ISMS Auditing Guideline

Prepared by a team of volunteers from the ISO27k Forum

Version 1, March 12th 2008

Introduction

This guideline has been written by members of the ISO27k Forum at ISO27001security.com, an international community of practitioners who are actively using the ISO/IEC 27000-family of Information Security Management Systems (ISMS) standards known colloquially as "ISO27k". We wrote this guideline primarily to contribute to the development of ISO/IEC 27007 by providing what we, as experienced ISMS implementers and IT/ISMS auditors, believe is worthwhile content. A secondary aim was to provide a pragmatic and useful guideline for those involved in auditing ISMSs.

At the time of writing (February-March 2008), ISO/IEC 27007 is currently at the first Working Draft stage ("ISO/IEC WD 27007") and has been circulated to ISO member bodies for study and comment by March 14th 2008. Its working title is "Information technology - Security techniques - Guidelines for information security management systems auditing".

The proposed outline structure of ISO/IEC WD 27007 is presently as follows:

- Foreword and introduction

1. Scope
2. Normative references
3. Terms and definitions
4. Principles of auditing
5. Managing an audit programme
6. Audit activities
7. Competence and evaluation of auditors

- Bibliography

In the proposed structure, section 6 should presumably explain how to go about auditing an ISMS. The current working draft has headings for a guide to the audit process but little content on the actual audit tests to be performed, although in section 6.3.1 it identifies a list of items that are required by ISO/IEC 27001 and says that "Auditors should check that all these documents exist and conform to the requirements in ISO/IEC 27001:2005". This is probably the most basic type of ISMS audit test: are the specified ISMS documents present? We feel that a generic ISMS audit checklist (often called an "Internal Controls Questionnaire" by IT auditors) would be a very useful addition to the standard and producing one was a key aim of this guideline – in fact we have produced two (see the appendices). We also aim to contribute content to various other parts of the draft 27007 and hope to track its development through future revisions.

This guideline follows the present structure and section numbering of ISO/IEC WD 27007 for convenient cross-referencing.

1. Scope

This guideline provides advice to IT auditors reviewing compliance with the ISO/IEC 27000 family of standards, principally ISO/IEC 27001 (the ISMS certification standard) and to a lesser extent ISO/IEC 27002 (the code of practice for information security management). It is also meant to help those who are implementing or have implemented the ISO/IEC 27000 family of standards, to conduct internal audits and management reviews of their ISMS. Like the other related standards, it is generic and needs to be tailored to the specific requirements of each situation. In particular, we wish to point out that audits are best planned and conducted in relation to the risks facing the organization being audited, in other words the starting point for audit planning is an initial assessment of the main risks (commonly known as a pre-audit survey or gap analysis). As with ISO/IEC 27001 and ISO/IEC 27002, being risk-based provides a natural priority to the audit tests and relates directly to the organization's business requirements for information security.

2. Normative references

Please refer to:

- **ISO/IEC 27000**: this standard is currently at Committee Draft stage and is due to be published, hopefully, later in 2008. It contains an overview of the ISO27k standards and a vocabulary or definition of terms common to many of the ISO27k standards
- **ISO/IEC 27001:2005** *Information technology -- Security techniques -- Information security management system requirements*. This is the formal specification for an ISMS against which organizations may be certified compliant. Section 6 introduces the need for "Internal ISMS audits" and briefly sets the main requirements for audit procedures. Section 7 also identifies the need for periodic (at least annual) management reviews of the ISMS.
- **ISO/IEC 27002:2005** *Information technology -- Security techniques -- Code of practice for information security management*. Provides more pragmatic guidance than 27001 on how to design, implement, manage and improve an ISMS.
- **ISO/IEC 27006:2007** Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems. Accreditation criteria for ISMS certification bodies.
- **ISO/IEC 17021:2006** Conformity assessment — Requirements for bodies providing audit and certification of management systems
- **ISO 19011:2002** *Guidelines for quality and/or environmental management systems auditing.* [A new version of this standard is in preparation, so changes may be necessary once it is published].

3. Terms and definitions

Most ISMS-related terms used in this guide and in related standards will be defined in ISO/IEC 27000 when published. Specific IT/ISMS audit-related terms should be defined here if they are not used or defined in other ISO27k standards.

[Note: various general audit terms that are defined in ISO 19011 should be referenced here in place of the following working definitions.]

- **Audit** - the process by which a subject area is independently reviewed and reported on by one or more competent auditors on behalf of stakeholders
- **Audit checklist** - a structured questionnaire or workplan to guide the auditors in testing the area being audited
- **Audit evidence** - information gathered from the area being audited such as written documentation, computer printouts, interviews and observation
- **Audit finding** - the auditor's summary/description and analysis of an inadequately mitigated risk to the organization

- **Audit observation** - an optional or advisory audit recommendation which carries less weight than an audit recommendation
- **Audit plan or programme** - a project plan for an audit laying out the main audit activities and heir timing
- **Audit recommendation** - a corrective action that is proposed to address one or more identified audit findings, that must be addressed prior to certification or recertification of the ISMS
- **Audit report** - a formal report to management documenting the key findings and conclusions of the audit
- **Audit risk** - the potential for an audit to fail to meet its objectives, for example by using unreliable, incomplete or inaccurate information
- **Audit schedule** - a diary of planned audits
- **Audit subject** - the in-scope organization/s, or parts of an organization, which are being audited
- **Audit test** - a check conducted by the auditors to verify whether a control is effective, efficient and adequate to mitigate one or more risks to the organization
- **Audit work papers** - documents written by the auditors recording their examination, findings and analysis of the ISMS, including completed audit checklists
- **Compliance audit** - a type of audit specifically designed to assess the extent to which the audit subject conforms to stated requirements
- **ISMS audit** - an audit centred on the organization's Information Security Management System (ISMS)
- **Risk-based audit** - an audit planned on the basis of an assessment of risks

4. Principles of auditing

ISO 19011 section 4 covers the principles of auditing. Rather than duplicate ISO 19011, this section need only cover any aspects that are different or particularly relevant to ISMS audits such as …

- Important but generic audit principles *e.g.* independent evaluation against agreed criteria, plus more specific principles aimed at ISMS audits
- In all matters related to the audit, the ISMS auditor should be independent of the auditee in both attitude and appearance. The ISMS audit function should be independent of the area or activity being reviewed to permit objective completion of the audit assignment.
- Information security is a dynamic field with frequent changes to the risks (*i.e.* the threats, vulnerabilities and/or impacts), controls and environment. It is therefore important that auditors auditing information security controls should maintain knowledge of the state of the art (*e.g.* emerging information security threats and currently-exploited vulnerabilities) and the organizational situation (*e.g.* changing business processes and relationships, technology changes).

5. Managing an audit programme

This section should document activities involved in managing (*i.e.* planning, controlling and overseeing) the ISMS audit such as …

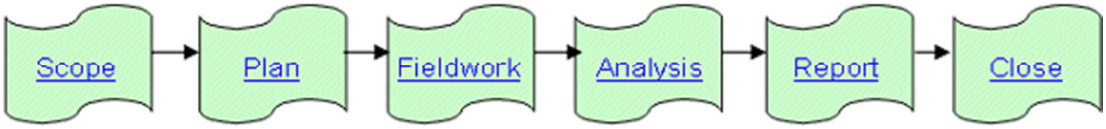
- Advice on planning and scoping individual ISMS audits within the overall audit work programme, *e.g.* the idea of combining wide but shallow ISMS audits with more narrow but deeper audits on areas of particular concern.
- ISMS audits at multi-site organizations including multinationals and 'group' structures, where comparisons between the ISMSs in operation within individual business units can help share and promote good practices

- Auditing business partners' ISMSs, emphasizing the value of ISO/IEC 27001 certification as a means of gaining a level of confidence in the status of their ISMSs without necessarily having to do the audit work
- Developing an internal program for auditing the ISMS. From an IRCA point of view you develop an Audit Plan when preparing to audit an organization. This plan is derived from the "Scope of Registration" document that an individual fills out when requesting a certification audit from a registrar. Besides the scope of registration the domain definition will also feed the audit plan.

6. Audit activities

The generic audit process of ISO 19011 may need to be customized to reflect the process steps specifically involved in IT audits and, further, for ISMS audits

The main stages of a 'typical' IT audit assignment are as follows:



6.1 Scoping and pre-audit survey

During this phase, the ISMS auditors determine the main area/s of focus for the audit and any areas that are explicitly out-of-scope, based normally on an initial risk-based assessment plus discussion with those who commissioned the ISMS audit. Information sources include general research on the industry and the organization, previous ISMS and perhaps other audit reports, and ISMS documents such as the Statement of Applicability, Risk Treatment Plan and ISMS Policy.

The ISMS auditors should ensure that the scope 'makes sense' in relation to the organization. The audit scope should normally match the scope of the ISMS being certified. For example, large organizations with multiple divisions or business units may have separate ISMS's, an all-encompassing enterprise-wide ISMS, or some combination of local and centralized ISMS. If the ISMS certification is for the entire organization, the auditors may need to review the ISMS in operation at all or at least a representative sample of business locations, such as the headquarters and a selection of discrete business units chosen by the auditors.

The auditors should pay particular attention to information security risks and controls associated with information conduits to other entities (organizations, business units *etc*.) that fall outside the scope of the ISMS, for example checking the adequacy of information security-related clauses in Service Level Agreements or contracts with IT service suppliers. This process should be easier where the out-of-scope entities have been certified compliant with ISO/IEC 27001.

During the pre-audit survey, the ISMS auditors identify and ideally make contact with the main stakeholders in the ISMS such as the ISM manager/s, security architects, ISMS developers, ISMS implementers and other influential figures such as the CIO and CEO, taking the opportunity to request pertinent documentation *etc*. that will be reviewed during the audit. The organization normally nominates one or more audit "escorts", individuals who are responsible for ensuring that the auditors can move freely about the organization and rapidly find the people, information *etc*. necessary to conduct their work, and act as management liaison points.

The primary output of this phase is an agreed ISMS audit scope, charter, engagement letter or similar. Contact lists and other preliminary documents are also obtained and the audit files are opened to contain documentation (audit working papers, evidence, reports *etc*.) arising from the audit.

6.2 Planning and preparation

The overall ISMS scope is broken down into greater detail, typically by generating an ISMS audit workplan/checklist (please see the appendices for two generic examples).

*Note: the generic example workplan/checklists supplied with this guideline are **not** intended to be used without due consideration and modification. This paper is merely a general guideline. It is anticipated that ISMS auditors will normally generate a custom workplan/checklist reflecting the specific scope and scale of the particular ISMS being audited, taking into account any information security requirements that are already evident at this stage (such as information-security relevant laws, regulations and standards that are known to apply to similar organizations in the industry). Also, the audit workplan/checklist may be modified during the course of the audit if previously underappreciated areas of concern come to light.*

The overall timing and resourcing of the audit is negotiated and agreed by management of both the organization being audited and the ISMS auditors, in the form of an audit plan. Conventional project planning techniques (such as GANTT charts) are normally used.

Audit plans identify and put broad boundaries around the remaining phases of the audit. It is common to make preliminary bookings for the formal audit report/discussion meeting to allow participants to schedule their attendance.

Audit plans often also include "checkpoints", that is specific opportunities for the auditors to provide informal interim updates to their management contacts including preliminary notification of any observed inconsistencies or potential nonconformities *etc*. Interim updates also provide opportunities for the auditors to raise any concerns over limited access to information or people, and for management to raise any concerns over the nature of the audit work. While the auditors are necessarily independent of the organization, they must establish a level of trust and a cooperative working environment in order to engage sufficiently and obtain the information necessary to audit the ISMS.

Finally, the timing of important audit work elements may be determined, particularly in order to prioritize aspects that are believed to represent the greatest risks to the organization if the ISMS are found to be inadequate.

The output of this phase is the (customized) audit workplan/checklist and an audit plan agreed with management.

6.3 Fieldwork

During the fieldwork phase, audit evidence is gathered by the auditor/s working methodically through the workplan or checklist, for example interviewing staff, managers and other stakeholders associated with the ISMS, reviewing ISMS documents, printouts and data (including records of ISMS activities such as security log reviews), observing ISMS processes in action and checking system security configurations *etc*. Audit tests are performed to validate the evidence as it is gathered. Audit work papers are prepared, documenting the tests performed.

The first part of the fieldwork typically involves a documentation review. The auditor reads and makes notes about documentation relating to and arising from the ISMS (such as the Statement of Applicability, Risk Treatment Plan, ISMS policy *etc*.). The documentation comprises audit evidence, with the audit notes being audit working papers.

Findings from the documentation review often indicate the need for specific audit tests to determine how closely the ISMS as currently implemented follows the documentation, as well as testing the general level of compliance and testing appropriateness of the documentation in relation to ISO/IEC 27001. The results of the audit tests are normally recorded in checklists such as those provided in Appendix A and Appendix B.

Technical compliance tests may be necessary to verify that IT systems are configured in accordance with the organization's information security policies, standards and guidelines. Automated configuration checking and vulnerability assessment tools may speed up the rate at

which technical compliance checks are performed but potentially introduce their own security issues that need to be taken into account*.

The output of this phase is an accumulation of audit working papers and evidence in the audit files.

6.4 Analysis

The accumulated audit evidence is sorted out and filed, reviewed and examined in relation to the risks and control objectives. Sometimes analysis identifies gaps in the evidence or indicates the need for additional audit tests, in which case further fieldwork may be performed unless scheduled time and resources have been exhausted. However, prioritizing audit activities by risk implies that the most important areas should have been covered already.

6.5 Reporting

Reporting is an important part of the audit process, and an involved sub-process all by itself:

A typical ISMS audit report contains the following elements, some of which may be split into appendices or separate documents:

- Title and introduction naming the organization and clarifying the scope, objectives, period of coverage and the nature, timing and extent of the audit work performed.
- An executive summary indicating the key audit findings, a brief analysis and commentary, and an overall conclusion, typically along the lines of "We find the ISMS compliant with ISO/IEC 27001 and worthy of certification".
- The intended report recipients plus (since the contents may be confidential) appropriate document classification or restrictions on circulation.
- An outline of the auditors' credentials, audit methods *etc*.
- Detailed audit findings and analysis, sometimes with extracts from the supporting evidence in the audit files where this aides comprehension.
- The audit conclusions and recommendations, perhaps initially presented as tentative proposals to be discussed with management and eventually incorporated as agreed action plans depending on local practices;
- A formal statement by the auditors of any reservations, qualifications, scope limitations or other caveats with respect to the audit.
- Depending on normal audit practices, management may be invited to provide a short commentary or formal response, accepting the results of the audit and committing to any agreed actions.

It is important that there is sufficient, appropriate audit evidence to support the results reported. Audit's quality assurance processes therefore ensure that 'everything reportable is reported and everything reported is reportable', normally based on a review of the audit file by a senior auditor. The wording of the draft audit report is checked to ensure readability, avoiding ambiguity and unsupported statements. When approved by audit management for circulation, the draft audit report is usually presented to and discussed with management. Further cycles of review and revision of the report may take place until it is finalized. Finalization typically involves management committing to the action plan.

* Note: automated system security audit tools are powerful utilities but are not appropriate in all environments. They can potentially undermine system security, perhaps introducing additional technical vulnerabilities, extracting highly sensitive information and affecting system performance or availability. Furthermore, auditors using such tools must be competent to use and obtain meaningful data from them: a "pass" from an automated vulnerability assessment tool does *not* necessarily mean that a system is free of vulnerabilities and is hence secure. A wrongly-configured or ineptly used database security review tool may bring down a production system. Such tools should only be introduced using the organization's conventional change management processes, including pre-implementation security testing, where appropriate.

In addition to the formal audit recommendations relating to any major non-conformance, auditors sometimes provide audit observations on minor non-conformance and other advice, for instance potential process improvements or good practice suggestions from their experience with other organizations. These may or may not be part of the formal audit report, depending on local practices. While such observations and advice will not preclude certification of the ISMS, they will be recorded on the audit file and may trigger follow-up audit work in a future surveillance or recertification audit. The auditors believe that it is in the organization's best interests to address all recommendations and observations, although the organization's management must decide about what to do and when to do it, if at all.

The output of this phase is a completed ISMS audit report, signed, dated and distributed according to the terms of the audit charter or engagement letter.

6.6 Closure

In addition to indexing and cross-referencing and literally shutting the audit files, closure involves preparing notes for future audits and following up to check that the agreed actions are in fact completed on time.

If the ISMS qualifies for certification (in other words, if all mandatory audit recommendations have been resolved to the satisfaction of the auditors), the organization's ISMS certificate is prepared and issued.

7. Competence and evaluation of auditors

The requirements from ISO/IEC 17021:2006, Clause 9.2 apply. In addition, the following ISMS-specific requirements and guidance apply.

7.1 Auditor competence

The following requirements apply to the audit team as a whole, or to the auditor if working individually.

In each of the following areas at least one audit team member shall take responsibility within the team:

1) managing the team, planning the audit, and audit quality assurance processes;

2) audit principles, methods and processes;

3) management systems in general and ISMS in particular;

4) legislative and regulatory requirements for information security applicable to the organization being audited;

5) information security related threats, vulnerabilities and incidents, particularly in relation to the organization being audited and comparable organizations, for example an appreciation of the likelihood of various types of information security incident, their potential impacts and the control methods used to mitigate the risks;

6) ISMS measurement techniques;

7) related and/or relevant ISMS standards, industry best practices, security policies and procedures;

8) information assets, business impact assessment, incident management and business continuity;

9) the application of information technology to business and hence the relevance of and need for information security; and

10) information security risk management principles, methods and processes.

The audit team must be competent to trace indications of security incidents in the ISMS back to the appropriate elements of the ISMS, implying that the auditors have appropriate work experience and practical expertise in relation to the items noted above. This does not mean that every auditor needs the complete range of experience and competence in all aspects of information security, but the audit team as a whole should have a sufficiently broad range of experience and sufficiently deep competencies to cover the entire scope of the ISMS being audited.

7.2 Demonstration of auditor competence

Auditors must be able to demonstrate their knowledge and experience for example through:

- holding recognized ISMS-specific qualifications;
- registration as auditor;
- completion of approved ISMS training courses;
- up to date continuous professional development records; and/or
- practical demonstration to more experienced ISMS auditors by following the ISMS audit process.

References and additional information

- The IT Audit FAQ offers general advice on conducting IT audits, auditor qualifications and competencies, audit process *etc.*
- ISACA offers advice on the audit charter.
- ISACA audit standards, guidelines and procedures.
- The Audit Quality Framework from the UK's Financial Reporting Council provides general advice on quality assurance for external auditors.
- This document was created as an international collaborative online team effort thanks to Google Docs.

Contributors/authors

The following members of the ISO27k implementers' forum volunteered to contribute to this guideline:

- **Gary Hinson** - IT auditor and information security manager for over 20 years; MBA, CISSP, CISM and CISA qualified; ISO27k user since the dawn of time; project leader.
- **Bala Ramanan** - ISMS Lead Auditor, CISM, ITIL(F), Six Sigma Green Belt trained. Consulting for the last 12 years on different management models like ISO 27001, COBIT, ISO 9000, ISO 14000, BS 15000, ISO 20000, TS 16949, QS 9000 and OHSAS 18001.
- **Jesus Benitez** - Big Four ISMS auditor
- **Anton Aylward** - CISSP, CISM, InfoSec consultant and IT Auditor for Canadian banks. COBIT user since its inception.
- **Richard Regalado** - Information Security Consultant (13 completed and certified ISMS projects); ISO 9000 Lead QMS Auditor (150 organizations audited to date)
- **Khawaja Faisal Javed** - CISA, MCP, MBA, IRCA reg. ISO27001 LA, itSMF reg. ISO 20000 LA, ISO 9001 LA, ISO 14001 LA, OHSAS18001 LA, IRCA approved ISMS Lead Tutor for Lead Auditor courses. More than 15 years in IT, InfoSec, System Analysis and Design, BPR QA/QC, including a management system auditing experience of more than 9 years.
- **Kim Sassaman** - ISO/IEC 27001 Lead Auditor, CISSP, IRCA Instructor for 27k LA course and Implementors course, member ISO/IEC JTC1 SC27 CS1.
- **Prasad Pendse** - ISO /IEC 27001 Lead Auditor,CISA

- **Mninikhaya Qwabaza (Khaya)** - IT Governance Officer - Information Assurance, governance, compliance, secure infrastructure design, DRP, IT Audit and evaluation, security assessment. Eight years hands-on experience in information security.
- **Javier Cao Avellaneda** -Information Security Consultant (1 completed and certified ISMS project), IRCA 27001 Auditor, CISA
- Plus **Renato Aquilino Pujol, Marappan Ramiah, Mooney Sherman, Jasmina Trajkovski, John South, Rob Whitcher, Alchap, Lakshminarayanan, Lee Evans, Rocky Lam, Pritam Bankar** and others who provided comments through the forum.

Document change record

March 12th 2008 – First release of the guideline completed and submitted to the ISO/IEC JTC1/SC27 committee working on ISO/IEC via Standards New Zealand.

Feedback

Comments, queries and improvement suggestions (especially improvement suggestions!) are welcome either via the ISO27k Implementers' Forum or to the project leader and forum administrator Gary Hinson. We plan to continue developing this guideline in parallel with ISO/IEC 27007 and the other ISO27k standards still in development.

Copyright

Appendix A - Generic ISO/IEC 27001 audit checklist

Introduction

The following checklist is generic. It reflects and refers to ISO/IEC 27001's requirements for Information Security Management Systems without regard to any specific ISMS requirements that an individual organization might have (for example if they are subject to legal, regulatory or contractual obligations to implement particular information security controls).

The checklist is primarily intended to guide, or to be adapted and used by, competent auditors including those working for internal audit functions, external audit bodies and ISMS certification bodies. It can also be used for internal management reviews of the ISMS including pre-certification checks to determine whether the ISMS is in a fit state to be formally audited. Finally, it serves as a general guide to the likely depth and breadth of coverage in ISMS certification audits, helping the organization to prepare the necessary records and information (identified in bold below) that the auditors will probably want to review.

The audit tests noted below are intended as prompts or reminders of the main aspects to be checked by competent, qualified and experienced IT auditors. They do not cover every single aspect of ISO/IEC 27001. They are not meant to be asked verbatim or checked-off piecemeal. They are not suitable for use by inexperienced auditors working without supervision.

*Reminder: the workplan/checklist is **not** intended to be used without due consideration and modification. It is anticipated that ISMS auditors will normally generate a custom workplan/checklist reflecting the specific scope and scale of the particular ISMS being audited, taking into account any information security requirements that are already evident at this stage (such as information-security relevant laws, regulations and standards that are known to apply to similar organizations in the industry). Also, the audit workplan/checklist may be modified during the course of the audit if previously underappreciated areas of concern come to light. Finally, the workplan/checklist should reflect the auditors' normal working practices, for example it may need additional columns to reference audit evidence, indicate SWOT/PEST analyses of the findings etc.*

ISMS audit test	Findings
4. Information security management system	
4.2.1a) Review the documented '**scope and boundaries' of the ISMS**, particularly any exclusions. To what extent does the ISMS match the organization? Are there justified reasons for excluding any elements?	
4.2.1b) Review the organization's **ISMS policy**. Does it adequately reflect the organization's general characteristics and its strategic risk management approach? Does it incorporate the organization's business requirements plus any legal or regulatory obligations for information security? Confirm that it has been formally approved by management and sets meaningful criteria for evaluating information security risks. [Note: in the context of ISO/IEC 27001, "ISMS policy" refers to management's statement of the main information security objectives or requirements, the overarching broad principles of information security. The more detailed information security policies, standards, procedures and guidelines will be reviewed under 4.2.1 and 4.2.2].	
4.2.1c) Ascertain and review the organization's choice/s of **risk assessment method/s** (whether bespoke or a generally-accepted method - see ISO/IEC 27005, when issued, for further guidance). Are the results of risk assessments comparable and reproducible? Look for any examples of anomalous results to determine how they were addressed and resolved. Was the risk assessment method updated as a result? Also review management's definition of criteria to accept or mitigate risks (the "risk appetite"). Is the definition sensible and practicable in relation to information security risks?	

ISMS audit test	Findings
4.2.1d) and e) Review the **information asset inventory** and **information security risks** identified by the organization. Are all relevant in-scope information assets included? Are accountable owners identified for all the assets? Review the analysis/evaluation of threats, vulnerabilities and impacts, the documentation of risk scenarios plus the prioritization or ranking of risks. Look for risks that are materially mis-stated or under-played, for example those where the corresponding controls are expensive or difficult to implement, perhaps where the risks have been misunderstood.	
4.2.1f) Review the organization's **Risk Treatment Plan**. Are appropriate "treatments" (*i.e.* mitigation through applying suitable controls, avoiding the risk, transferring the risk to third parties or knowingly accepting the risks if they fall within management's risk appetite) specified for all identified risks? Look for gaps and other anomalies. Check also whether recent changes (*e.g.* new IT systems or business processes) have been suitably incorporated, in other words is the Risk Treatment Plan being used and updated proactively as an information security management tool?	
4.2.1g) For those information security risks that are to be mitigated, review the defined **control objectives and selected controls** using suitable sampling *e.g.* stratified sampling by types of control (technical, physical, procedural or legal), by risk ranking (high, medium or low), by location (business units, sites/buildings *etc.*) or by other audit sampling criteria. Compare the objectives and controls against those suggested by ISO/IEC 27002 and summarized in Annex A of ISO/IEC 27001, in particular identifying and reviewing any significant discrepancies from the standards (*e.g.* commonplace objectives or controls from the standards that are not used by the organization, or any that may have been added). Also check that any information security requirements explicitly mandated by corporate policies, industry regulations, laws or contracts *etc.* are properly reflected in the documented control objectives and controls. [Note: the ISM audit checklist in Appendix B may prove useful in auditing the controls, but beware of sinking too much audit time into this one aspect]	
4.2.1h) Briefly evaluate the **residual information security risks**. Has management formally considered and approved them? Are they within the organization's defined **risk appetite**?	

ISMS audit test	Findings
4.2.1i) Confirm whether management has authorized the implementation and operation of the ISMS, for example through a **formal memorandum, project approval, letter of support from the CEO *etc.*** Is this a mere formality or is there evidence that management genuinely understands and supports the ISMS?	
4.2.1j) Review the organization's **Statement of Applicability** documenting and justifying the control objectives and controls, both those that are applicable and any that have been excluded/deselected. Confirm that suitable entries exist for all control objectives and controls listed in Annex A of ISO/IEC 27001. Has the Statement of Applicability been reviewed and endorsed/authorized by an appropriate level of management?	
4.2.2 Review **the ISMS as implemented and operated** against the documented ISMS requirements by sampling (see 4.2.1g and Annex A of ISO/IEC 27001). Look for evidence supporting or refuting the correlation between documented risks and controls and those actually in operation.	*[Note: this short checklist entry belies potentially a large amount of further audit work depending on factors such as the importance of the ISMS to the organization and to other stakeholders and hence the rigor and amount of audit sampling necessary to confirm the ISMS independently, the quality of the ISMS documentation and hence the amount of audit work necessary to obtain review it, and so forth. The ISM checklist in Appendix B indicates the range of audit tests potentially involved in fully reviewing information security management controls.]*
4.2.3 Review the **ISMS monitoring and review processes** using evidence such as plans, minutes of review meetings, management review/internal audit reports, breach/incident reports *etc.* Assess the extent to which processing errors, security breaches and other incidents are detected, reported and addressed. Determine whether and how the organization is effectively and proactively reviewing the implementation of the ISMS to ensure that the security controls identified in the Risk Treatment Plan, policies *etc.* are actually implemented and are in fact in operation. Also review ISMS metrics and their use to drive continuous ISMS improvements.	
4.2.4 Review the means by which the need for **ISMS improvements** are determined and improvements are implemented. Look for evidence in the form of management memos, reports, emails *etc.* documenting the need for improvements, authorizing them and making them happen.	

ISMS audit test	Findings
4.3.1 Review ISMS documentation including: • **ISMS policy statements, control objectives, procedures, standards, guidelines *etc*.** • **ISMS scope** • Management's choice of **risk assessment method/s** plus the risk assessment report/s arising and the **Risk Treatment Plan** • **Other procedures** relating to the planning, operation and review of the ISMS • **ISMS records** (see 4.3.3) • The **Statement of Applicability**	*[Note: section 4.3.1 briefly reiterates many aspects already covered. There is no need to review the ISMS documentation more than once if all requirements are taken into account and audited at the same time, but it is worth checking for and if necessary closing any gaps.]*
4.3.2 Check for the presence of, and compliance with, a documented **procedure for controlling updates** to ISMS documentation, policies, procedures, records *etc.* Determine whether ISMS documentation changes are formally controlled *e.g.* changes are reviewed and pre-approved by management, and are promulgated to all users of the ISMS documentation *e.g.* by updating a definitive reference set of materials maintained on the corporate intranet and/or explicitly notifying all applicable users.	
4.3.3 Evaluate the **controls protecting important ISMS records** such as various information security review and audit reports, action plans, formal ISMS documents (including changes to same), visitors' books, access authorization/change forms *etc*. Review the adequacy of controls over the identification, storage, protection, retrieval, retention time and disposition of such records, particularly in situations where there are legal, regulatory or contractual obligations to implement an ISMS in compliance with ISO/IEC 27001 (*e.g.* to protect personal data).	

ISMS audit test	Findings
5. Management responsibility	
5.1 Review the extent of management commitment to information security, using evidence such as: • Formal management approval of the ISMS policy manual • Management acceptance of ISMS objectives and implementation plans, along with the allocation of adequate resources and assignment of suitable priorities to the associated activities (see also 5.2.1) • Clear roles and responsibilities for information security including a process for allocating and accepting accountability for the proper protection of valuable information assets • Management memoranda, emails, presentations, briefings *etc.* expressing support for and commitment to the ISMS • Risk acceptance criteria, risk appetite *etc.* relating to information security risks • The scoping, resourcing and initiation of internal audits and management reviews of the ISMS	
5.2.1 Review the resources allocated to the ISMS in terms of budget, manpower *etc.*, in relation to the organization's stated aims for the ISMS and (where applicable) by comparison to comparable organizations (benchmarking). Is the ISMS adequately funded in practice? Are sufficient funds allocated by management to address information security issues in a reasonable timescale and to a suitable level of quality?	

ISMS audit test	Findings
5.2.2 Review the training of those specifically involved in operating the ISMS, and general information security awareness activities targeting all employees. Are necessary competencies and training/awareness requirements for information security professionals and others with specific roles and responsibilities explicitly identified? Are training/awareness budgets adequate to fund the associated training and awareness activities? Review training evaluation reports *etc*. and seek evidence to confirm that any necessary improvement actions have in fact been taken. Check by sampling that employee HR records note ISMS-related training *etc*. (where applicable). Assess the general level of information security awareness by surveying/sampling, or review the results of surveys/samples conducted as part of the ISMS.	
6. Internal ISMS audits	
6 Review the organization's internal audits of the ISMS, using ISMS audit plans, audit reports, action plans *etc*. Are responsibilities for conducting ISMS internal audits formally assigned to competent, adequately trained IT auditors? Determine the extent to which the internal audits confirm that the ISMS meets its requirements defined in ISO/IEC 27001 plus relevant legal, regulatory or contractual obligations, organizational ISMS requirements specified through the risk assessment process. Check that agreed action plans, corrective actions *etc*. are generally being addressed and verified within the agreed timescales, paying particular attention to any currently overdue actions for topical examples.	*[Note: it is quite normal for some corrective actions agreed as part of ISMS audits to remain incomplete at the agreed completion dates, especially in the case of recommendations that are complex, costly or involve third parties. The point is not that everything must be done exactly as planned so much as that management remains on top of the situation, proactively managing the work and allocating sufficient resources to achieve a sensible rate of progress, with a reasonably proportion of agreed actions being completed 'on time'. Continuous ISMS improvement more important than strict compliance with the plans – see also section 8.]*
7 Management review of the ISMS	
7.1 Determine when management has previously reviewed the ISMS, and when it next plans to do so. Such reviews must occur at least once a year. The frequency of reviews must be defined *e.g*. in the ISMS policy or ISM policy manual.	*[Note: it is a moot point whether an ISMS certification audit, performed at management's request, could be considered a "management review" within the terms of the ISO/IEC standard.]*

ISMS audit test	Findings
7.2 By reviewing management reports and other records, and/or by interviewing those who were involved, check what went in to the previous management review/s (ISO/IEC 27001 identifies nine items such as the results of other audits/reviews, feedback and improvement suggestions, information on vulnerabilities and threats *etc.*). Assess the extent to which management played an active part and was fully engaged in the review/s.	
7.3 Check the outputs of any previous management review/s including key management decisions, action plans and records relating to the confirmation that agreed actions were duly actioned. If necessary, confirm that closed actions have in fact been properly completed, focusing perhaps on any that were not completed promptly or on time.	
8 ISMS improvement	
8.2 Obtain and review information relating to ISMS corrective actions such as reports and action plans from ISMS management review/s or audits (see 7.3), ISMS change requests, budget/investment proposals and business cases *etc.* Seek evidence that the ISMS is in fact being materially improved as a result of the feedback - more than just fine words, check the documentation relating to closure of action plan items *etc.* to confirm whether nonconformities and their root causes are actually being resolved by management within reasonable timescales. Review that the corrective actions taken address the root cause of the nonconformities and are effective.	
8.3 In addition to making ISMS improvements resulting from actual nonconformities previously identified, determine whether the organization takes a more proactive stance towards addressing potential improvements, emerging or projected new requirements *etc.* Seek evidence of ISMS changes (such as adding, changing or removing information security controls) in response to the identification of significantly changed risks.	
*** End of checklist ***	

Appendix B - Generic ISO/IEC 27002 audit checklist

Introduction

The following checklist is generic. It reflects and refers to ISO/IEC 27002's requirements for Information Security Management Systems without regard to any specific control requirements that an individual organization might have in relation to information security risks identified through the risk assessment and risk management processes.

This is a generic checklist to guide a general review of the organization's security controls against the guidance provided in ISO/IEC 27002. It cannot provide specific guidance on the particular risks and controls applicable to every situation and must therefore be customized by an experienced IT auditor to suit the situation. For example, the organization's risk analysis may have determined that certain control objectives are not applicable and hence the corresponding controls may not be required, whereas in other areas the control objectives may be more rigorous than suggested in the standard and additional controls may be required. The Risk Treatment Plan should provide further details on this.

The audit tests noted below are intended as prompts or reminders of the main aspects to be checked by competent, qualified and experienced IT auditors. They do not cover every single aspect of ISO/IEC 27002. They are not meant to be asked verbatim or checked-off piecemeal. They are not suitable for use by inexperienced auditors working without supervision.

*Reminder: the workplan/checklist is **not** intended to be used without due consideration and modification. It is anticipated that ISMS auditors will normally generate a custom workplan/checklist reflecting the specific scope and scale of the particular ISMS being audited, taking into account any information security requirements that are already evident at this stage (such as information-security relevant laws, regulations and standards that are known to apply to similar organizations in the industry). Also, the audit workplan/checklist may be modified during the course of the audit if previously underappreciated areas of concern come to light. Finally, the workplan/checklist should reflect the auditors' normal working practices, for example it may need additional columns to reference audit evidence, indicate SWOT/PEST analyses of the findings etc.*

ISM audit test	Findings
5. Security policy	
5.1 Information security policy. Are the organisation's Information Security Management (ISM) policies available locally? Are the policies communicated, understood and accepted? Obtain and review copies of any local Business Unit (BU) policies, standards, procedures, guidelines *etc.* covering ISM, such as: • Standards for physical security of the computer and telecommunications installation and associated facilities; • HR procedures governing access to and use of IT services (*e.g.* issue of usernames and passwords, disciplinary procedures); • End user guidelines covering PC software licensing and virus prevention**.** • Check issue status, confirm when last reviewed and whether any recent changes have been incorporated**.** Are references to relevant standards (*e.g.* ISO/IEC 27002) and laws (*e.g.* Computer Misuse Act, Privacy/Data Protection Act) incorporated? Do BU standards *etc.* comply with the organisation policies? Are they reasonable and workable? Do they incorporate suitable and sufficient controls? Do they cover all essential computing and telecommunications services? Would any of the BU standards, guidelines *etc.* be useful/applicable elsewhere in the organisation (best practice)?	

ISM audit test	Findings
6. Organizing information security	
6.1 Internal organization. Identify BU ISM structure and main contacts for this audit, whether employees, outsourced, contractors or consultants *e.g.*: • Senior manager responsible for IT and ISM (often the audit sponsor); • Information security professionals; • Security administrators; • Site/physical security manager and Facilities contacts; • HR contact for HR matters such as disciplinary action and training; • Systems and network managers, security architects and other IT professionals. Review ISM structure. Is ISM given sufficient emphasis (is there a 'driving force'?) and management support? Is there a senior management forum to discuss ISM policies, risks and issues? Are roles and responsibilities clearly defined and assigned to skilled individuals? Is there a budget for ISM activities (*e.g.* awareness campaigns)? Is there sufficient co-ordination both within the BU, between BUs and with HQ? Are the information flows (*e.g.* incident reporting) operating effectively in practice?	

ISM audit test	Findings
6.2 External parties. Ascertain the arrangements to identify and implement ISM requirements for 3rd-party connections. Is there a risk analysis process in place for 3rd-party communications connections? Who has responsibility for ensuring that all 3rd-party links are in fact identified and risk assessed? Is a comprehensive register of authorised 3rd-party connections and modems maintained? Are ISM arrangements in operation on 3rd-party connections routinely reviewed against the requirements? Are there formal contracts covering 3rd-party links, if so do they cover ISM aspects (*e.g.* specific mention of ISO/IEC 27002 and corporate ISM standards)? Where applicable, does the outsourcing contract adequately address the following issues: • Ownership and responsibility for ISM issues? • Legal requirements (see section 15.1) • Protection of systems, networks and data via physical, logical and procedural controls *e.g.* risk assessment, integrity and confidentiality of business assets, availability of services in the event of disasters, management notification/escalation route for security incidents, security clearance of staff? • The right of audit by the organisation?	
7. Asset management	
7.1 Responsibility for assets. Review arrangements to establish and maintain an inventory of information assets (computer and communications hardware/systems, application software, data, printed information). How is the inventory maintained fully up-to-date, accurate and complete despite equipment/staff moves, new systems *etc.*? Is there a 'registration process' for new application systems? Are there asset tags on all PCs, network equipment *etc.*? Are power and data cables clearly labelled and are wiring diagrams kept complete and up-to-date?	

ISM audit test	Findings
7.2 Information classification. Establish whether classification guidelines are in place, covering business requirements for confidentiality, integrity and availability. Are appropriate markings used on documents, forms, reports, screens, backup media, emails, file transfers *etc.*? Are staff made aware of the corresponding security requirements for handling sensitive materials (*e.g.* no 'secret' data to be generated, processed or stored on any system connected to the main corporate LAN/WAN or Internet)?	
8. Human resources security	
8.1 Prior to employment. Determine whether information security roles and responsibilities are defined in job descriptions, terms and conditions of employment *etc.* for specific IT security staff, system/network managers, managers and end users in general. Are there suitable confidentiality and similar clauses? Are staff and contractors recruited into sensitive positions pre-screened (including taking out of references and security clearance where appropriate)? Are there enhanced screening processes for staff/managers in particularly sensitive roles (*e.g.* those with ROOT-equivalent access to sensitive systems) or sites? Are there appropriate HR policies and procedures *e.g.* disciplinary actions for staff and contractors that transgress IT security rules?	
8.2 During employment. Review information security awareness, training and educational arrangements. Do end users and their managers routinely receive appropriate training on information security including roles and responsibilities, login procedures *etc.*, within the context of general IT systems training? Review disciplinary procedures, ideally using one or more recent cases involving information security to assess the process as followed.	

ISM audit test	Findings
8.3 Termination or change of employment. Review policies, standards, procedures and guidelines relating to information security elements of the termination process *e.g.* retrieving information assets (papers, data, systems), keys, removal of access rights *etc.*	
9. Physical and environmental security *[Note: this part of the ISM audit checklist goes into more detail than ISO/.IEC 27002 section 9.2]*	
9.1 Secure areas. Check defined security perimeter to site and IT rooms. Are facilities discreet and sited to minimise disaster potential or cost of protective countermeasures (*e.g.* not adjacent to canteen or runway)? Is the construction physically sound *e.g.* walls go "slab-to-slab", thick solid doors, all windows strong and permanently locked (care: fire exit requirements may conflict)? Are suitable access control systems employed (*e.g.* card-swipe, security locks, CCTV, intruder detection) with matching procedures (*e.g.* key issue/return, regular access code changes, out-of-hours inspections by security guards, visitors routinely escorted and visits logged in room visitors book)? Is there appropriate physical protection for external cables, junction boxes, air conditioner chillers, microwave dishes, air inlets *etc.* against accidental damage or deliberate interference?	

ISM audit test	Findings
9.2 Equipment security ***Fire and smoke protection:*** review protection/controls *e.g.* fire/smoke alarm system with local and remote sounders, no smoking policy in and around computer and telecommunications rooms, appropriate fire suppression equipment (*e.g.* suitable fire extinguishers at marked fire points near doors, CO_2 flood systems *etc.* ["gas-tight" rooms if CO_2 is used]), fire-resistant/low-smoke construction materials, wiring *etc.* including fire-doors, proper fire-stopping/smoke sealing of voids, cable runs *etc.* Is there any evidence of smoking? Are no-smoking signs displayed? Are fire systems and interlocks regularly inspected and maintained *e.g.* fire safety inspections by competent fire safety engineers and, where appropriate, direct contact with local fire service (check maintenance records/contracts/fire certificates). Check training and awareness of fire evacuation procedures *etc.* including visitors and maintenance staff and out-of-hours working.	
Power supply: computer-grade "on-line" UPS - permanent filtered supply – for shared systems (servers, PABX, communications hubs *etc.*). Adequate UPS capacity to support all essential computer equipment and peripherals, and all such equipment in fact uses the secure supply. Back-up generator, operated and maintained as per manufacturer's specifications and tested on-load regularly (~monthly). Dual-routed mains supplies where available (feeds from separate substations).	
Air conditioning: computer-grade air conditioners properly fitted. Chillers/condensers appropriately sited. Adequate A/C capacity to support heat load. Redundant/spare units or portables available to improve resilience and permit maintenance without affecting service. Temperature sensing with remote-reading over-temperature alarms and incident procedures. A/C equipment installed, operated and maintained regularly as per manufacturer's specifications. Appropriate procedures (including how to deal with alarms).	

ISM audit test	Findings
Water/flood protection: facilities appropriately sited to minimize flood potential (*e.g.* above water table, not adjacent to water tanks, no water pipes overhead *etc.*). Where appropriate, additional/secondary protection installed *e.g.* waterproof membranes, drip trays under A/C units, water detection with remote alarms and incident procedures. Regular surveys of roofs, under-floor voids, *etc.* for signs of water leakage/penetration.	
Dust avoidance: check that computer and telecommunications rooms are maintained in clean condition *e.g.* specialist "deep cleaned" including floor and ceiling voids, low dust wall covering, under-floor sealed.	*[Note: cleaners in sensitive areas such as computer rooms should always be accompanied, or else cleaning should be done, by IT staff. Cleaners may need to be security cleared if the organization uses government classified information.]*
Earthing and lightning protection: confirm that all exposed metalwork is earth bonded to a common safety earth point for both safety and static reduction reasons. Confirm the use of mounted lightning conductors, cable isolators, fuses *etc.* where applicable (see BS 6651). Are these controls tested annually and following major changes?	
Other physical security controls: verify the following: • Clear desk policy and clear screen policy • Adequate protection of removable assets *e.g.* laptops and PDAs • Management authorization process for removal of information assets from site • Secure disposal processes to erase sensitive corporate and personal data fully from removable or fixed media before disposal.	

ISM audit test	Findings
10. Communications and operations management	
10.1 Operational procedures and responsibilities. Review general state of documented IT procedures for general IT operations, systems and network management, incident management, IT security admin., change management *etc.* Is there a full set of security procedures in place and when were they last reviewed? Are the procedures reasonably well controlled? Are information security aspects properly included (*e.g.* incompatible duties segregated to separate staff, incident notification procedures *etc.*)? Are corresponding responsibilities assigned to individuals?	
10.2 Third party service delivery management. If applicable, review the controls addressing information security risks arising from outsourced IT/IT Service Delivery. Check whether 3rd party IT services and/or the service providers are routinely monitored for security compliance (with both internal and external security requirements) and actual or potential security incidents. Are security aspects covered in regular relationship management meetings, reports *etc.*? How are any changes in the security risks identified and responded to?	
10.3 System planning and acceptance. Review capacity planning including CPU usage, disk space, network capacity *etc.* How are acceptance tests (including IT security aspects) completed prior to the introduction of new systems onto the network? Are DCP/fallback arrangements updated to reflect new/retired systems?	

ISM audit test	Findings
10.4 Protection against malicious and mobile code. Review malware protection. Review malware incident response procedures and any malware incident reports. Are there continuous/frequent virus-checks on all PCs including standalones/portables? Are infection levels minimised (is the situation broadly under control)? Are staff and managers aware of the procedures? How is anti-virus software updated – is it manual or automated? Are viruses detected by scanners reported to an appropriate co-ordinator? If notification is manual, roughly what proportion is probably notified (all, most, some or just a few)? What protection is there against Trojans, worms, spyware, rootkits, keyloggers *etc.*?	
10.5 Backups. Check the backup strategies and procedures. Are they documented and tested? Do the strategies cover data, programs, system files, parameter files *etc.* for all systems including servers, desktops, phone/network systems, system/network management systems, standalone/portable systems, control systems *etc.*? Are backup frequencies and types appropriate? Are backup media protected against loss, theft, damage, fire including both on-site and off-site/remote storage *e.g.* are fire safes BS-certified or better and normally locked shut? Using a small sample, check whether backup tapes listed in the procedures/records actually exist in the right place and are properly labelled. Request proof of management review of backups against backup policy	
10.6 Network security management. Review the security elements of network management procedures. Are they properly documented? Are information security aspects such as security arrangements for 3rd-party connections adequately covered?	

ISM audit test	Findings
10.7 Media handling. Review computer media handling procedures. Is there an up-to-date and complete asset register for tapes, removable disk packs, CDs *etc.*? Are tapes *etc.* properly labelled? Are archival media duplicated and verified prior to deletion of source data? Are archive tapes periodically verified and re-tensioned as per manufacturer's specifications (typically annually)? Are there appropriate controls to maintain confidentiality of stored data (*e.g.* limited access to tapes and drives, end users not given direct access to tapes/drives, special courier arrangements for the most sensitive media)?	
10.8 Exchange of information. Review policies and procedures for data exchanges *e.g.* communications network links, dial-up links, tape transfers *etc.* Are there suitable security controls (*e.g.* trusted couriers, link encryption, authentication and non-repudiation *etc.*)? Also review security arrangements for Internet, Intranet and related systems (bulletin boards *etc.*).	
10.9 Electronic commerce services. If the organization uses or provides Web-based applications or other eCommerce systems, review the corresponding information security controls over access and user authentication, data integrity and service availability. Check for the enforced use of https, for example, to protect sensitive data *en route* between browser and Web server. Review system security documentation.	
10.10 Monitoring. Ascertain how the main systems monitor, log and report security incidents. Who is responsible for reviewing and following-up on reports? Is the process running reasonably well in practice? Is there a process in place for reviewing and responding appropriately to security alerts from vendors, CERTs, government sources *etc.*? Check for evidence that the process is working effectively.	

ISM audit test	Findings
11. Access control	
11.1 Business requirements for access control. Are business requirements for access control *etc.* properly documented and approved by information asset owners *e.g.* in system security design specifications? Review a sample of design documents (*e.g.* for major business systems) for breadth and depth of coverage of business requirements for access control and related information security issues.	
11.2 User access management. Review security administration processes and systems by observing them in action, interviewing security administrators and reviewing documentation such as security admin system designs, procedures and forms. Evaluate the controls in place to prevent people gaining unauthorized access to systems, for example by fraudulently obtaining user IDs or passwords. Explore the security admin processes relating to joiners, movers and leavers. Sample user admin records for evidence that user IDs and password changes are properly authorized, that granted access rights are normally limited as far as practicable, and that access rights are regularly reviewed and if necessary promptly revoked (*e.g.* cross-check a small sample of security admin records against active accounts to ascertain whether all active accounts were properly authorized and appropriate access was granted, and look for user accounts for people who have recently left that have not been disabled/deleted). When was the last user account review performed (review results)?	*[Note: pay special attention to **privileged users**. Review system access/account controls for the users of privileged system-, database-, application- & network-managers user IDs such as ADMIN and ROOT. Verify that there are enhanced controls to reflect the greater potential for abuse of privileges e.g. special account authorisation procedures and monitoring systems to detect & respond to any such abuse. Is there a process in operation for more frequent regular reviews of privileged accounts to identify & disable/delete redundant privileged accounts and/or reduce the privileges?]*
11.3 User responsibilities. Review the organization's password controls *e.g.* policies on minimum password length, maximum password lifetime, enforced complexity rules, forced change of passwords on first use *etc.* Evaluate the mix of technical/automated controls and manual procedures, management reviews *etc.* Does anyone routinely check for weak passwords and follow-up with user security awareness/training?	

ISM audit test	Findings
11.4 Network access control. How are network access points secured against unauthorized access? How does the system limit access by authorized individuals to legitimate applications/services? Are users authenticated appropriately at logon (including dial-in and remote/Web users)? How are network nodes authenticated and are distinct security domains established using firewalls *etc.*? Confirm protection of system management ports *e.g.* secure modems, challenge-response systems, key lock-out *etc.*	
11.5 Operating system access control. Evaluate security controls relating to secure logon, user identification and authentication, password management, use of system utilities, session timeout and limited connection times. Are session timeouts implemented on the desktop, network, application or operating system levels, for example, and if the former, is it possible for someone to hijack an active session?	
11.6 Application and information access control. Review security designs or other documentation for a sample of major systems to determine whether suitable access controls are in place, including the use of individual user identities, user authentication, automated access controls, encryption *etc.*	
11.7 Mobile computing and teleworking. Review security controls relating to mobile and home users *e.g.* the use of corporate laptops, PDAs, USB/other mobile storage devices, VPNs *etc.* How are portable systems maintained and controlled (*e.g.* to ensure that they are kept up to date on antivirus definitions and security patches)? Confirm that all portable devices containing sensitive proprietary of personal data employ adequate access controls, normally implying whole-disk encryption and often strong user authentication.	

ISM audit test	Findings
12. Information systems acquisition, development and maintenance	
12.1 Security requirements of information systems. Determine whether formal systems development methods are used routinely and whether they insist on risk analysis, information security functional requirements specifications, security designs, security testing *etc.* Also assess whether changes to systems (*e.g.* maintenance updates, operating system/application upgrades, crypto changes *etc.*) trigger security reviews/risk assessments and, if necessary, re-certification of systems.	
12.2 Correct processing in applications. Briefly review security designs for a small sample of major systems to determine whether controls such as input data validation, processing validation, encryption, message authentication *etc.* are employed appropriately.	
12.3 Cryptographic controls. Has a formal policy covering the use of cryptographic controls been implemented? Ensure that it covers: • The general principles under which business information should be protected; • Standards to be applied for the effective implementation of crypto; • A process to determine the level the level of protection to be applied; • Management of crypto keys, including recovery of information in the event of lost, damaged or compromised keys; • Alignment with any documented requirements relating to IT equipment or services covered by contracts.	
12.4 Security of system files. Review the controls isolating development from testing from production environments. How is software promoted and released? Who is responsible for ensuring that new/changed software does not disrupt other operations? How are test data derived and protected against disclosure?	

ISM audit test	Findings
12.5 Security in development and support processes. Review change control procedures. Are they documented and appropriate? Do they cover significant changes to computing and telecommunications equipment (hardware), key operating system parameters and software, application software *etc.*? Review a small sample of change control records. Are changes properly documented, justified and authorized by management?	
12.6 Technical vulnerability management. Evaluate how the organization identifies and responds to technical vulnerabilities in desktops, servers, applications, network devices and other components, for example by reviewing change control records for evidence relating to recent patches. Are there suitable processes in place to review the inventory of systems and identify whether announced vulnerabilities are relevant? Are patches assessed for applicability and risks before being implemented? Are the processes for implementing urgent patches sufficiently slick and comprehensive? To what extent does the organization depend on automated patch management, in effect accepting the associated risks of implementing rogue patches? Look for any evidence of important systems that have not been maintained at current release levels and/or patched against known vulnerabilities.	
13. Information security incident management	
13.1 Reporting information security events and weaknesses. Check the processes for reporting security events and weaknesses. Trace the process using a sample of documentation such as Help Desk records, comparing what actually happened with the policies, procedures and guidelines. Confirm that those who should be reporting security events and weaknesses are aware of, and in fact use, the process.	

ISM audit test	Findings
13.2 Management of information security incidents and improvements. Review the evaluation/investigation, corrective action and later parts of the processes for managing security incidents and improvement opportunities. Does the organization have a relatively mature incident management process in place? Is it proactively learning from incidents, improving risk knowledge and security controls accordingly? Check the records relating to recent incidents for further evidence.	

ISM audit test	Findings
14. Business continuity management	
14.1 Information security aspects of business continuity management. Evaluate the way the organization determines and satisfies its business continuity requirements. Review the associated policies, procedures, standards and guidelines. Determine whether suitable 'high availability' designs are employed for IT systems, networks *etc*. supporting critical business processes. Verify whether those involved understand the risks the organization is facing, correctly identify business critical processes and the associated assets, identify potential incident impacts, and mandate suitable preventative, detective and corrective controls. Evaluate business continuity plans, continuity exercises/tests *etc*. by sampling and reviewing the process documentation, reports *etc*. Verify that events likely to interrupt business processes will be promptly identified and assessed, triggering disaster recovery-type activities. Verify that suitable plans are in place to maintain business operations or restore them within defined timeframes following interruption or failure. Do the plans take into account the identification and agreement of responsibilities, identification of acceptable loss, implementation of recovery and restoration procedure, documentation of procedure and regular testing/exercises? Verify that there is a single coherent framework for business continuity planning. Verify whether the framework ensures that all plans are consistent and identifies priorities for testing and maintenance. Determine whether the business continuity plans and the planning process, taken as a whole, are adequate to satisfy the identified information security requirements. Verify if business continuity plans are regularly exercised/tested to ensure that they are remain up to date and effective. Verify whether members of the crisis/incident management and recovery teams and other relevant staff are aware of the plans and are clear on their personal roles and responsibilities.	

ISM audit test	Findings
15 COMPLIANCE	
15.1 Compliance with legal requirements. Ascertain how statutory, regulatory, contractual and business requirements for information security that are relevant and applicable to the organization, are identified, including changes and new requirements. Determine whether the organization is subject to specific legal obligations for data protection and privacy (such as HIPAA, Act of Protection of Personal Information, Data Protection Act, Privacy Act *etc*.) and/or similar contractual obligations, then ascertain whether the corresponding information security controls are in place. Check for example that procedures are in place to comply with requirements on the use of copyright materials, such as software licenses. Ascertain how important organizational records are protected from loss, destruction and falsification in accordance with statutory, regulatory and business requirements. Do the storage/archival arrangements take account of the possibility of media deterioration (*e.g.* controlled storage conditions, periodic integrity checks and/or transfer to fresh media)? Are appropriate long-life storage media used for long term storage? Review policies and practices to determine whether the use of IT facilities for any non-business or unauthorized purpose, without management approval, is treated as improper use. Verify whether an appropriate warning message is presented to users that they must acknowledge to continue with the log-on process. Verify whether any monitoring procedures have been approved by legal counsel. Verify whether the use of cryptography is in compliance with all relevant laws, agreements/contracts and regulations.	

ISM audit test	Findings
15.2 Compliance with security policies and standards, and technical compliance. Verify whether managers ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards. Verify the regular review of the compliance of information processing facility within their area of responsibility for compliance with appropriate security policies and standards. Verify whether information systems are regularly checked for compliance with applicable security implementation standards. Verify whether technical compliance checks are carried out by, or under the supervision of, competent, authorized personnel using suitable tools where applicable.	
15.3 Information systems audit considerations. Verify whether audit requirements involving checks on operational systems are carefully planned and agreed to minimise the risk of disruptions to business process. Verify whether the audit requirements, scope are agreed with appropriate management. Verify that access to information system audit tools/software is controlled to prevent misuse and compromise. Verify the segregation of system audit tools from development and operational systems, unless given an appropriate level of protection.	
*** End of checklist ***	