



**IRCA**

INTERNATIONAL  
REGISTER OF  
CERTIFICATED  
AUDITORS



Certification criteria for

# Information Security Management Systems Auditor Conversion Training Course

# CONTENTS

1. INTRODUCTION
2. PRIOR KNOWLEDGE REQUIREMENTS
3. LEARNING OBJECTIVES
4. ENABLING OBJECTIVES – KNOWLEDGE & SKILLS
5. TRAINING METHODS
6. COURSE CONTENT
7. COURSE DURATION
8. TUTORS & STUDENTS
9. VARIATIONS
10. STUDENT ASSESSMENT & EXAMINATION
11. COURSE PUBLICITY & ADVERTISING

## APPENDIX 1: NOTES FOR GUIDANCE

### **Copyright IRCA – 2006**

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means - electronic, mechanical, photocopying, recording or otherwise, without prior permission of the CQI International Register of Certificated Auditors (IRCA).

## 1. INTRODUCTION

- 1.1 We, the International Register of Certificated Auditors (IRCA), have developed this document to help you, the Training Organization, achieve certification of an IRCA/2060, **Information Security Management Systems (ISMS) Auditor Conversion** training course.
- 1.2 Before designing an *ISMS Auditor Conversion* training course to meet the requirements of this document you should consider the following:
- 1.2.1 **Aim of this course.** ISO 27001:2005 provides all types of industry and commerce with a useful international specification for managing and improving information security within organizations. The aim of this course is to equip students with the knowledge and skills required to perform audits of information security management systems against ISO/IEC 27001:2005 in accordance with ISO 19011 and EA 7/03.
- 1.2.2 **Auditor certification.** Students who successfully complete this *ISMS Auditor Conversion* training course certified by IRCA (within the three years prior to making an application to become a certificated auditor) will satisfy part of the training requirements for initial certification as an IRCA *ISMS Auditor* (IRCA/802).
- 1.2.3 **Reference standards and documents.** The course content is based on the international standard ISO/IEC 27001:2005, the international standard ISO/IEC 17799:2005 and ISO/IEC TR 13335 Parts 1 and 2 (MICTS) and ISO/IEC TR 18044:2004. Unless otherwise indicated, all references within this document to ISO/IEC 27001 will indicate the ISO/IEC 27001:2005 version.
- 1.2.4 **Flexibility in course design:** These criteria specify the requirements for training courses including the knowledge and skills to be covered during the course. Your training course must be designed and delivered in accordance with these criteria, although you may exercise flexibility in the inclusion of additional material, and in the structure and selection of specific training methods used during the course. Many of the certification requirements common to the management and control of courses are detailed in IRCA/2000, *Requirements for training organization approval*. These requirements are in addition to the requirements of this document and are mandatory. It is essential, therefore, that you are familiar with the requirements of IRCA/2000.
- 1.2.5 **Training methods.** This course may be designed to be presented in a variety of ways:
- a. Classroom-based over 3 days full-time (i.e. over three consecutive working days).
  - b. Classroom-based as a series of part-time modules over a longer period.
  - c. Blended as a combination of self-study (i.e. e-learning course, correspondence course etc) and classroom-based learning.
- 1.2.6 **Training vs Assessment.** There must be two distinct aspects to courses based on these criteria:
- a. Effective training to help students develop the knowledge and skills defined in this document.
  - b. Effective assessment of each individual student's achievement of the learning objectives through objective testing based on defined outputs.

## 2 PRIOR KNOWLEDGE REQUIREMENTS

- 2.1 This course is designed for experienced management systems auditors who are also information security professionals, with an understanding of the principles and concepts underlying information security management, who seek an understanding of the skills required to audit effectively against ISO/IEC 27001. It is not intended to be an implementer's course, or one that will create an expert in the relevant legislation, or one that will train to an acceptable standard a student with no prior knowledge of the standard or of information security management systems.
- 2.2 Before attending this training course students who intend to seek certification as an ISMS auditor with IRCA are required to have successfully completed an IRCA certified (or equivalent) 5-day Lead Auditor training course in another discipline (QMS, EMS, FSMS, OH&S etc)<sup>1</sup>.
- 2.3 You must inform prospective students of the required pre-course knowledge and provide clear guidance for tutors, who find that they have students lacking this prior knowledge, to ensure that this does not adversely affect other students' learning on this course.

## 3. LEARNING OBJECTIVES

- 3.1 Learning Objectives describe in outline what successful students will know and be able to do by the end of the course. By the end of the course students will be able to:

### **Knowledge:**

- 3.1.1 Explain the purpose of an information security management system (ISMS) and explain the processes involved in establishing, implementing, operating, monitoring, reviewing and improving an ISMS as defined in ISO/IEC 27001 including the significance of these for ISMS auditors (see also 4.1).
- 3.1.2 Explain the purpose, content and interrelationship of ISO/IEC 27001, ISO/IEC 17799 and ISO 19011, ISO/IEC 13335 Parts 1 and 2 (MICTS), and ISO/IEC TR 18044:2004 and EA 7/03 and the legislative framework relevant to an ISMS (see also 4.2).

### **Skills:**

- 3.1.3 Interpret the requirements of ISO/IEC 27001 and EA 7/03 in the context of an ISMS audit (see also 4.3).
- 3.1.4 Undertake the role of an auditor to plan, conduct, report and follow up an audit in accordance with ISO 19011 (see also 4.4).

---

<sup>1</sup> Note that students who successfully complete this course and wish to apply for certification as an ISMS Auditor must be able to demonstrate to IRCA that he/she has completed this course.

#### 4. ENABLING OBJECTIVES – KNOWLEDGE & SKILLS

In order for students to achieve the overall Learning Objectives, they will need to acquire and develop specific **knowledge** and **skills**. These are specified below as Enabling Objectives and can be considered as steps to the achievement of the Learning Objectives. By the end of the course students must be able to:

##### 4.1 Explain the purpose of an information security management system (ISMS) and explain the processes involved in establishing, implementing, operating, monitoring, reviewing and improving an ISMS as defined in BS ISO/IEC 27001, including the significance of these for ISMS auditors.

###### Knowledge:

- 4.1.1 Explain the purpose and business benefits of an information security management system.
- 4.1.2 Explain the process approach to information security management systems.
- 4.1.3 Explain the processes involved in establishing, implementing and operating, monitoring and reviewing and improving an ISMS, including the significance of this for ISMS auditors.
- 4.1.4 Describe in detail what is involved in selecting a system of controls through the process of risk assessment, treatment and management, including:
  - a) ISMS scope and policy.
  - b) Identifying and explain the element of the risk assessment process.
  - c) Risk treatment plan and options.
  - d) Risk reduction through the selection and implementation of a system of controls.
  - e) Statement of Applicability in relation to an organization's business activities and associated risks.
- 4.1.5 Explain the importance and methods used in security incident handling and business continuity.

##### 4.2 Explain the purpose, content and interrelationship of ISO/IEC 27001, ISO/IEC 17799 and ISO 19011, ISO/IEC 13335 Parts 1 and 2 (MICTS), and ISO/IEC TR 18044:2004 and EA 7/03 and the legislative framework relevant to an ISMS.

###### Knowledge

- 4.2.1 Describe the difference between auditable standards and guidance documents and standards.
- 4.2.2 Explain the purpose and content of ISO/IEC 17799 and its relationship to ISO/IEC 27001.
- 4.2.3 Explain the control objectives and controls defined in Annex A of ISO/IEC 27001 drawing on ISO/IEC 17799
- 4.2.4 Explain the purpose and content of ISO/IEC 13335 Parts 1 and 2 (MICTS) the role it plays in using ISO/IEC 27001.
- 4.2.5 Explain ISO/IEC 27001 related concepts and terminology of quality management systems, drawing on ISMS terminology and definitions.

- 4.2.6 Explain the difference between legal compliance and conformance with ISO standards and outline relevant applicable legislation, intellectual property rights, data protection and privacy of personal information.

**4.3 Interpret the requirements of ISO/IEC 27001 and EA 7/03 in the context of an ISMS audit.**

**Skills**

- 4.3.1 Draw links between the PDCA model and correctly apply this to the ISMS process requirements specified in ISO/IEC 27001.

- 4.3.2 Interpret and apply ISO/IEC 27001 appropriately in an audit situation.

- a) Suggest what objective evidence might be needed to demonstrate conformance with ISO/IEC 27001 requirements.
- b) Verifying the scope of ISMS certification in the context of ISO/IEC 27001.
- c) Auditing multi-site ISMS scopes and the use of a sample based approach to multiple site assessments.
- d) Describe the basis on which exclusion of controls might be permissible to comply with all requirements of ISMS.

- 4.3.3 Check and confirm the following ISMS audit objectives:

- a) That the organization adheres to its own policies, objectives and procedures.
- b) That the ISMS conforms with all the requirements of the ISMS standard or normative document and is achieving the organization's policy objectives.

- 4.3.4 Identify and evaluate in an ISMS audit context:

- a) Assessment of information security related risks to control of its organizational assets and the resulting design of the ISMS.
- b) The organization's security risk assessment approach, including the assessment of the adequacy of any given approach.
- c) The suitability of the organization's Statement of Applicability in relation to its business activities and associated risks.
- d) Objectives and targets derived from this process.
- e) Performance monitoring, measuring, reporting and reviewing against the objectives and targets.
- f) Security and management reviews.
- g) Management responsibility for the information security policy.
- h) Links between policy, the results of information security risk assessments, objectives and targets, responsibilities, programmes, procedures, performance data, and security reviews.
- i) The activities and/or controls which the organization is permitted to exclude from their ISMS.

4.3.5 Evaluate the information security related threats to assets, vulnerabilities and impacts on the organization.

- a) Establishing and maintaining procedures for the identification, examination and evaluation of information security related threats to assets, vulnerabilities and impacts on the organization, taking account of the following factors:
  - i. The criteria by which information security related threats to assets, vulnerabilities and impacts on the organization are identified as significant, and to develop procedure(s) for doing this.
  - ii. That the analysis of security related threats is relevant and adequate for the operation of the organization.
  - iii. There is no inconsistency between the organization's policy, objectives and targets and its procedure(s) or the results of their application.
- b) The procedures employed in analysis of significance are sound and properly implemented. If an information-related threat to assets, vulnerability or an impact on the organization is identified as being significant, it should be managed within the ISMS.

4.3.6 Evaluate regulatory and legal compliance:

- a) The organization has a management system that should achieve continuing compliance with regulatory requirements applicable to the information security impacts of its activities, products and services and that this system is fully implemented.
- b) The organization has evaluated legal and regulatory compliance and can show that action has been taken in cases of non-compliance with relevant regulations.

**4.4 Undertake the role of an auditor to plan, conduct, report and follow up an ISMS audit in accordance with ISO 19011**

**Skills**

4.4.1 Undertake the roles of an auditor and/or audit team leader to:

- a) Write an audit scope, prepare an on-site ISMS audit plan that is appropriate to the sequence and interaction of the organization's business processes, their information security safety risks, and produce a process-based audit checklist (or alternative).
- b) Perform a stage one audit in order to assess whether documentation meets ISO/IEC 27001 requirements and to determine whether adequate arrangements are in place to justify proceeding with the implementation audit.

4.4.2 Undertake the role of an auditor to evaluate an organization's effective implementation of processes, procedures and methodologies for conformance with ISO/IEC 27001 including those areas described in 4.3 above.

4.4.3 Undertake the roles of an auditor to report the audit, including writing valid, factual and value-adding non-conformity reports, and undertake audit follow-up activities, including evaluating the effectiveness of corrective action.

## TRAINING METHODS

- 5.1 Your course may be presented as a wholly classroom-based course or as a blended course (in other words part self-study and part classroom-based). You may also present the course as a series of separate modules, either as full-time or part-time study.
- 5.2 **Classroom-based training**
- 5.2.1 You must provide for students **an environment conducive to effective learning**. At the beginning of the course you must provide the students with a description of the learning objectives, course structure, format and programme, student responsibilities and the assessment processes and assessment criteria, and you must deal with any concerns or worries that students may have.
- 5.2.2 Your course must be based on a clear **learning cycle** (see guidance in Appendix 1) and include opportunities for students to:
- Experience new ideas and skills. (Note that tutor-led slide presentations as a sole method to help students learn new knowledge is not acceptable).
  - Reflect on their learning and identify strengths and weaknesses. (Note that your course must include methods for monitoring and providing time for tutors and students to review tasks and activities and each student's achievement of the learning objectives).
  - Address and improve on areas of weakness. (Note that your course must include provision for review and remedial work, and individual coaching, where necessary.)
- 5.2.3 Your course must include a **variety of learning methods** to suit the range of learning styles (see guidance in Appendix 1).
- 5.2.4 Your course must not rely on tutor presentations and tutor-led discussions to teach **knowledge-based learning objectives**. We expect to see students learning these elements mostly through a process that requires students to complete a task or activities, often in teams, and to produce a defined output.
- 5.2.5 All students must practise the **skill-based learning objectives** of the course (learning objectives 3.1.3 and 3.1.4) through participation in appropriate tasks and activities (role play, simulation etc).
- 5.2.6 Timekeeping, planning and programme management are essential elements in the performance of an audit and, although we recognise that effective training is responsive to students' needs, deviations from the timetable must be managed so that all learning objectives are adequately covered and students are kept informed of significant changes to the programme.
- 5.2.7 You must submit **session plans** or tutor notes for each individual training session. Session plans must specify:
- learning objectives and duration for the session
  - nature of the activity and training method to be used
  - organizational arrangements, tutor and student briefing details
  - deliverables required from students for practical sessions
  - materials, exercises and equipment required to run the session
  - where training methods or use of exercises etc. are optional, this must be clearly indicated in session plans.

Note: The format of your session plans will depend on your approach to tutor competence and the size and complexity of your organization. Medium and high complexity training organizations (see IRCA/3000 appendix) will require more comprehensive tutor notes to ensure that training in new and amended materials is controlled and effective.

5.3 **Blended courses** (a combination of self-study, including electronic media, and classroom based learning)

- 5.3.1 Only knowledge-based learning objectives 3.1.1 and 3.1.2 may be covered by self-study methods.
- 5.3.2 Learning objectives 3.1.3 and 3.1.4 (auditing skills) must be completed in a classroom environment in terms of practice and student assessment. See clause 5.2 of this document for requirements for the classroom element of blended learning courses.
- 5.3.3 Training methods selected should seek to involve and engage students throughout the duration of the course. Simply providing students with a set of reading materials will not be acceptable. Your self-study materials must be designed around a clearly structured learning process with:
- Theory.
  - Examples (scenarios, case studies etc).
  - Practice (activities, case studies, progress tests etc).
  - Feedback/self-assessment on activities and tests where relevant, to ensure students can self-assess their understanding and achievement of the learning objectives and identify any areas requiring further work.
- 5.3.4 Self-study course materials must be clearly presented and structured for ease of use, with appropriate navigational aids. You must make the following clear to students to help them manage their learning:
- The learning objectives for the overall self-study element of the course.
  - The learning objectives for each section within the course.
  - How the self-study element of the course links with the classroom component
  - The structure and suggested or intended sequence of the materials.
  - Instructions for the students' use of the materials, including realistic timescales
  - Examples of typical documents, reports, forms etc.
  - How, when and how often students may contact tutors for help, guidance and feedback.
  - Methods for students to assess their learning and to seek timely feedback and coaching from the tutor(s).
- 5.3.5 You must ensure that each student has timely access to a course tutor to answer questions and queries.

Note: as a guide, a response to communications from students within 24 hours would be acceptable.

## **COURSE CONTENT**

- 6.1 At the beginning of your course you must provide the students with a description of the Learning Objectives, course structure, format and programme, student responsibilities and the assessment processes and assessment criteria against which they will be measured.
- 6.2 Your course must cover:
  - 6.2.1 All aspects defined in clause 3 Learning Objectives and amplified in clause 4 Enabling Objectives.
  - 6.2.2 Local requirements, culture, practices or approaches to auditing and the application of ISO/IEC 27001 as appropriate for each country in which the course is presented.
- 6.3 Your course must cover the benefits of certification as an IRCA ISMS Auditor, including brief details of the IRCA *ISMS Auditor* certification programme (IRCA/802), and provide students with details of how to contact IRCA and apply for certification. You must use IRCA/190 and IRCA/167 (or equivalents) for this.

## **COURSE DURATION**

### **7.1 Classroom-based learning**

- 7.1.1 Where the course is wholly classroom-based, the total course must be at least 24 hours, calculated as detailed in IRCA/2000.
- 7.1.2 The course may be presented over a minimum of 3 consecutive days full-time or on a part-time (modular) basis over a maximum of 8 weeks.

Note: although not mandatory, we recommend that this course be residential if presented over 3 consecutive days.

### **7.2 Blended learning**

- 7.2.1 Elements of the courses that are delivered through self-study will allow students three times longer than classroom training (i.e. approximately 40 hours for learning objectives 3.1.1 & 3.1.2).
- 7.2.2 The classroom element (i.e. the skills learning objectives 3.1.3 and 3.1.4 as a minimum) must be timed to allow each student to practise and be assessed on the skills learning objective. The amount of time given to this classroom element will depend on the learning objectives being covered, however normally 60% (or 2 days, or 14 hours gross as calculated in IRCA/2000) duration will be devoted to classroom-based learning and assessment. Courses with a reduction in classroom time may be allowed if agreed in advance with IRCA. See the Appendix for guidance for instances where reduced classroom time may be allowed.
- 7.2.3 Each student must complete the both the self-study and the classroom part of the training course in no more than 90 days.
- 7.2.4 Students must complete each element of blended courses in the correct sequence. For example, for courses designed with a self-study element to be followed by a classroom element, you must ensure that students who do not complete the self-study element of the course are not accepted onto the classroom-based element. You must have a process for recording and validating each student's completion of each element of blended courses to ensure students complete the course in the correct order.

### 7.3 Translators

- 7.3.1 If the course is given through translators, the time must be increased as necessary to satisfy the learning objectives.

## TUTORS & STUDENTS

### 8.1 Classroom-based learning

- 8.1.1 The number of students per course shall not exceed 20, or be less than 4.
- 8.1.2 Where the number of students is 11 to 20 inclusive, the course must be run with two designated tutors, both of whom shall be present for the full duration of the course. At least one tutor shall satisfy the requirements for a lead tutor as stated in IRCA/2000.
- 8.1.3 Where the number of students is 4 to 10 inclusive, the course may be run with one designated tutor, who shall be present for the full duration of the course. That tutor shall satisfy the requirements for a lead tutor.
- 8.1.4 Where additional tutors, including trainee tutors and specialists are used the two tutors remain responsible for the entire presentation.

### 8.2 Self-study based learning

- 8.2.1 Tutors who provide educational support on self-study elements of blended learning must be competent to operate any media required.

### 8.3 All courses. Tutors for this course must demonstrate competence in key attributes:

- 8.3.1 Competence in Training; by satisfying the Tutor or Lead Tutor requirements as appropriate (see IRCA/2000).
- 8.3.2 Competence in Auditing against ISO/IEC 27001; by demonstrating auditing competence as a currently certified ISMS Lead Auditor for Lead Tutors (or ISMS Auditor for Tutors) as described in IRCA/802 or meeting the requirements for such certification.
- 8.3.3 Competence to deliver training **and** student assessment on your specific course.
- 8.3.4 Knowledge of the specific local regulatory requirements in which the course is presented, or have a local expert attending at the necessary times.

## 9. Variations

- 9.1 We will consider requests for variations to any of these criteria, or in respect of any special circumstances. In this situation you should submit a **written** request to us immediately the requirement for the variation becomes apparent.
- 9.2 We will consider the following when evaluating any request for variation:
  - 9.2.1 Reasons for the requested variation.
  - 9.2.2 Proposed modifications to the training.
  - 9.2.3 The impact on the learning and assessment processes and how this will be managed.

## STUDENT ASSESSMENT & EXAMINATION

We regard the assessment and examination of students to be a very important part of this course.

**Successful Completion:** in order to satisfactorily complete the course each student must:

Complete all elements of the course.

Pass the Continuous Assessment (focused on the 4 Learning Objectives).

Pass the Written Examination (focused on the 4 Learning Objectives).

### Conduct and management of continuous assessment

Students must demonstrate acceptable levels of performance in the Learning Objectives. During the course you must test each student's achievement of the Learning Objectives. These tests must be based on practical tasks and activities with defined outputs that students must produce.

You must provide tutors with model outputs and a marking scheme/guidance to assess each student's performance and outputs (see appendix).

Tutors must provide students with feedback on their performance.

Tutors must provide further help and guidance to students who do not initially achieve elements of the Learning Objectives. They must provide these students with an opportunity to complete further tasks to demonstrate competence.

Each student's achievement of the learning objectives must be recorded on his/her continuous assessment record.

Note: See appendix for guidance on continuous assessment.

### 10.3 Conduct and Management of the ISMS Examination.

10.3.1 IRCA ISMS examinations must be conducted in accordance with the criteria set out in IRCA/2000.

10.3.2 Each training organisation is free to adopt a form of presentation that suits its needs. However ALL examination papers must state on every page:

"IRCA EXAMINATION PAPER NUMBER [X]" amended for use on approved course [xxxx] operated by [TO], [the date of issue and page number].

Please insert at **X** the IRCA reference number for the paper, at **TO** the name and IRCA certification number of your training organisation and at **xxxx** the IRCA certification number of your course.

10.3.3 You may modify these examinations papers as indicated below, but must not change the structure of the paper.

- a) Minor changes in the wording may be made to reflect local language differences.
- b) Changes in wording may be made to better reflect a specific context; e.g. a banking or a retail application. These changes must NOT represent substantive changes to either the question or the solution.

- c) A maximum of 25% of each paper may be replaced but this must NOT change the structure of the paper.
- d) On replacing a question, you must:
  - Provide a solution and marking scheme for the alternative question.
  - Send IRCA the alternative question (identifying clearly which question it is intended to replace) and its solution for approval before it is incorporated into the IRCA examination paper.

#### **COURSE PUBLICITY & ADVERTISING**

- 11.1 Your course advertising and promotional literature must not state or imply that this course satisfies more than part of the training requirements for certification as an IRCA ISMS auditor.
- 11.2 Promotional material shall clearly state that, prior to the commencement of your course, all students are expected to be experienced management system auditors with an understanding of the principles supporting information security management systems and of ISO/IEC 27001.

## **Appendix 1: Notes for Guidance**

### **Coverage of ISO/IEC 27001**

This document requires that students be able to explain the intent and requirements of each clause, and all clauses will be considered for inclusion in the examination. However, it is recognised that students are expected have knowledge of the ISO/IEC 27001 requirements before attending the course, either from previous training, experience or pre-course work. Tutors will not be expected to present a clause-by-clause analysis of ISO/IEC 27001 but they will need to satisfy themselves that this objective is met.

This document also requires students to interpret and apply ISO/IEC 27001 requirements. This requirement should be tested through practical exercises and it is recognised that students will only be able to gain this practical experience of limited parts of ISO/IEC 27001. Tutors should use their judgement in deciding which requirements to concentrate on in such practical activities.

### **Process Auditing**

The move to a process approach to auditing will have particular impact on the planning and conducting of audits. The following notes are for guidance and include considerations auditors may need to take into account when planning and conducting process audits.

#### **Planning the on-site audit:**

- Audit plan includes all activities applicable to the scope of audit and the audit standard (e.g., ISO/IEC 27001 or the contract).
- Audit trails are established from top level ISMS policy to all relevant functions and levels in the organization.
- Audit programme enables links between policy, objectives, targets, monitoring and continual improvement to be established.
- Audit programme reflects the structure, sequence and interrelationship of processes in the organization.
- Audit programme is sufficiently flexible and enables objective evidence to be gathered to verify activities and results.
- Audit programme reflects the organization's goals and priorities.

#### **Conducting the audit:**

- The purpose, inputs, outputs, controls and resources applicable to each process are clear.
- Links are established between processes and high level and local ISMS objectives.
- The outputs of the process are compared with desired outcomes, the purpose of the process and any specific quality objectives.
- The steps in the process and associated responsibilities are determined, where necessary.
- Inter-relating processes are identified.
- Process measures are identified.
- Evidence of continual improvement is sought.
- Needs of internal and external customers are clear.

### **Document Review**

Changes in the year 2005 issue version of ISO/IEC 17799 have implications for the process of document review. In many instances it will not be possible to assess whether ISO/IEC 27001 requirements are satisfied in principle from looking only at the information security policy document and procedures. Auditors will need to take a more holistic approach to assessing the adequacy of system documentation (not just procedures) and may perform part or all of this activity on-site. Your course should reflect this more holistic approach in both input sessions and exercises.

## Helping students learn new knowledge & skills - Accelerated Learning

We promote the use of accelerated learning approaches because they are more efficient, in terms of speed and depth of comprehension, and more effective, in terms of long-term retention of new knowledge. Therefore, you should employ practical tasks and activities to help students to understand new concepts and ideas. You should not rely on tutor-focused lecture/presentation to transfer new ideas and concepts.

### 1. The Learning cycle

There is a clear link between Deming's familiar Plan-Do-Check-Act and the learning cycle:

- a. **students experience something** (e.g. complete a task to find out about the requirements of ISO 9001)
- b. **students reflect on what they did & identify what they learned and what they still don't fully understand or can't do** (e.g. feedback to compare their answers to other students' answers and / or model answers, and identify any problems)
- c. **students take action to address weak areas** (e.g. ask tutor for help or complete task/activity again or complete another task)

Ensuring that your training sessions follow this simple model will make students' learning more effective. We referenced the learning cycle described by David A Kolb in developing these criteria and you might find it useful to consider this when developing your course.

### 2. Learning styles

We promote a variety of training methods in your course design. Different people learn in different ways so your sessions should follow the learning cycle and your course should include a variety of different learning activities to cater for all needs as far as possible. Honey and Mumford (*Learning Style Questionnaire*, Peter Honey Publications, ISBN 1 902899 07 5) provide one model for describing different learning styles that you may find useful as a basis.

### 3. Session plans

Developing session plans is a natural part of designing learning and training processes. Session plans should be simple and easy to use working documents to help your tutors manage effective learning. For organizations with only a few tutors, outline session plans are acceptable. For larger organizations with a number of branches or subcontractors, and the consequent number and turnover of tutors, we will require more comprehensive session plans. A sample session plan is provided below.

### 4. Continuous assessment

Continuous assessment should have a clear link between: session plans (for tutors), clear task/activity instructions with defined and measurable outputs (for students and tutors), activity marking schemes / model answers (for tutors), model answers (for students), individual student continuous assessment record (for recording student performance).

## Blended Learning – course duration & tutor:student ratios

We will consider courses designed with less than 60% of the course duration (as calculated in IRCA/2000) devoted to classroom activity in circumstances where, for example, there is a smaller tutor:student ratio: for example 2 tutors and a maximum of 6 students.

## **Self-Study**

We recommend that you consider the following documents when developing training based on information technology solutions:

BS 7988:2002 A Code of Practice for the use of information technology for the delivery of assessments

BS 8426:2003 A Code of Practice for e-support in e-learning systems

## Sample Session Plan

<b>SESSION PLAN</b>		
<b>Course Title:</b> The ISMS Auditor/Lead Auditor Course		
<b>Session Title:</b> Preparing an audit checklist	<b>Session Number:</b> 6	<b>Duration:</b> 1 hr 30 mins
<b>Purpose of the session:</b> To provide students with practical experience in preparing an audit checklist.		
<b>Learning Objectives:</b> Identify documents and sources of information required to produce a checklist. Produce an audit checklist to be used in audit practical later in the course.		
<b>Tutor Notes: Training Activities and Methods</b>	<b>Materials and Equipment</b>	
<p><b>Introduction</b> Explain that this session builds on the previous session in which the preparation of an audit checklist was discussed and demonstrated. Opportunity to try it out in practice. Explain that students will be formally assessed during this session</p>	<b>OHP session 6 intro</b>	
<p><b>Introduce exercise</b> Talk through the exercise brief, highlighting the following points: <b>Task:</b> to prepare a checklist that will enable the students to conduct an effective, process based audit of that area of the case study organization. <b>Process:</b> Pairs exercise. If the students require further help on how to approach the exercise, highlight suggested steps that they might follow in order to accomplish the task. <b>Output:</b> Audit checklist (either on the pro-forma sheets, or using any format preferred by the students) A list of the documents and sources of information used in the preparation of the checklist. <b>Note</b> The output from this exercise is part of the formal continual assessment, and will therefore be marked.</p>	<p><b>Handout student brief: "preparing an audit checklist"</b></p> <p><b>Flip chart process steps</b></p> <p><b>Audit checklist pro-forma sheets</b></p>	
<p><b>Run exercise</b> Tutors to monitor pairs regularly, and provide clarification, support and coaching as required. <b>Time for exercise:</b> 1 hour</p>		
<p><b>Feedback from exercise</b> Collect output from students Lead a brief discussion of the exercise, i.e., how they went about it, what was easy/difficult etc. Draw out any general points observed by tutors during the exercise.</p>		
<p><b>Marking exercise</b> Mark each submission in accordance with the marking scheme. Provide feedback to students on the results of the exercise and any further points for improvement at the earliest opportunity.</p>	<b>Audit checklist marking scheme (see below)</b>	

## Sample Audit Checklist Marking Scheme

### AUDIT CHECKLIST MARKING SCHEME: SESSION 6

Learning objective: Plan and conduct an audit

Enabling objectives:

Identify requirements for process auditing

Produce an audit checklist.

Criteria	Marks
Checklist covers all areas within the scope of the audit	2 marks
Relevant ISO/IEC 27001 requirements addressed	2 marks
Checklist identifies evidence to be viewed during audit	2 marks
Reference to policy/objectives and planned results included	2 marks
Logical structure for audit, picking up relevant audit trails	2 marks

Maximum 10 marks. Students must score a minimum of 6 marks to successfully complete the exercise. Students achieving less than this may be invited to re-submit.

**Sample Continuous Assessment Record (Completed)**

This example document has been designed to meet the minimum requirements of IRCA/2060 and IRCA/2000.

**PERSONAL CONTINUOUS ASSESSMENT RECORD**

Name:           **A Person**           Course dates:           **2- 4 April**          

Competence	Day 1	Day 2	Day 3	Overall Score
1. Interpreting the requirements of ISO/IEC 27001 in the context of an audit. Tutor Comments:	4	6	8	<b>8</b>
2. Planning and preparing an audit. Tutor Comments:		6		<b>6</b>
3. Gathering objective evidence, through effective interviewing observation, sampling & note taking. Tutor Comments:		4	6	<b>6</b>
4. Analysing & interpreting information in order to determine conformance with requirements. Tutor Comments:			6	<b>6</b>
5. Reporting the audit, including writing valid, factual and value adding non-conformity reports. Tutor Comments:			6	<b>6</b>

Performance in each area of competence is scored from 1-10 (1-2 = unacceptable, 3-4 = poor, 5-6 = acceptable, 7-8 = good and 9-10 = excellent). To pass the course students must pass each section (i.e. score at least 6 in each section) and achieve at least 70% in the examination. Students may not be assessed on every competence area every day (greyed areas show days when formal continuous assessment for particular learning objectives is not scheduled).

Tutor Signature:           **A Tutor**          

Date:           **4 April 2001**          

Tutor Signature:           **B Tutor**          

Date:           **4 April 2001**