specified objectives;
  - identification of areas for potential improvement of the management system.

- The audit criteria includes applicable policies, procedures, standards, legal requirements, management system requirements, contractual requirements, etc.
Implementing the audit program

Selecting the audit methods:

- Typically a combination of interviews, record review, completion of checklists, and associated with a sampling plan
- Annex B of ISO 19011 gives detailed guidance
Implementing the audit program

Selecting the audit team leader and audit team members:

- Responsibility for the audit assigned to the audit team leader
- Audit team members are selected to support the audit objectives, and need to have appropriate background, skills and competence in regards to the audit being planned
- “Technical Experts” often used but role differs from an audit team member
Implementing the audit program

Managing the audit program outcome:

- The person managing the audit program should ensure that the following activities are performed:
  - review and approval of audit reports, including evaluating the suitability and adequacy of audit findings;
  - review of root cause analysis and the effectiveness of corrective actions and preventive actions;
  - distribution of audit reports to the top management and other relevant parties;
  - determination of the necessity for any follow-up audit.

- Audit program records need to created, managed and maintained to demonstrate the implementation of the audit program (including confidentiality concerns)
Implementing the audit program

Monitoring the audit program:
- Monitor its implementation for performance of teams and achievement of audit objectives

Reviewing and improving the audit program:
- Review the audit program to assess whether its objectives have been achieved.
- Lessons learned from the audit program review should be used as inputs for the continual improvement process for the program.
Performing an audit

General Considerations:
- Initiating the audit
- Preparing audit activities
- Conducting the audit activities
- Preparing and distributing the audit report
-Completing the audit
- Conducting audit follow-up
Performing an audit

Initiating the audit:

- Establish initial contact with the auditee
- Communicate with the auditee concerning audit objectives, scope, scheduling, methods, audit team composition and evaluation of on-site considerations

Determining the feasibility of the audit:

- Need reasonable confidence that the audit objectives can be achieved (time, resources, cooperation from the auditee)
Performing an audit

Performing document review in preparation for the audit:

- The relevant management system documentation (e.g. quality manuals, procedures) of the auditee should be reviewed in order to:
  - gather information to prepare audit activities and applicable work documents, e.g. on processes, functions;
  - establish an overview of the extent of the system documentation to detect possible gaps.

- Annex B in ISO 19011 provides more detailed guidance
Performing an audit

Preparing the audit plan:

- Information based on the structure of the audit program and tailored to the audit being performed
- Dependent on scope and complexity of the audit, but should include:
  - The audit objectives
  - The audit scope, including identification of program structure, as well as processes to be audited
  - The audit criteria and any reference documents
  - The locations, dates, expected time and duration of audit activities to be conducted, including meetings with the auditee’s management
  - The audit methods to be used, including a sampling plan, if applicable
  - The roles and responsibilities of the audit team members, as well as guides and observers
Performing an audit

Preparing work documents:

- Collect and review the information relevant to the audit assignments and prepare work documents, as necessary, for reference and for recording audit evidence:
  - checklists;
  - audit sampling plans;
  - forms for recording information, such as supporting evidence, audit findings and records of meetings.

- The use of checklists and forms should not restrict the extent of audit activities, which can change as a result of information collected during the audit.

- Annex B in ISO 19011 provides more detailed guidance
Performing an audit

- Conducting an audit includes:
  - Conducting the opening meeting
  - Performing document review while conducting the audit
  - Communicating during the audit
  - Collecting and verifying information
  - Generating audit findings
  - Preparing audit conclusions
  - Conducting the closing meeting
Performing an audit

Opening Meeting:

- Should be held with the auditee’s management and, where appropriate, those responsible for the functions or processes to be audited. During the meeting, an opportunity to ask questions should be provided.

- The degree of detail should be consistent with the familiarity of the auditee with the audit process. In many instances, e.g. internal audits in a small organization, the opening meeting may simply consist of communicating that an audit is being conducted and explaining the nature of the audit.
Performing an audit

Performing document review while conducting the audit:

- The auditee’s relevant documentation should be reviewed to:
  - determine the conformity of the system, as far as documented, with audit criteria;
  - gather information to support the audit activities.

- The review may be combined with the other audit activities and may continue throughout the audit, providing this is not detrimental to the effectiveness of the conduct of the audit.

- Annex B in ISO 19011 provides more detailed guidance
Performing an audit

Communicating during the audit:

- Arrange formal communication within the audit team, as well as with the auditee, the audit client and potentially with external bodies (e.g. regulators), especially where legal requirements require the mandatory reporting of non-compliances.
- The audit team should confer periodically to exchange information, assess audit progress, and reassign work between the audit team members, as needed.
- During the audit, the audit team leader should periodically communicate the progress of the audit and any concerns to the auditee and audit client, as appropriate.
Performing an audit

Collecting and verifying information:

- Collect information relevant to the audit objectives, scope and criteria, information relating to functions, activities and processes, should be collected by means of appropriate sampling and should be verified.

- Only information that is verifiable should be accepted as audit evidence.

- Sources include: Interviews, observations, review of documents.

- Annex B in ISO 19011 provides more detailed guidance.
Performing an audit

- Source of information
- Collecting by means of appropriate sampling
- Audit evidence
- Evaluating against audit criteria
- Audit findings
- Reviewing
- Audit conclusions

Figure 3 — Overview of the process of collecting and verifying information
Performing an audit

Generating audit findings:

- Audit evidence should be evaluated against the audit criteria in order to determine audit findings.
- Audit findings can indicate conformity or nonconformity with audit criteria.
- When specified by the audit plan, individual audit findings should include conformity and good practices along with their supporting evidence, opportunities for improvement, and any recommendations to the auditee.
- Nonconformities and their supporting audit evidence should be recorded. Nonconformities may be graded.
- They should be reviewed with the auditee in order to obtain acknowledgement that the audit evidence is accurate, and that the nonconformities are understood.
- Every attempt should be made to resolve any diverging opinions concerning the audit evidence or findings, and unresolved points should be recorded.
Performing an audit

Preparing audit conclusions:

- The audit team should confer prior to the closing meeting in order to:
  - review the audit findings, and any other appropriate information collected during the audit, against the audit objectives;
  - agree on the audit conclusions, taking into account the uncertainty inherent in the audit process;
  - prepare recommendations, if specified by the audit plan;
  - discuss audit follow-up, as applicable.
Performing an Audit

**Conducting the closing meeting:**

- Facilitated by the audit team leader, to present the audit findings and conclusions.
- Appropriate attendance by auditee’s management + other staff.
- Communicate the following:
  - Advising that the audit evidence collected was based on a sample of the information available;
  - The method of reporting;
  - The process of handling of audit findings and possible consequences;
  - Presentation of the audit findings and conclusions in such a manner that they are understood and acknowledged by the auditee’s management;
  - Any related post-audit activities (e.g. implementation of corrective actions, audit complaint handling, appeal process).
- Any diverging opinions regarding the audit findings or conclusions between the audit team and the auditee should be discussed and, if possible, resolved.
Post-audit activities

Preparing and distributing the audit report:

- Report the audit results in accordance with the audit program procedures.
- The audit report should provide a complete, accurate, concise and clear record of the audit, and should include or refer to the following:
  - the audit objectives;
  - the audit scope, particularly identification of the organizational and functional units or processes audited;
  - identification of the audit client;
  - identification of audit team and auditee’s participants in the audit;
  - the dates and locations where the audit activities were conducted;
  - the audit criteria;
  - the audit findings and related evidence;
  - the audit conclusions;
  - a statement on the degree to which the audit criteria have been fulfilled.
- The audit report should be dated, reviewed and approved, as appropriate, and distributed in accordance with audit program procedures.
Post-audit activities

Completing the audit:

- The audit is completed when all planned audit activities have been carried out, or as otherwise agreed with the audit client (e.g. there might be an unexpected situation that prevents the audit being completed according to the plan).

- Documents pertaining to the audit should be retained or destroyed by agreement between the participating parties and in accordance with audit program procedures and applicable requirements.

- Lessons learned from the audit should be entered into the continual improvement process of the management system of the audited organizations.
Post-audit activities

Conducting audit follow-up:

- The conclusions of the audit can, depending on the audit objectives, indicate the need for corrections, or for corrective, preventive or improvement actions.

- Such actions are usually decided and undertaken by the auditee within an agreed timeframe. As appropriate, the auditee should keep the person managing the audit program and the audit team informed of the status of these actions.

- The completion and effectiveness of these actions should be verified. This verification may be part of a subsequent audit.
Other considerations

- Additional guidance in ISO 19011 for:
  - Competence and evaluation of auditors
  - Monitoring of auditor performance
  - Annex A contains detailed guidance
Summary

- Parts or all of ISO 19011 can be used to build a robust internal audit program
- Adherence to the six principles of auditing lays the foundation
- Management commitment to the internal audit program is key
- Follow the audit procedure and audit plan for success
Thank you!
and questions