Your Risk Management Advantage

CLIENT INFORMATION NOTE

ISO/IEC 42001:2023 Audit process

CIN (042)

Overview

This Client Information Note explains the main stages of our process for ISO/IEC 42001 Artificial Intelligence Management System (AIMS) audit and certification.

The audit process normally includes two visits to your site before we can recommend approval. We call these two visits:

- Stage 1 (document review and planning visit), and
- Stage 2 (initial audit).

Once we have issued your approval certificate, we will carry out surveillance visits to maintain your approval.

At each visit, our auditors will be open and helpful and will follow a practical approach. In this way we believe that we add value to the audit process.

Before we visit, we will discuss and agree with you the visit dates, start and finish times, the audit team members, how long the visit will last, and which parts of your business we will visit.

Stage 1 – Document review and planning visit

Purpose of the visit
We do this visit to:

- confirm that your management system documents required by the standard are available, in place and put into practice so that a meaningful Stage 2 audit can take place
- ensure that there is top management commitment and alignment of the AIMS to business objectives
- confirm the scope, audit team requirements and timing for the Stage 2 audit
- ensure the selected controls are appropriate and focused on addressing identified risks and other requirements.
- we will obtain a sufficient understanding of the design of AIMS in context of your organization, risk assessment and management, AI & IS Policy & Objectives.
- confirm other relevant information about your organization, its context, processes and activities so that we can develop a plan for your Stage 2 audit
- answer any questions you may have about our service.

Carrying out the visit

The visit (which usually lasts for two days), starts with an opening meeting. The auditor will explain to your management team how we carry out audits, and you will be able to introduce your company. The auditor will agree a plan for the visit with you before the visit including a time to interview the key Visit activities will include:

- a review with top management of the business context, strategic direction and expected outcomes, to ensure alignment of the management system with business objectives
- Understanding impact of AI systems, AI system life cycle
- an evaluation of the risk audit and treatment processes, validation of the interfaces and dependencies not in scope, and validation of the selection of controls;
- a review of the design and documentation of your system against the audit standard, proposed audit scope and in the light of discussions with senior management.
- an audit of any planning controls to ensure control objectives can be achieved

- a site tour, if appropriate
- the production of a detailed plan for the Stage 2 visit
- production of a focused report which describes both positive findings and any issues requiring your attention before the Stage 2 visit takes place. The report will identify the grading or severity of these issues.

The auditor will usually need to review:

- business context and strategic direction
- AIMS policy and objectives
- scope of the AIMS; identify & confirm type of AI organization
- risk audit and selection of controls, review SOA
- key roles and responsibilities
- communications plans
- compliance and statutory requirements
- risk treatment plans and actions
- measurement and analysis plans
- internal Audits and management review records.

The visit ends with a closing meeting to present the Stage 1 report and agree the next stage of the audit process, including any health and safety, security, Privacy and administrative issues.

Your Stage 2 will not be confirmed until Stage 1 has been independently reviewed (technical review).

During this visit the auditor will focus on how your management system has been put into practice. The Stage 2 visit aims to confirm that:

- your policies, objectives, programmes and procedures are effectively put into practice
- at least one management review and internal audit covering the scope has taken place
- there is a planned and systematic approach for improvement
- you are managing your processes effectively
- the management system meets all the requirements of the audit standard.

Carrying out the visit

The audit follows the plan prepared during the Stage 1 visit. Members of the audit team will visit areas with guides who can witness the findings and help the audit. The Stage 2 audit usually includes a meeting with the representative of senior management with overall responsibility for the management system.

Our audit team will report, as a minimum, any findings related to:

- follow-up of findings from the Stage 1 visit
- activities, products and services identified in the agreed scope for the audit
- how effective the management system is at achieving your organization's security policy and objectives and continual improvement
- progress to achieve objectives through the management programme
- putting into practice the systems needed by the management system, and maintaining appropriate records
- putting into practice monitoring and measurement arrangements to
- assess how the management system performs and whether objectives are being achieved
- how involved in, and committed
- to, the management system the senior management are, and
- how effective the internal audit, corrective action and management review processes are.
- functional testing for the documentation requirements, controls, committees, risk assessment processes, reporting processes and handling of complaints listed in ISO/IEC 42001
- AIMS requirements for functional testing through representative sampling for controls that affect the quality of the product, service, or process related to the quantity of AI products placed on the market or related to the amount of users of an AI system.
- Specific elements included in our audit would include:
- a) require the organisation to demonstrate that the assessment of AI-specific related risks is relevant and appropriate to the AIMS operation covered by the scope of the management system;
- b) determine whether the client's procedures for identifying, investigating, and assessing AI-specific related risks and the results of implementation are consistent with the client's policies and objectives.

The audit team will hold review meetings with you each day to discuss any findings. Appropriate staff should be present to confirm that you accept these findings. Please see below in the 'Reporting' section how we define findings. We finalize the grade of findings at the end of the visit.

The visit ends with a closing meeting to present a summary of the findings, and to agree the next stage of the audit process. The auditor will give a complete report to the management representative. If we have not reported any Major Nonconformities, and you have informed the auditor of your proposed corrective action for any Minor Nonconformities, the auditor will recommend approval to the audit standard (although this depends on an independent technical review by our office). However, if any Major Nonconformities have been reported, we will delay approval and carry out a follow-up audit to review corrective actions. Our team leader will agree with you the arrangements for this visit.

Surveillance visits

Purpose of the visit

Once we have certified your management system, we will begin a programme of surveillance visits (which normally take place every six months). The surveillance visits aim to confirm that the approved management system continues to:

- be maintained
- be in operation, and
- deliver continual improvements.

We will check for any appeals or complaints brought to our attention.

We also consider the implications of changes to the system. Such changes may have been carried out as a result of changes in your activities, products or services. We will then consider whether you continue to meet certification requirements.

Carrying out the visit

Themes for surveillance visits will normally have been agreed with you at your previous visit. We will confirm the details with you at an opening meeting.
Themes chosen will allow us to review:

- internal audit and management review processes
- incident reporting (including client complaints) and management
- progress in meeting AIMS objectives and KPIs
- corrective action and risk treatment processes
- changes to the system, their impact on risk management, and the effectiveness of their implementation
- how you manage changes relating to responsibilities and the authority of main staff

We will also review any outstanding findings.

If we report any Minor Nonconformities during a visit and the next visit is within six months, we will normally follow them up during our next visit to you, otherwise we will make arrangements with you for the follow up.

If we report a Major Nonconformity during a surveillance visit, we will arrange a special surveillance visit to follow up the necessary corrective action (normally within three months).

This is the first phase of our suspension and withdrawal of approval process.

At the closing meeting, our auditor will report on the current visit and agree with you the theme for the next visit. If any Major Nonconformities have been reported, the auditor will also agree arrangements for follow-up of actions you will take.

Certificate renewal
Planning for the certificate renewal

We conduct certificate renewals on a three-yearly basis, planned at the previous surveillance visit and agreed with you.

The certificate renewal planning process contains three steps: Review, Preview and Planning.

Review

This step includes the review of past performance such as:

- trend information on complaints and other performance indicators
- system documentation improvements
- achievement of AIMS objectives
- lessons learned from audits
- trends in our findings.

Based on this review of past performance, our auditor will identify any potential risks in the present management system regarding successful implementation of the strategies and objectives.

Preview

The aim of the preview is to align our audit activities with your strategy and objectives. The auditor will use their conversation with senior management to understand your longer term expectations, for example, strategy issues such as business and operational risks, competitive issues, changes to internal and external environment etc.

Our auditor will establish, through the interview, whether these expectations, objectives and strategies will affect the complexity of your management system or the interested parties to your organisation.

The preview stage will be used to identify further themes that can be used in the coming certificate renewal visit and for the next three-year cycle.

Planning

The next step in the visit is planning the certificate renewal. In this part of the visit our auditor will:

- identify any aspects of the system that have not been appropriately addressed during the surveillance cycle, and plan how to review these
- use the information gained during the review and preview stages to support the planning process
- if appropriate, consider how best to give attention to any themes identified
- identify the areas, departments, processes and activities to be audited
- agree with you sensible durations for each of these, commensurate with risk
- try to identify the best use of resources, and avoid duplication
- add appropriate time for reporting, consolidating and presenting reports
- consolidate the information into a sensible visit plan.

Our auditor will allow time for discussion with all relevant managers and for a review of records for all relevant departments.

Conducting certificate renewal visits

We conduct the certificate renewal visit similarly to a Stage 2 audit. In addition, we include a review of your system documentation to ensure that it:

- continues to suit your company, and
- complies with the certification requirements and the scope of certification, including continual improvement.

Changes to your approval

For any significant change in the scope of your certificate of approval (e.g. change in headcount), please submit a formal request for the change. LRQA will review the request to consider:

- additions or changes to competency requirements for the visit team(s)
- additions or reductions in visit duration requirements

and you will be notified of any changes by an amended contract. We will undertake a separate document review visit (Stage 1) if the change requested has meant a major change or addition to your documented system.

The change to approval visit will be performed in line with our process for Stage 2 audit visits, although a formal visit plan is not normally produced. If no document review (Stage 1) has been undertaken, time will be allowed during the visit for the team leader to review relevant documentation and to agree a plan for any additional visit activities.

Such visits may be performed as separate visits or may be combined with a scheduled (Surveillance or Certificate Renewal) visit.

LRQA will issue an amended certificate(s), using the same expiry date as on the current certificate.

Reporting

The reporting process for all our visits is similar. We fill in visit reports to record audit findings, progress against the audit plan, positive comments, and also points of clarification or interpretation.

We record audit findings in an Audit Findings Log, and identify them as Major Nonconformity or Minor Nonconformity. We define these findings as follows:

Major Nonconformity: The absence of, or the failure to implement and maintain, one or more management system elements, or a situation which would, on the basis of the available objective evidence, raise significant doubt of the management to achieve:

- the policy, objectives or public commitments of the organisation
- compliance with the applicable regulatory requirements
- conformance to applicable client requirements
- conformance with the audit criteria deliverables.
- Audit report will include a reference to the version of the SOA reviewed

Generally, a major nonconformity will be a system failure that:

- is already affecting system effectiveness or deliverables
- puts at risk the capability of the management system
- requires immediate containment
- requires immediate root cause analysis and corrective action.
- Our team leader will make arrangements with you for follow up

Minor Nonconformity: A finding indicative of a weakness in the implemented and maintained system, which has not significantly impacted on the capability of the management system or put at risk the system deliverables, but needs to be addressed to assure the future capability of the system.

Generally, a minor nonconformity will be a weakness in an internal facing process or procedure; or a finding for which any further deterioration of control could reasonably be considered likely to result in the system becoming ineffective .Requires root cause investigation and corrective action.

If raised at a visit that results in a certificate being issued, then the auditor will ask you to indicate the corrective action that you will take. This corrective action plan will form part of the independent review by our office before your certificate is issued. If raised at a surveillance visit, although you need to take corrective action within an appropriate time after the visit, you do not normally need to provide us with details of the action until we next visit you.

In both cases, at the next visit the auditor will review the Suggestions for improvements that could be made to your compliant management system that would improve the efficiency of the processes undertaken, we will record in either:

- the executive summary, for strategic improvement suggestions, or
- The body of the report, for improvement suggestions that are related to particular area.

Please keep copies of all our visit reports for three years. In exceptional circumstances, we may ask you to provide copies of previous reports.

Sampling

It is important to remember that even though a problem may not have been identified in an area of activity, it does not necessarily mean that there are no problems. As audit work is based on sampling techniques, statistically there is always a possibility that issues will not be identified during an audit. Please remember this when you audit your own management system.

Confidentiality

We will not pass on any of the information we gather about your organization (including the contents of reports) to any other person or organization without your permission (except as required by the accreditation body).

Further information

To find out more about how LRQA can help you to increase performance and reduce risk, please visit our website lrqa.com. From here you can also visit one of our country specific websites to find out about LRQA in your country.

Your Risk Management Advantage

Get in touch

Visit **www.lrqa.com** for more information

LRQA
1 Trinity Park
Bickenhill Lane
Birmingham
B37 7ES
United Kingdom