IL7 Security – Guide to the ISO 27001 Internal Audit

The International Standards Organisation has its own standard for conducting audits. These are laid down in ISO 19011. Below IL7 draws from this and what has been learnt from experience and gleaned from industry experts as to how to conduct an Internal Audit against ISO 27001.

The main purpose of the internal audit is to improve the ISMS. The external audit is to get the certificate and for this you need to supply the annual Audit Programme and the Internal Audit report (amongst the other mandatory documents). Other optional but recommended documents are the Audit Procedure, defining when, how and what is being audited and the Audit Plan which covers the details, The Audit Programme is a schedule outlining the frequency of audit and defines the objectives, reasons and criteria, who is responsible for conducting the audit and who should follow up the audit findings. The Audit Report detailing those findings, positive and negative observations as well as major and minor non-conformities is to be reviewed by management.

It is important that the internal audit is by somebody who knows the business and has the right consultancy qualities, is technically knowledgeable and confident in purpose. It is important to avoid a conflict of interest and the internal auditor should be apart from the group responsible for the ISMS.

The Audit Plan can outline whether the audit is to be conducted clause by clause (start with 4) of the standard or by review of all relevant processes. It could also be through review of all mandatory documents and the supporting policies, procedures of the ISMS and Statement of Applicability. It is recommended here that the document review is the preferred route with the auditor applying knowledge of the standard and acknowledging the relevant processes as integral to the review. It is important to clarify audit criteria including the clauses in the standard but make explicit reference to 3rd party requirements (ICO regulator, Legislation and contracts, including supplier management agreements and policy). This should be discussed with senior stakeholders, management and information asset managers prior to completing the plan. With consensus, the Audit Plan can address the timescales, roles and responsibilities realistically with manageable targets. It is important that the audit follows the next seven stages in sequence.

1. Document review:
    a. ISMS Scope.
    b. Security Policy and supporting procedures.
    c. Mandatory documents (are they fit-for-purpose? e.g. does the Business Continuity Plan conform to ISO22301?).
    d. Records of Security Working Groups, Change Management etc.
    e. Risk Assessment Report (are assets, impacts and probabilities adequately addressed?).
    f. Statement of Applicability (are all arguments for or against applicability tangible?).
    g. Risk Treatment Plan (are targets realistic and ownership allotted fairly?).

2. Create Checklist. The checklist is created during the document review. It is a spreadsheet containing actions the auditor feels necessary to execute in order to verify the validity of processes undertaken and their compliance with the standard. Actions should be cross-referenced with relevant clauses in the standard.
3. Detailed Audit Plan. Define who needs to be interviewed. Allocate time to each interview and if relevant appoint a member of the audit team to the duty (unless there is just one internal auditor). Determine whether the interview needs to be in person (recommended in all but the most rudimentary cases), by telephone or whether an email is sufficient.
4. Audit Actions. Complete checks on all processes as required in the checklist. Interview responsible personal to discover if there are discrepancies between policy and procedure and actual operation. Do not make assumptions. Keep an open mind – doing something different does not make it wrong (it may be the written procedure should be changed not the practice!). Look at records available on visits (training records, new recruits' induction, provisioning etc.). Dip Sample records if necessary but the choice of review rests with the auditor, not the interviewee. Ask open questions, those not just requiring a yes/no answer but requiring an explanation which can lead to another why, what, when, how type question. Use the 'five why's' technique. Be friendly but assertive. Only when you reach the unavoidable yes or no conclusion can you ascertain the real reason, or core causal factor of any discrepancy. Sometimes it is advisable to interview a number of people doing the same process to ensure compliance is organisation-wide. Make a careful note in the checklist against the action and maintain neat and tidy records of all conversations (who, when, where etc.). Also, where relevant record the 'records' sampled/reviewed and document any discrepancy found with full reference details. This is EVIDENCE, after all.
5. Corrective Action Report (CAR) Produce a report detailing all positive and negative observations and all non-conformities. For all major or minor non-conformities deliver a description of how these might have developed and how best they might be mitigated or mollified.
6. Corrective (Remedial) Action Plan. This differs from the Risk Treatment Plan, produced in the core ISO 27001 implementation, but can be prioritised in the same way, by the severity of the risk involved. However, other things can be taken into account like 'quick wins'. It is important to assign ownership and timeframe for all major non-conformities. Where possible all negative observations should be addressed.
7. Follow-Up. Before delivering the final Internal Audit Report check on progress with actioners. Make sure agreed timescales and/or solutions are still realistic.

Finally check with the owner of the ISMS whether this has been appropriately altered, as with the Statement of Applicability to reflect the findings of the Internal Audit.