



IRCA

INTERNATIONAL
REGISTER OF
CERTIFICATED
AUDITORS



Certification as an

Information Security Auditor



Contents

1. General Information about IRCA and the ISMS Programme
2. Certification Grades
3. Initial Certification
4. How to Apply
5. Fees
6. Renewal of Certification
7. How to Regrade
8. Other Information

Appendix I

Guidance on Continuing Professional Development

Appendix II

Definitions

Appendix III

Code of Conduct

The information detailed within this document was correct at time of publication. For more details about this programme and other services we provide, we advise you to see the IRCA website at www.irca.org.

Copyright IRCA - 2007

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 International Register of Certificated Auditors (IRCA)

1.

General Information about IRCA and the ISMS Programme

IRCA and Auditor Certification

History:

The International Register of Certificated Auditors (IRCA) began certifying auditors in 1984. It was set up as part of an initiative by the UK government to make business and industry more competitive. The aim of this initiative was to achieve efficiencies by reducing the costs of supplier audits by replacing them with a fewer number of third party audits. Each third party audit of a supplier would then be accepted and recognized by all customers of that supplier.

In addition to IRCA, the other bodies involved in this new structure included an accreditation body (now UKAS), a national standards making body (BSI Standards) and a number of certification bodies. The quality management standard used was the British standard BS 5750, which later became ISO 9001.

This quality infrastructure proved to be extremely successful and is now recognized worldwide to be the most effective and most commonly used method for assuring the quality of supplier organizations. This same structure is now used in other contexts, e.g. to assure the compliance of organizations' management systems to occupational health & safety, food safety and environmental requirements. But whatever the context, because the structure relies heavily on competent auditors and consultants, the role played by IRCA has been essential to its success.

During the years since its establishment, IRCA has earned a reputation for integrity and for adding value. The evaluation and certification methods developed and used by IRCA have been adopted by most other auditor certification bodies. Although most countries now offer alternatives to IRCA through their own national auditor certification programmes, IRCA certification remains internationally as popular as ever. Around 30,000 auditors have been awarded certification since 1984, and over 120 countries are currently represented on the IRCA register. IRCA is the only auditor certification body that has international recognition and remains the certification that supplier organizations, certification bodies and auditors value most.

IRCA Training:

IRCA certification of auditor training courses is recognized and valued internationally. Although developed originally to support auditor certification, IRCA has evolved certification of training to become an independent activity, successful in its own right. Originally designed for auditors wishing to become certified, the courses proved very popular with students who were seeking information on quality, environmental and health & safety management for a variety of reasons. Now only a small minority of students attending these courses are auditors. Training organizations in many parts of the world regard IRCA certification as an essential requirement for trading. The number of courses IRCA offers has increased to cover a wide range of applications and continues to expand as training organizations demand certification for an increasing range of course types. Around 60,000 students a year attend IRCA certified training in all parts of the world.

Links with the CQI:

IRCA is the Chartered Quality Institute's (CQI) personnel certification body. The CQI in its own right is recognized worldwide as one of the international champions of quality. Together, in their respective roles, IRCA and the CQI provide a successful contribution to business and industry based on integrity, absolute impartiality and adding value to the business process.



The ISMS Programme

To have credibility, the conformity assessment bodies need competent auditors. To be efficient and competitive, business and industry needs competent auditors. The purpose of our Information Security Management Systems Auditor Certification Programme (the ISMS Programme) is to provide confidence to the conformity assessment bodies and to business and industry that auditors certified to this programme are competent.

As part of the certification process we will evaluate you against requirements which reflect the key skills, knowledge and experience that define competence and which you, the ISMS auditor, need to have and demonstrate during an audit.

The ISMS Auditor Certification Programme is based on the key standards:

- ISO/IEC 27001:2005, *Information Technology – Security Techniques – Information Security Management Systems – Requirements*
- ISO/IEC 17799:2005, *Information Technology Security Techniques – Code of Practice for Information Security Management*

and the auditing guidance standard:

- ISO 19011:2002, *Guidelines on Quality and/or Environmental Management Systems Auditing*

and the accreditation guidance given in:

- EA 7/03, *Guidelines for the Accreditation of Bodies Operating Certification/Registration of Information Security Management Systems.*

ISO/IEC 27001:2005 provides correspondence and alignment with ISO 9001:2000, *Quality Management Systems – Requirements* and ISO 14001:2004, *Environmental Management Systems – Requirements with Guidance for Use.*

Our award of certification means we have recognized that you understand and are competent (depending on the grade awarded) to:

- uphold the principles of proper ethical conduct, fair presentation and due professional care
- communicate clearly orally and in writing with personnel at all levels of an organization
- plan and organize an audit of an ISMS
- identify and understand relevant business processes
- evaluate objective evidence and determine the effectiveness of an ISMS
- report accurately audit findings and conclusions

- lead the audit team and manage the audit process
- audit a management process.

The scope of certification is general, i.e. it does not include nor does it require any industry sector specific competences. You may select from a list up to 6 standard industry sectors within which you have acquired work experience. These details, although included within the register, are self-declarations and are outside the scope of certification.

The details of all certified auditors are included within a register which is publicly available.

The Programme is intended for:

- ISMS auditors, e.g. those employed/contracted by third party certification/registration bodies and those involved in first or second party ISMS audits
- information security practitioners, e.g. information security consultants, IT security managers and IT personnel
- employees conducting ISMS audits within their own organization, i.e. internal ISMS audits.

This document provides you (new applicants and existing IRCA certified auditors) with information and instructions on:

- the certification process and how to apply
- the requirements for initial certification
- the requirements for renewal of certification, including CPD requirements
- the types of audits acceptable for certification
- fees
- the Code of Conduct.

Certification within the ISMS Programme is available, without restriction, to all individuals worldwide who satisfy the certification requirements.

We gratefully acknowledge the contributions made by Ted Humphreys of XiSEC to the development of these criteria and the updates provided by Brian Henry IRCA ISMS Reviewing Officer.

2.

Certification Grades

The ISMS Programme has six grades of certification:

- ➔ ISMS Provisional Internal Auditor
- ➔ ISMS Internal Auditor
- ➔ ISMS Provisional Auditor
- ➔ ISMS Auditor
- ➔ ISMS Lead Auditor
- ➔ ISMS Principal Auditor

To assist you in determining which grade is right for you, we have listed below descriptions of the characteristics of each grade and a brief summary of the certification requirements. You will find a more comprehensive description of these in the next section 'Initial Certification'.

ISMS Provisional Internal Auditor

Who is suited to this grade?

You should consider this if you intend to perform internal ISMS audits. The grade recognizes you to have the appropriate personal attributes, educational, professional and technical competences but have not yet had sufficient opportunity to meet the auditing experience requirements necessary for certification to the internal auditor grades. Most internal auditors start at this grade and it is seen as the first step.

Summary of certification requirements for this grade:

Education

- At least secondary education

Work Experience

- Five years, or 4 years with a degree or near degree
- One year of information security work experience

Auditor Training

- An IRCA certified ISMS Foundation course or accepted alternative
- An IRCA certified ISMS Internal Auditor course or accepted alternative

Auditing Experience

- None.

ISMS Internal Auditor

Who is suited to this grade?

You should consider this if you perform internal ISMS audits for your organization. The grade recognizes you to have the appropriate personal attributes, educational, professional, technical and auditing competences to meet the auditing experience requirements necessary for certification to the internal auditor grade.

Summary of certification requirements for this grade:

Education

- At least secondary education

Work Experience

- Five years, or 4 years with a degree or near degree
- One year of information security work experience

Auditor Training

- An IRCA certified ISMS Foundation course or accepted alternative
- An IRCA certified ISMS Internal Auditor course or accepted alternative

Auditing Experience

- Five audits totalling at least 15 hours.

ISMS Provisional Auditor

Who is suited to this grade?

This is the entry or training grade, and you should consider this if you intend to make auditing your career. The grade recognizes you to have the appropriate personal attributes, educational, professional and technical competences but have not yet had sufficient opportunity to meet the auditing experience requirements necessary for certification to the other grades. Most career auditors start at this grade and it is seen as the first step.

This grade is also used by experienced auditors who are taking a temporary break from auditing or have moved from auditing to management and who still see value in maintaining IRCA certification.

Summary of certification requirements for this grade:

Education

- At least secondary education

Work Experience

- Five years, or 4 years with a degree or near degree
- Two years of information security work experience

Auditor Training

- An IRCA certified ISMS Auditor/Lead Auditor course or accepted alternative

Auditing Experience

- None.

ISMS Auditor

Who is suited to this grade?

This grade is a natural progression from the provisional grade and you should apply for regrade (from provisional) as soon as you have completed the required auditing experience. This grade recognizes you as a competent auditor, contributing as an effective member of an audit team. It is regarded as the next step in the career ladder and most auditors who hold this grade intend to move onto either the lead or the principal grades.

Summary of certification requirements for this grade:

Education

- At least secondary education

Work Experience

- Five years, or 4 years with a degree or near degree
- Two years of information security work experience

Auditor Training

- An IRCA certified ISMS Auditor/Lead Auditor course or accepted alternative

Auditing Experience

- Four audits as an auditor-in-training totalling 20 days, 10 days minimum on-site.

ISMS Lead Auditor

Who is suited to this grade?

Most ISMS auditors working for certification bodies are Lead Auditors, as are those auditors who perform supplier (second party) audits for large purchasing organizations. This grade is reserved for competent auditors experienced at managing audits and leading teams.

Summary of certification requirements for this grade:

Education

- At least secondary education

Work Experience

- Five years, or 4 years with a degree or near degree
- Two years of information security work experience

Auditor Training

- An IRCA certified ISMS Auditor/Lead Auditor course or accepted alternative

Auditing Experience (in total, i.e. assuming you do not currently hold the ISMS Auditor grade)

- Four audits as an auditor-in-training totalling 20 days, 10 days minimum on-site
- Three audits as lead auditor-in-training totalling 15 days, 10 days minimum on-site.

ISMS Principal Auditor

Who is suited to this grade?

This grade is designed as an alternative to the Lead Auditor grade and is intended to recognize the considerable experience and competence of two categories of auditors who operate on their own (i.e. as a team of one, performing sole audits);

- Auditors with a background in information security consulting (whose key competences are implementing information security systems and who possess experience in performing all aspects of the audit process effectively and without assistance)
- Auditors with a background in leading audit teams (as lead auditors) but who now audit on their own (whose key competences are audit management and team leadership).

We consider the Principal Auditor and Lead Auditor grades as being, on balance, of an equivalent standard and we do not intend that auditors hold the Principal Auditor and Lead Auditor grade, or any other grade, at the same time.

Summary of certification requirements for this grade:

Education

Consultant route:

- A degree or near degree

or

Team leader route:

- At least secondary education

Work Experience

Consultant route:

- Six years of information security work experience

or

Team leader route:

- Five years, or 4 years with a degree or near degree
- Two years of information security work experience

Auditor Training

- An IRCA certified ISMS Auditor/Lead Auditor course or accepted alternative

Auditing Experience

Consultant route:

- Seven sole or lead audits totalling 35 days of which a minimum of 20 days must have been on-site (these numbers assume you do not currently hold the ISMS Auditor or ISMS Lead Auditor grade)

or

Team leader route:

- Six years certified to the Lead Auditor grade
- Three sole audits where you were required to demonstrate effective audit management skills within complex and demanding situations.

3.

Initial Certification

We will evaluate your application based on your demonstration of the competences¹ needed for effective audit of ISMS management systems. You can demonstrate these competences through a combination of education, work experience, auditor training and audit experience.

Unless otherwise indicated, we will accept a less comprehensive coverage of the scope and depth of competences for the ISMS Internal Auditor grade.

Competences

Generic Auditing Competences

- Audit principles, procedures and techniques that enable you to apply these as appropriate to different audits and ensure that you conduct audits in a consistent and systematic manner
- Management system and reference documents that enable you to comprehend the scope of the audit and apply audit criteria
- Organizational situations that enable you to comprehend the organization's operational context
- Applicable laws, regulations and other requirements relevant to the discipline that enable you to work within, and be aware of, the requirements that apply to the organization being audited.

ISMS Auditing Competences

- Information security related methods and techniques that enable you to examine those processes (specified in ISO/IEC 27001:2005, clauses 4 – 8) that have been used to establish, implement and operate, monitor and review as well as improve an ISMS in order to assess its effectiveness and to generate appropriate audit findings and conclusions
- Processes and products, including services, that enable you to comprehend the technological context in which the audit is being conducted.

Education

For all grades except ISMS Principal Auditor (consultant route):

You need to have completed a minimum of secondary education. If you have a degree or near degree² level qualification, we will reduce the requirement for work experience.

Acceptable qualifications include those awarded by an institution, recognized by a national governmental body or accredited by a national professional body.

For ISMS Principal Auditor grade (consultant route):

You need a degree, near degree, or acceptable equivalent.

All post graduate diplomas, undergraduate and post graduate degrees awarded in a relevant subject will normally be accepted.

Work Experience

General, relevant work experience:

For all grades except for ISMS Principal Auditor (consultant route):

You need to have at least 5 years of relevant work experience, this is reduced to 4 years if you have a degree or near degree. We consider relevant work experience to be a technical, managerial or professional position where you are required to exercise judgement, solve problems and communicate with other managers, employees and customers.

For ISMS Principal Auditor (consultant route):

You must have at least 6 years of work experience, all of which must be ISMS work experience.

ISMS work experience:

For all grades except the ISMS Principal Auditor (consultant route) and Internal Auditor grades:

You must also have completed 2 years (which may be included as part of the 4 or 5 years total work experience) within a context where information

¹ You will find a more complete listing of the competences in ISO 19011:2002, section 7.3.

² We use the UK definition of a degree as the degree benchmark. We recognize that not all degrees awarded in the UK and in other countries meet this standard. Many fall just short, either in content or in duration and we call these 'near degrees'. For the purposes of this programme we recognize a near degree as meeting the tertiary education requirement.

security issues formed the major part of the job. Such experience must have provided you with the practical knowledge necessary to audit information security management systems effectively.

For the Provisional Internal Auditor and Internal Auditor grades:

You must have completed 1 year (which may be included as part of the 4 or 5 years total work experience) within a context where information security issues formed the major part of the job. Such experience must have provided you with the practical knowledge necessary to audit information security management systems effectively.

For ISMS Principal Auditor (consultant route):

You must be able to demonstrate at least 6 years of work experience acquired within the previous 10 year period that related to the development, implementation, maintenance and auditing of information security management systems. The significant majority of this work experience must have been conducted at a senior level within an organization. You may have acquired this experience either as an employee or as a contractor. Because we are looking for evidence of information security related competences acquired through working within relevant fields, we will only accept auditing experience as contributing up to a maximum of half of this requirement. You must have acquired the 6 years of ISMS experience within the previous 10 years.

For all grades, periods of training cannot be included in this work experience requirement.

Auditor Training

For all grades except the Provisional Internal Auditor and Internal Auditor grades:

You must have successfully completed an IRCA certified ISMS Auditor/Lead Auditor course (or an acceptable alternative).

For the Provisional Internal Auditor and Internal Auditor grades:

You must have successfully completed either an IRCA certified ISMS Auditor/Lead Auditor course (or an acceptable alternative) or an IRCA certified ISMS Foundation course (or an acceptable alternative) and an IRCA certified ISMS Internal Auditor course (or an acceptable alternative).

Exceptionally, we will consider accepting training completed through other ways as meeting part or all of the training requirement, e.g. the ISACA Certified Information Security Auditor (CISA)

qualification, but the onus will be on you to satisfy us that this training at least meets the learning outcomes of the relevant IRCA certified course.

You should normally have successfully completed auditor training within the 3 year period immediately prior to application for certification. We may accept training completed prior to this period if you provide evidence of recent, relevant work experience and currency of your auditing skills.

We advise you to refer to the IRCA website www.irca.org for a current listing of all IRCA approved training organizations offering IRCA certified ISMS auditor training courses.

Auditing Experience

For ISMS Provisional Internal Auditor grade:

No auditing experience is required for certification to this grade.

For ISMS Internal Auditor grade:

You need to have performed at least 5 internal audits, each of which must have been of at least 3 hours duration and must have included all elements of the audit cycle; audit planning, document review, auditing, interviewing, audit reporting and must not have involved areas or activities that you yourself perform. (However, we will accept audits of activities for which you are directly or indirectly responsible, e.g. as a line manager).

For ISMS Provisional Auditor grade:

No auditing experience is required for certification to this grade.

For ISMS Auditor grade:

You need to have performed at least 4 complete audits. Auditing activity must include document review, preparation and performance of on-site audit activities and audit reporting.

The duration of these audits must not be less than 20 days, 10 days of which must have been acquired on-site.

Although we recommend you should complete all of the audits under the direction and guidance³ of an auditor competent as a team leader (currently certified as a lead auditor or who has equivalent competence), we acknowledge that for many auditors this will be very difficult and costly to arrange. Consequently, we will accept a minimum of 1 audit under these conditions. We may require this team leader to attest to your competence to audit as a team member.

³ Direction and guidance does not mean you must be under constant supervision, nor does it mean someone needs to be assigned solely to perform this task.

For ISMS Lead Auditor grade:

In addition to the audit requirement for the ISMS Auditor grade listed above, you must have completed 3 acceptable audits as the leader of an audit team which included at least one other auditor.

The duration of the 3 lead audits must not be less than 15 days, 10 days of which must have been acquired on-site.

Although we recommend you should complete all of the audits under the direction and guidance⁴ of an auditor competent as a team leader (currently certified as a lead auditor or who has equivalent competence), we acknowledge that for many auditors this will be very difficult and costly to arrange. Consequently, we will accept a minimum of 1 lead audit under these conditions. We may require this team leader to attest to your competence to lead an audit team.

If you are already certified to the ISMS Auditor grade, you need only perform the 3 lead audits as stated above.

For ISMS Principal Auditor grade:

For the consultant route, you must have completed a minimum of 7 acceptable sole or lead audits totalling 35 days, 20 days of which must have been acquired on-site.

If you are already certified to the ISMS Auditor grade, you need only perform 3 sole or lead audits of a duration of not less than 15 days, 10 days of which must have been acquired on-site.

For the team leader route, you must have acquired a minimum of 6 years of experience as a certified lead auditor (exceptionally, we will consider accepting less than 6 years as a certified lead auditor if you are able to demonstrate a very considerable and comprehensive experience in leading teams within a shorter period) and conducted 3 sole audits, where you were required to demonstrate effective audit management skills in complex and demanding situations. As guidance, we anticipate these to be initial audits of more than 1 day's duration performed within a complex organization.

⁴ Direction and guidance does not mean you must be under constant supervision, nor does it mean someone needs to be assigned solely to perform this task.

General Guidance on Acceptance of Audits:

*What audits do we accept?***For all grades except ISMS Lead Auditor:**

We will only accept audits performed during the previous 3 year period.

For ISMS Lead Auditor grade:

You must have acquired the lead audit experience during the previous 2 years. We define 'previous period' as being that period immediately prior to the date we receive your completed application.

We must be able to verify all audit experience you submit in your log sheets. Please make sure you include detailed information of the audits you perform and provide sufficient contact details so that we are able to perform the verification.

We will only accept audits that have been performed in accordance with the auditing guidance standard ISO 19011:2002 and against ISO/IEC 27001:2005 or an alternative standard we accept as being equivalent. Please note that we will not accept audits against BS 7799-2:2002 that were conducted after 31 March 2006. Audits performed against alternative national, international, industry or company standards may also be acceptable.

We will accept supplier audits (also known as *second party* audits), certification audits (also known as *third party* audits) and internal audits (also known as *first party* audits, see below). We also accept consultancy audits (see below), which can be performed as first, second or third party audits.

Internal (first party) audits:

For ISMS Internal Auditor grade we will accept internal audits performed by you on parts of your own organization where you are independent from the operational activities you are auditing.

We will accept internal audits providing that in addition to you being independent from the operational activities you are auditing, the scope of the audit was sufficiently broad and the audit was sufficiently complex to require you to use a range of auditing skills. So that we can consider your internal audits for acceptance, we advise you to provide us with appropriate and relevant supporting information.

Consultancy Audits:

We will accept audits performed by you when acting as a consultant for a client if all of the following are satisfied:

- the client (auditee) already had a fully established ISMS prior to the audit
- you had no part in setting up the ISMS being audited (except in specific circumstances as described below)
- you were independent of the auditee
- the scope of the audit included all elements of the ISMS.

We will also accept pre-assessment audits performed by you on an ISMS that you were involved in developing if the certification body subsequently awarded certification at the first attempt.

Surveillance (partial system) audits:

We do not normally accept surveillance (partial system) audits when submitted for initial certification (except for ISMS Internal Auditor). However, we do accept surveillance audits for renewal of certification. As a general rule we consider five surveillance audits to be equivalent to one full ISMS audit, but recognize that some surveillance audits can be very extensive. In such instances, we will accept fewer than five surveillance audits (as being equal to one full ISMS audit) if you provide us with evidence that supports your claim.

Audits we do not accept:

We do not accept:

- audits of the same ISMS that are repeated more frequently than once every 12 months
- audits of less than 1 day (6 hours of on-site audit activity exclusive of breaks) duration, except for Internal Auditor grade where we will accept audits of 3 hours exclusive of breaks
- gap analysis, close out or follow up visits
- audits performed before successful completion of the formal training requirement.

4.

How to Apply

What you do

Request an application pack

We will provide you with an application pack free of charge. Either contact us and we will send it to you by post, or download all the documents yourself from our website.

Tel: +44 (0)20 7245 6833

Fax: +44 (0)20 7245 6755

Email: irca@irca.org

Website: www.irca.org

Complete and submit the application form and documents

When you apply for certification, please complete the forms as instructed, enclose all the additional material requested and send to us with the application fee.

At the application stage, please send only the application fee. Do not send the annual certification fee. If your application is successful, we will write and ask you to pay the annual certification fee.

We accept applications and supporting documentation in the following languages:

- English
- Chinese
- Japanese
- Italian
- Spanish

For all the other languages we will need all correspondence in support of the application to be in the English language or to be accompanied by certified translations of the originals. This is particularly important for educational qualifications, training courses and audits.

All qualifications submitted must be supported by documentary evidence. An example of acceptable evidence would be a good quality photocopy of the original certificate indicating the awarding body, the title and date of the award and the name of the person to whom the award was made. If any of this information is not available or is not clear, we may ask you to supply us with more evidence.

The same applies if a copy of the certificate is not available, for example where it has been lost or destroyed. Acceptable evidence would include an official letter from the awarding body confirming the award.

A transcript (i.e. an official, detailed account of the course content) of an award would also be acceptable evidence if it clearly states the date and title of the award.

If no documentary evidence can be supplied by the awarding body, it is unlikely we would accept your qualification.

What we do

We usually take about four weeks to process each application. But that time may vary depending on the time required to verify the information submitted with the application. Giving us all the information we need will speed up the application process.

The process has four parts:

Administrative check

All applications are checked first by our administration staff to make sure you have included all the information we need.

Technical evaluation

This phase is performed by IRCA's technical experts, the Reviewing Officers. The Reviewing Officers evaluate the information submitted against the certification requirements and perform verification of some or all of this information. At the conclusion of the technical evaluation, the Reviewing Officers will make a recommendation on certification to the Certification Manager.

We consider verification to be an essential element supporting the overall credibility of the certification process. Consequently, great care is taken by the Reviewing Officers in reviewing and verifying applications against all aspects of the certification requirements. We will perform the evaluation as speedily as we can, but sometimes it is not possible to be as quick as we (or you) would like. Processing your application is likely to take longer if you have unusual educational qualifications, if your current (or former) employers are slow to provide verification information or if the auditee organizations are not helpful.

Certification

The final decision on your certification is made by the Certification Manager. The certification decision is performed independently from the technical evaluation process (detailed above).

Offer and award of certification

The Certification Manager will write formally to you with an offer of certification to the appropriate grade. We will send you this offer and ask you to pay your first annual fee.

Certification will be awarded when we receive your payment of the annual fee.

Your details are then added to our online register of certificated auditors and we will send you your certification card.

5.

Fees

Fees are set annually and apply for the calendar year (1 January - 31 December). Contact us direct or see www.irca.org for details of current fees applicable for your country.

Application Fee

We need you to pay this fee when you send in your application. Alternatively, we will invoice you on receipt of your application. This fee covers the costs of the application process and is not refunded if the application is unsuccessful.

Annual Certification Fee

This fee covers the annual cost of administering your certification. We will normally invoice you for this fee when we first offer you certification following your application, and thereafter each year one month⁵ before payment is due.

Application for Regrade Fee

This fee covers the costs of evaluating your regrade. We need you to pay this fee when you submit your request and, as with the application fee, the regrade fee is not refundable. If you are regraded during the year, we will not ask you to pay any further certification fees for that current year. You may request a regrade at any stage during the certification period. There is no regrade fee if we regrade you as part of the (3 year) renewal of certification process.

⁵ Except every third year when your renewal is due. We invoice you after we have completed your renewal, on the basis that your grade (and fee) may have changed as a result of renewal.

6.

Renewal of Certification

You must renew your certification every three years, i.e. at the end of the third complete year. We will write to you two months before your certification period expires and ask you to send us your audit and CPD logs and other documents. We will evaluate these against the renewal requirements listed below and make a certification decision. We will then write to you with the results.

The renewal of certification process involves these five requirements:

- Continuing Professional Development (CPD)
- Audit experience
- Declaration of Complaints
- Compliance with the IRCA Code of Conduct
- Payment of the Annual Fee.

Continuing Professional Development

For all grades except the Provisional Internal Auditor and Internal Auditor grades:

You must have completed at least 45 hours of appropriate CPD during the 3 year period immediately prior to renewal of certification.

We need you to provide us with evidence that you have met this requirement. (See Appendix I for guidance.)

For ISMS Provisional Internal and Internal Auditor grades:

There is no CPD requirement.

Audit Experience

We need you to record and submit your audit experience on the audit log sheets (IRCA/106) which we supply.

For ISMS Provisional Internal Auditor grade:

There is no requirement to perform audits.

For ISMS Internal Auditor grade:

You need to have completed a minimum of 5 audits, the total duration of which must be at least 15 hours.

For ISMS Provisional Auditor grade:

There is no requirement to perform audits.

For ISMS Auditor grade:

You need to have completed at least 5 acceptable audits.

For ISMS Lead Auditor grade:

You need to have completed at least 5 acceptable audits, any 2 of which must have been as the leader of a team which included at least one other auditor.

For ISMS Principal Auditor grade

You need to have completed at least 5 acceptable audits, all 5 must have been either lead audits or sole audits.

You must have performed all audits within the previous three year certification period.

Declaration of Complaints

We need you to tell us about any complaints made against your professional conduct. It is important that we know of any complaints as we need to consider these as part of the renewal of certification process. We will investigate all instances of complaints. If complaints are made against your conduct and you do not declare them, the consequences will be far more serious and may result in suspension or withdrawal of your certification.

Compliance with the Code of Conduct

We need you to make a declaration that you have always acted in compliance with the Code of Conduct (see Appendix III).

Payment of the Annual Fee

And finally, we need you to pay the annual fee (please note there is no additional fee for renewal). Because the fee will be dependent on the grade we offer you after renewal, we do not ask you to pay this fee until after we have completed the renewal. We will write to you with the results of the renewal and enclose the fee invoice and your new certification card.

7.

How to Regrade

You can apply to be regraded to another grade at any time. When we offer you initial certification we will indicate the audit experience and competences you need to attain the next grade(s) of certification. To apply for regrade, you should complete IRCA/106 log sheets, enclose any additional information requested and send to us with the regrade fee.

A successful application for regrade will not normally result in a change to your renewal of certification date.

If you decide not to apply for regrade during your certification period, we will write to you two months before your certification period expires as part of the renewal of certification process and ask you to send us your audit and CPD logs. At this point we will let you know the current regrade requirement. There is no regrade fee if you are regraded as part of the (3 year) renewal of certification process.

Please contact us if you need further advice on how to regrade.

8.

Other Information

The Certification Period

When your application is successful, we award certification for a period of 3 years, beginning in the month we award certification. This 3 year period is referred to as the certification period. At the end of each certification period we require you to renew your certification. If you are successful at renewal, we award you certification for a further 3 year certification period, and so on.

During the certification period, at the end of the first and second years, you may maintain certification by payment of the annual certification fee and by compliance with the Code of Conduct. We don't require you to submit any other documentation at the end of year 1 and year 2. At the end of the third year, all certified auditors are required to complete the renewal of certification process.

ISMS Standards other than ISO/IEC 27001:2005

We will accept audits performed against standards which we evaluate as being equivalent to ISO/IEC 27001:2005. We maintain a list of acceptable alternative standards but it is possible that you may claim audits against a standard that is not on this list. We have a procedure for evaluating new standards and you are advised to contact us for advice where you consider an alternative standard may be acceptable to us.

Certification Cards, Certificates and the Register

We will send you a Certification Card following initial award of certification and annually thereafter when you pay your annual fee and comply with any other applicable requirements.

This card is your primary evidence of certification and you should present this when you first begin an audit and thereafter whenever appropriate.

Although the card is issued to you, it remains our property and you must return it to us should we ask you to.

The IRCA Certificate is intended for display as a formal recognition of your certification to a specific grade. You should not use it as proof of certification. Please contact us if you wish to purchase a certificate.

You can find details of all certified auditors in each country on the 'Find an Auditor' section of the IRCA website www.irca.org.

Appeals and Complaints

You have the right to appeal against any certification decision taken by us. We operate a quality system that includes established procedures for considering appeals and complaints.

Enforcement of Certification

We enforce certification for two reasons:

1. If you fail to meet the certification criteria for the grade to which you are certified. This enforcement occurs when you apply to renew your certification. In most cases withdrawal will be preceded by an offer of an alternative grade for a period during which you have the opportunity to meet the requirements and be reinstated to the grade you originally held.
2. If you breach the Code of Conduct, we reserve the right to undertake action against your certification if we find you to have acted contrary to the Code of Conduct. Options available include suspending, or in instances of serious or sustained breach, withdrawing your certification.

Confidentiality

We undertake to consider as strictly confidential all information, correspondence and documentation submitted by you to us in support of your certification activities⁶.

We reserve the right to publish relevant details of each certified auditor in the register available online at www.irca.org.

Legal Status

The certification of auditors by us and all activities associated with the administration of the register is governed in accordance with English Law and is subject to the exclusive jurisdiction of the English Courts.

⁶ We reserve the right to disclose details of your certification record to other auditor certification bodies and accreditation bodies. We will do so with discretion and only in instances where we consider withholding this information will compromise the integrity of certification, e.g. where we have taken action against (i.e. suspended or withdrawn) your certification and you have applied to another auditor certification body without fully disclosing your record while certified by us.

Appendix I

Guidance on Continuing Professional Development

CPD is a framework that encourages you to continuously update your professional knowledge, personal skills and competences. The purpose of CPD is to make you more effective as an auditor and to make the auditing profession more credible. The concept of CPD and the value it contributes is now recognized and accepted throughout all professional fields.

As part of the renewal of certification process, you must demonstrate to us you have completed at least 45 hours CPD within the last 3 years in subjects that are broadly related to auditing and ISMS. Because there are so many topics that we recognize will enhance your auditing competence, we do not attempt to list them here. But we categorize these into 2 areas which are consistent with the 2 main areas of competence required by ISMS auditors:

1. Information Security related
2. Auditing related

We recognize that no single method for learning suits everyone. Therefore, we will accept CPD acquired in ways that range from the very informal (e.g. reading and self study) to the formal (e.g. classroom training). We recognize that some ways of acquiring CPD are more effective than others, so we apply a 'weighting' where some activities are accorded more recognition than others. The activities are divided into 3 broad categories:

a) Unstructured; where 3 hours are accepted as one CPD hour

Included in this category would be distance and open learning study which is not assessed and does not lead to a qualification, the reading of professional and technical journals, books and other publications relevant aspects of on-the-job training, where specific outcomes have been planned and identified.

Reading IRCA INform, our e-magazine available from www.irca.org, or contributing to the IRCA online discussion forum⁷, also available from our website, is also accepted.

b) Semi-structured; where 2 hours are accepted as one CPD hour

Included in this category would be non-interactive lectures, talks, etc., informal professional body meetings of a more social nature (networking opportunities), the research, preparation and first delivery of lectures/courses, publishing articles and forms of open and distance learning that involve assessment and that result in the acquisition of a qualification.

⁷ A maximum of 4 hours of unstructured CPD will be accepted for contribution to the IRCA forum. Evidence must be documented and verified on IRCA/173 CPD logs.

c) Structured; where each hour is accepted as one CPD hour

Examples of this category would be interactive and highly participative training courses and seminars, professional body meetings with formal lectures, active participation in development of standards.

The range of activities that may be included within each category is extensive and the small number of examples above are intended to provide broad guidance only. Most auditors submit evidence of activities that include all 3 categories, but it is not a requirement that you do so. The only restriction we place is that unstructured CPD cannot constitute more than 1/3 (i.e. 15 hours) of the total acceptable CPD hours.

It remains your responsibility to provide a case for acceptance of any activity you submit, and this must be supported by sufficient, appropriate evidence. This will involve you making and retaining records of your activities and having these properly verified where possible. We have developed a CPD and training log sheet (IRCA/173) for this purpose.

It is in your interests to provide us with information in a clear, logical and easily understandable format. The speed with which we are able to evaluate and renew your certification will depend on this.

Appendix II

Definitions

Audit

A systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled.

Auditee

The organization being audited.

Audit Client

The person or organization requesting an audit.

Audit Team

Two or more auditors performing an audit, one of whom is appointed as leader.

Lead Audit

An audit where the auditor performed the audit whilst leading a team of at least one other auditor.

Sole Audit

An audit where one auditor performed all phases of the audit.

First Party Audit

An audit performed within an organization by that organization's own auditing resource. Also referred to as an internal audit.

Second Party Audit

An audit of contractors/suppliers undertaken by, or on behalf of, a purchasing organization. This may include the audit of companies or divisions supplying goods or services to others within the same group. Also referred to as a supplier audit.

Third Party Audit

An audit of an organization performed by a body that is independent of the organization being audited, e.g. certification body or registrar.

Appendix III

Code of Conduct

It is a condition of certification that you agree to act in accordance with, and be bound by the following Code of Conduct:

1. To act in a strictly trustworthy and unbiased manner in relation to both the organization to which you are employed, contracted or otherwise formally engaged (the audit organization) and any other organization involved in an audit performed by you or by personnel under your direct control.
2. To disclose to your employer any relationships you may have with the organization to be audited before undertaking any audit function in respect of that organization.
3. Not to accept any inducement, gift, commission, discount or any other profit from the organizations audited, from their representatives, or from any other interested person nor knowingly allow personnel for whom you are responsible to do so.
4. Not to disclose the findings, or any part of them, of the audit team for which you are responsible or of which you are part, or any other information gained in the course of the audit to any third party, unless authorized in writing by both the auditee and the audit organization to do so.
5. Not to act in any way prejudicial to the reputation or interest of the audit organization.
6. Not to act in any way prejudicial to the reputation, interests or credibility of IRCA.
7. In the event of any alleged breach of this code, to co-operate fully in any formal enquiry procedure.