

# ISO/IEC27001 Expectations and Guidance for Certification and Surveillance audits

## **Introduction**

This document identifies AQA International's expectations for organizations seeking registration to ISO 27001. ISO 27001 emphasizes the development of a process oriented Information Security Management System (ISMS) that provides for continual improvement, risk identification, analysis and control. The certification process will encompass the requirements of the international standard.

It is organized into the following sections:

- I. Readiness Review Expectations
- II. Preassessment Expectations
- III. Conformance Audit Expectations
- IV. Surveillance Audit Expectations
- V. Nonconformance Response Expectations

*Reading the expectations contained in this document will help an organization understand their role in the certification process. Additional guidance that should be utilized includes:*

- ISO 27001 International Standard (available at [www.iso.org](http://www.iso.org))
- ISO/IEC 17799:2005 available at [www.iso.org](http://www.iso.org))

If an organization wants their processes outside of the scope for their ISMS certified, then this needs to be communicated to AQA as part of the request for certification. AQA will work with the organization to determine if it meets the definition of scope, location, and site.

## **I. Readiness Review Expectations**

The ISMS, including definition of the scope and boundaries and procedures must be reviewed by the auditor prior to the audit to establish ISO 27001 requirements are addressed. The organization will complete AQA form ISF-019 to depict how the organization's ISMS addresses ISO 27001 requirements and send it to the auditor along with the ISMS manual and procedures. Guidance to the significant requirements that must be addressed include:

1. The scope of the ISMS. Verify Scope is complete and appropriate.
2. Verify Organization Size and Shifts
3. Verify total employees (Staff & Contracted Personnel)
4. Verify evidence of risk assessment, evaluation, risk treatment plans and controls
5. Organization's processes- including sequence and interactions.
6. Statement of Applicability: Addressed all controls or justified
7. Management approvals
8. Verify required documentation is present
9. Internal Audits including complete ROUND OF audits to ISO 27001
10. Verify audits are process based
11. Management Review must have all ISO 27001 required inputs/outputs including internal audits to ISO 27001

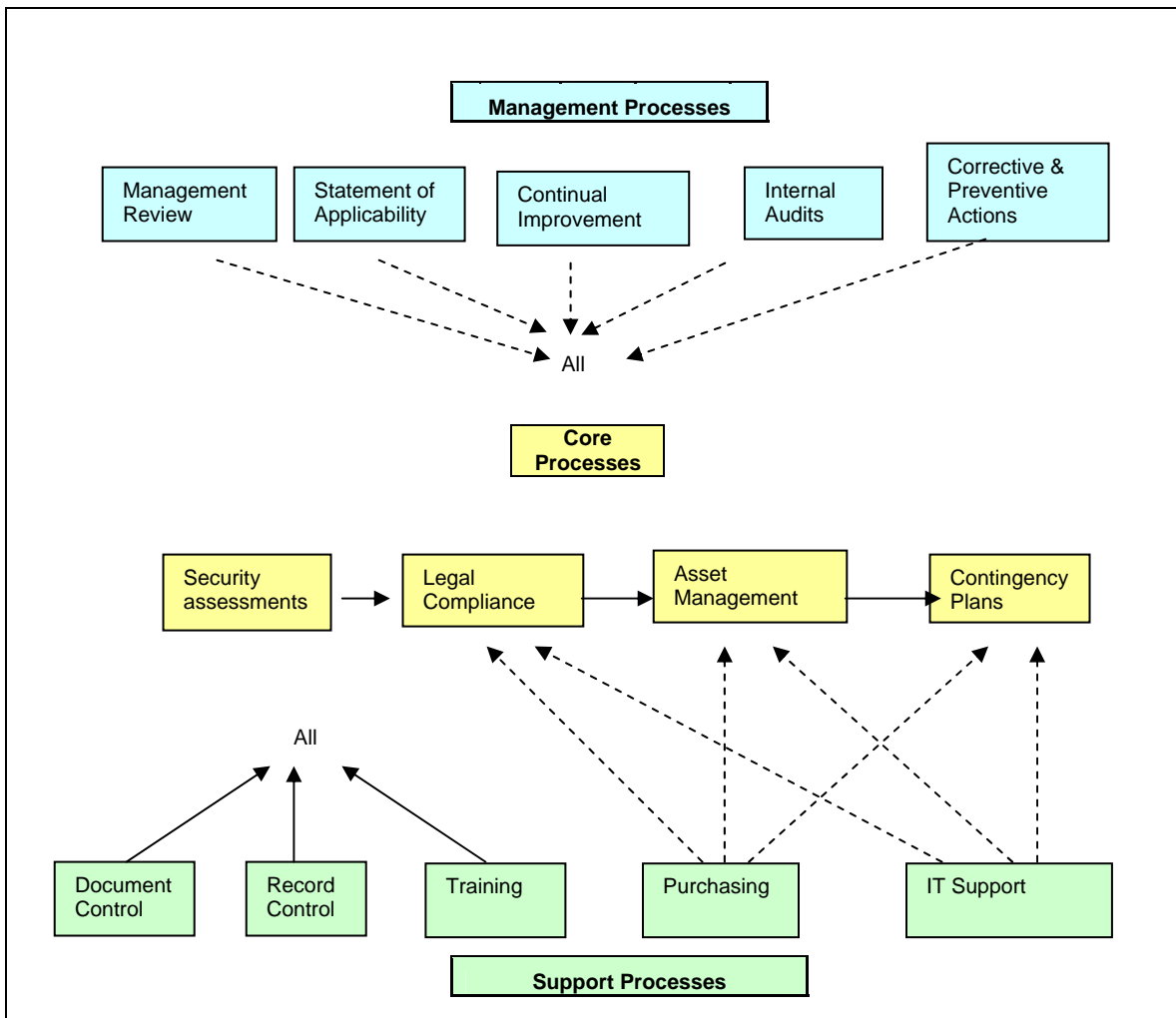
ISO 27001 promotes the adoption of an information security management system based on a



## ISO/IEC27001 Expectations and Guidance for Certification and Surveillance audits

process management approach. This approach identifies and manages those linked activities that together address the requirements ISO 27001. The documented ISMS must include a description of the interaction between the specific processes of the organization's information security management system. Core processes, support processes and management processes must be addressed. AQA strongly recommends linkage, or interaction, be shown pictorially, but any means to describe interactions between processes is acceptable as long as analysis of the interactions to ensure all processes operate as a network may be performed by the auditor. Figure 1 is an example of a pictorial representation of interaction between processes. Figures 2 & 3 are examples of filled portions of an ISF-019 form

Figure 1:



An example of the filled out portion of the core processes section of the ISF-019 matrix is below as Figure 2:



## ISO/IEC27001 Expectations and Guidance for Certification and Surveillance audits

<b>II. PROCESS – REQUIREMENT MATRIX</b>  A = clause addressed by process	4.1 General	4.2.1 Establish the ISMS	4.2.2 Implement & Operate	4.2.3 Monitor the ISMS	4.2.4 Maintain & Improve	4.3.1 Documentation	4.3.2 Document Control	4.3.3 Control of Records	5.1 Management Commitment	5.2.1 Provision of Resources	5.2.2 Training, Awareness and Competence	6.0 Internal Audits	7.0 Management Review	8.1 Continual Improvement	8.2 Corrective Action	8.3 Preventive Action
	Elements requiring address via documented procedure															
Mandatory Assessment E=every audit; Y= yearly		E	E	E	Y		E		E			E	E	E	E	E
Process: <b>Risk Assessments</b> Owner: Top Management Procedure: <b>RASOP-01</b>	X	X	X	X	X				X	X	X	X	X	X		
Process: <b>Legal Compliance</b> Owner: Top Management Procedure: <b>LCSOP-01</b>		X	X	X	X											
Process: Owner: Procedure:																

Organization management and support processes will often have a one to one correlation with requirements of the standard. One example for each type of process completed on the F-019(2K) matrix follows in Figure 3:

	4.1	4.2.1	4.2.2	4.2.3	4.2.4	4.3.1	4.3.2	4.3.3	5.1	5.2.1	5.2.2	6.0	7.0	8.1	8.2	8.3
<b>Support Processes</b>																
Process: <b>Document Control</b> Owner All Depts. Procedure: <b>DQSP-02</b>							X									
Process: <b>Training</b> Owner: HR Procedure: <b>HRSOP-01</b>											X					
Process: Owner: Procedure:																
<b>Management Processes</b>																
Process: <b>Management Review</b> Owner Management Procedure <b>DQSP-03</b>													X			
Process: <b>Internal Audits</b> Owner Management Procedure <b>DQSP-03</b>	X					X	X	X				X	X	X	X	X

**Figure 3 is an example - it is essential that organizations depict their management and support processes.**

12. At least one (1) management review, which includes an assessment of the information security systems suitability and effectiveness must be completed and recorded prior to the conformance audit.
13. At least one (1) full internal audit cycle must be completed and recorded prior to the conformance audit. All clauses of ISO 27001 must have been audited by qualified internal auditors. An AQA pre-assessment audit does not qualify as evidence of meeting this requirement.
14. At least three (3) months of records required by the information security management



# ISO/IEC27001 Expectations and Guidance for Certification and Surveillance audits

system **should** have been generated.

The organization must contact the auditor or AQA Office to reschedule the conformance audit if any of these expectations cannot be fulfilled by the scheduled audit date.

## **II. Preassessment Expectations:**

If a preassessment is requested by the organization, this will occur prior to the conformance audit. This activity is optional and is not required.

## **III. Conformance Expectations:**

AQA will utilize a process audit approach for the conformance audit. The audit plan will focus on management processes and core processes. Support processes will be audited as audit trails develop during management process and core process audit activities. The auditor will expect process owners to be identified and that processes be monitored, measured and analyzed to determine their effectiveness.

## **IV. Surveillance Audit Expectations:**

The process audit approach will be utilized for surveillance audits. The auditor will also expect:

1. Effective implementation of corrective actions in response to previous nonconformances
2. Evidence of efforts made toward *continuous improvement*.
3. A comprehensive list, or equivalent control system, identifying the nature of all revisions to the scope, policy and procedures.

## **IV. Nonconformance Response Expectations**

AQA Organizations are required to transfer each AQA identified nonconformance to their internal corrective action form and system. Failure to submit an acceptable response utilizing their corrective action form and system by the established due date may have a negative impact on new or existing registrations.

### **Acceptable Organization Corrective Action Responses Must Include:**

- 1. The results of an investigation to determine the root cause or most basic cause(s) of the nonconformance.**

If the root cause is not determined, it is unlikely the corrective actions will prevent recurrence of the nonconformance. In fact, a good test to determine if you have properly identified the root cause is to ask, “If we eliminate this cause, will the nonconformance happen again?” If the answer is no, then the root cause is properly identified. If the answer is yes or maybe, then the root cause needs to be further analyzed. It often takes asking “why did the potential root cause occur” several times to reach a root cause upon which corrective actions can be based to prevent recurrence

Below are some root causes that are usually inadequate and should be rarely used:

- “Operator error” or “Oversight on the part of the operator”,
- “Poor training” or “Training not effective ”,
- “Didn’t understand the requirement” or “Not aware of the requirement”
- “Isolated occurrence”

Use of these root causes may result in AQA asking for further clarification or investigation because they are not specific and lend themselves to narrow corrective actions that may not prevent recurrence



## ISO/IEC27001 Expectations and Guidance for Certification and Surveillance audits

of the nonconformance. When these are encountered, “why” should be asked at least once more to determine an underlying or more basic cause. For example, if asked why an operator error occurred, it may be determined to have been caused by the operator inadvertently selecting the wrong switch that looked similar and was close to the correct switch. This root cause would lend itself to mistake proofing that would separate or distinguish the switches to prevent recurrence.

Root causes must also be sought over which management has control. A root cause of “severe weather” does not support preventing recurrence of the nonconformance where-as root causes of inadequate contingency planning or a leaking roof do support preventing recurrence of the nonconformance.

### 2. Corrective actions including both:

- Corrective actions taken to determine the extent of, contain and correct (i.e. fix) the specific nonconformance
- Corrective actions taken in response to the root cause(s) to eliminate recurrence of the nonconformance. These corrective actions focus on changing a process to eliminate the root cause and thus eliminate recurrence of the nonconformance.
- Often, corrective actions are submitted that fix the specific nonconformance but do not address the root cause to prevent recurrence of the nonconformance.

### 3. Verification that corrective actions have been implemented.

The organization must verify corrective actions have been implemented and submit this verification, along with evidence of implementation (procedures, records, pictures, control plans, etc.) to AQA. Usually, corrective actions that have not been implemented are not acceptable. Corrective actions that, by nature, require more time to implement may be accepted for future verification if accompanied by specific target dates and adequate justification.

#### Examples of Good Root Cause and Corrective Actions:

<b>Nonconformance, Root cause and corrective action</b>
<p><b>Nonconformance:</b> Personal data was stolen from server by hacker.  <b>Immediate Response:</b> Secure Server from Internet, Notify authorities, notify victims as required.  <b>Root Cause:</b>                      Why? Internet connection was not secured by firewall.                      Why? Firewall was not working properly                      Why? License for Firewall program had expired                      Why? Purchase of new license was not in budget.                      Why? Procedure did not describe how to identify expiring software licenses.  <b>Corrective Action:</b> (1) Procedure changed to provide instructions for regular review of software licenses. (2) Log sheet created for all software licenses and expiration dates. (3) Budget procedure changed to include review of Software License log sheet.</p>
<p><b>Nonconformance:</b> Personal Data was lost during hurricane.  <b>Root Cause:</b>                      Why? Flooding damaged the information                      Why? Weather was not considered a risk                      Why? Inadequate understanding of all risks to information                      Why? Insufficient training                      Why? Lack of sufficient funding  <b>Corrective action:</b> (1) Budget was approved to identify and control all risks to information (2) Training was given and evaluated for effectiveness (3) Contingency plan created for threats to information (4) Personnel data relocated to 2<sup>nd</sup> floor</p>
<p><b>Nonconformance:</b> Several new employees have no records showing that they are competent.  <b>Root Cause:</b> These employees were determined to be competent during on the job training. Human resource manager had been keeping these records but the procedure was recently changed for supervisors to keep these records. This change was not properly communicated to supervisors. No acknowledgement of procedural changes is required.  <b>Corrective action:</b></p>



## ISO/IEC27001 Expectations and Guidance for Certification and Surveillance audits

Verified that on-the-job training records were on file with the Human Resource Manager for all new employees hired before the procedure was changed to have the supervisor keep these records. On-the-job training has been verified for all new employees hired after the procedure was changed and records are attached. The training procedure has been revised to require a procedure (new or revision) sign off for all affected people indicating that they are properly trained to the revision. Attached are the revised training procedure and the sign off sheet for all affected people. An audit has been scheduled for August 2005 to evaluate the effectiveness of training to new procedures and procedure revisions.

Nonconformance, Root cause and corrective action	Reason for <u>NOT</u> being acceptable
<p><b>Nonconformance:</b> Annual audit plan does not provide objective evidence to support how the audits are planned according to status and importance of the activity</p> <p><b>Root Cause:</b> Not all the key points of internal auditing were grasped</p> <p><b>Corrective Action:</b> Retraining is to be held for the internal auditor whose qualifications shall be conferred with by the management. The internal auditing plan for the year 2005 is to be formulated to ensure that the planned arrangements are prioritized as per the quality activities of the company</p>	<p><b>Root Cause</b> does not identify the underlying cause of the nonconformance.</p> <p><b>Corrective action</b> fixes the 2005 audit plan, but needs to be verified as complete or have a target date established for completion.</p> <p><b>Corrective action</b> of retraining of internal auditor suggests that the initial training was not effective. This should be examined as part of the root cause.</p>
<p><b>Nonconformance:</b> Security software license expired</p> <p><b>Root Cause:</b> Person responsible for software forgot to renew the license</p> <p><b>Corrective action:</b> Security software license renewed.</p>	<p><b>Root Cause</b> doesn't address why the system allows software license's to expire .</p> <p><b>Corrective Action</b> fixes "Security software", but is not clear if all software was identified and fixed.</p> <p><b>Corrective Action</b> the fix does not include an investigation to determine if any breaches occurred because it was expired</p> <p><b>Corrective Action</b> does not make any change to prevent it from recurring.</p>

### Examples of Poor Root Cause and Corrective Actions:

### Frequently Asked Questions

**FAQ 1: How is adequacy addressed in the ISF-019 matrix?**

The organization initially indicates where requirements are addressed on the matrix with an "A". The auditor will review the matrix and associated documentation. Any comments regarding adequacy are noted by "C1, C2, etc. on the matrix and explained in section VI.

**FAQ 2: What should be filled in for "owner of process"?**

The position (manager, etc.) is preferred but the name of the person is acceptable

**FAQ 3: What is meant on the ISF-019 matrix by "Mandatory Assessment - every audit"?**

Auditors are to address these elements each surveillance

**FAQ 4: Will organizations be requested to fill out an ISF-019 every surveillance?**

No, the AQA auditor will update it to reflect any changes after each audit.

