



Infosec Training Paths & Competencies: Examiner Information

Becoming an examiner
Assessing candidate
submissions
September 2005

Contents

Introduction	3
About the ITPC scheme	4
The role of the examiner	5
Applying to become an examiner	6
Confidentiality	7
Processing successful submissions	7
Processing failed submissions	7
Appeals	8
Key information for examiners	9
Candidate's supporter	9
Target competencies	9
Registration with the scheme	9
Attending the courses	9
The project	10
Making an assessment	11
Certificate submission	11
Table of target competencies	11
Certificates of attendance	11
Learning logs	12
Supporter's letter	12
Project dissertation	12
Judgement calls	12
The waiver path route	15
Scheme contacts	16

Introduction

Welcome to the Infosec Training Paths & Competencies Scheme.

This booklet is intended both for those considering applying to become an ITPC examiner and for those who have already been appointed to this important role. It includes details of the ITPC scheme, guidance on assessing candidate submissions and sources of help.

We hope that you will feel free to contribute any ideas you have for improvements – do get in touch with us.

The ITPC Scheme
Cabinet Office CSIA
6th Floor
Stockley House
130 Wilton Road
London SW1V 1LQ

itpc@cabinet-office.x.gsi.gov.uk

www.seriousaboutinfosec.gov.uk

About the ITPC scheme

The Infosec Training Paths & Competencies (ITPC) scheme offers competency-based qualifications that accredit the knowledge, learning and skills of information security specialists in the Manual of Protective Security (MPS) user community – government, police and accredited contractors.

ITPC is managed by the Cabinet Office Central Sponsor for Information Assurance (CSIA) with the support of a steering committee, including representatives from government and the police as well as academia and affiliated bodies.

The scheme awards a range of *Certificate of Infosec Competency* qualifications, each geared to a set of core competency profiles: these include the Government Practitioner Certificate, and specialist certificate for Accreditors and Comsec roles. The Certificate is recognised across the MPS community, and also as an entry qualification to Infosec MSc programmes offered by UK universities, and qualifications offered by bodies such as (ISC)² and ISACA (for further details see the ITPC website).

The Certificate syllabus for candidates comprises two tiers of formal training followed by a project applying the learning in their work, explained in a dissertation. The syllabus must normally be completed within two years, although it should be possible to complete it within one year. The training providers currently offering courses for this syllabus include the National School of Government (formerly CMPS) and CESG, as well as some private sector training providers. All three learning levels focus on addressing the core competencies contained in the Infosec competencies matrix, which can be found on the website. Further information is given in the Candidate handbook, also available on the website.

ITPC also recognises an optional level of learning, which may be taken following the two formal tiers and before or during the work-based project. This might be attendance at a technical security course available outside the scheme, or taking the BCS ISEB *Certificate in Information Security Management Principles*. While none of these are core requirements for the award of the certificate, ITPC recognises the benefits of such additional learning in the event that a candidate's certificate submission is considered borderline.

The role of the examiner

As an examiner, your role is to assess the dissertations sent to you by the ITPC scheme on behalf of the candidate. Every effort will be made to ensure you receive dissertations on subjects in which you have experience; submissions for the specialist certificates will wherever possible be sent only to examiners with relevant experience. Certificate submissions will normally be forwarded to you by the National School of Government, except where protective marking requires that they are handled by the ITPC staff within Cabinet Office CSIA.

It is important for the credibility of the scheme that certificate submissions are assessed promptly: you should aim to report your assessment of a submission to the National School of Government (NSG) within four weeks of receiving it. If, for whatever reason, you feel you are unable to do this, you should alert the National School who may elect to forward the submission to another examiner.

There is no fixed term for remaining an examiner: you must commit to a minimum of one year and may continue to do this work as long as you feel able to do so. The National School of Government will reimburse examiners for incidental expenses incurred in performing assessments – examples include telephone calls and postage charges.

Note that the scheme will perform quality assurance checks on assessments as well as on certificate submissions themselves.

The scheme reserves the right to remove examiners from its register if any of the following circumstances apply:

- The examiner has been shown to have allowed personal, commercial or other similar considerations to influence an assessment.
- The examiner has broken the confidentiality of the content of a submission, retained or used material/knowledge gained through assessment in an unauthorised manner.
- The examiner fails in a number of instances to report submission assessments within the maximum four week period.
- The examiner's assessments do not in a number of instances adequately justify their decisions to pass or to fail submissions.
- The examiner's feedback to candidates (in the event of submission failures) does not in a number of instances give adequate guidance on how to improve their submission for reassessment.

Applying to become an examiner

In order to maintain the integrity of the ITPC scheme, examiners are required to meet consistently high standards of assessment. Those applying to become examiners are therefore required to have:

- a minimum five years' practical experience of Infosec, relevant to their sphere of work
- a good knowledge of government Infosec policy and implementation implications; and
- an in-depth understanding of at least one particular aspect of Infosec.

Prospective examiners should complete the application form (available on the website) and submit this to the scheme together with:

1. A portfolio establishing the length and breadth of your Infosec experience. This should include:
 - a CV outlining your career to date;
 - an account of your current role, illustrating how this relates to other business functions;
 - an account of a recent piece of Infosec work which demonstrates a risk management approach to a particular information security challenge; and
 - a copy of the appropriate core competency profile, with illustrations of how you meet each competency description.
2. Supporting statements from two referees. These should preferably be involved in Infosec work themselves, though line manager references will also be acceptable.
3. A commitment to undertake the examiner role for a minimum period of one year.
4. A formal commitment to uphold the scheme's Code Of Conduct (see previous page).

On appointment, examiners are awarded the *Certificate of Infosec Competency*.

Processing candidate certificate submissions

The National School of Government acts as the clearing house for ITPC certificate submissions. The ITPC scheme retains submissions and examiner comments for a minimum period of one year, for quality assurance and to support the scheme appeals procedure.

ITPC asks that candidates aim to submit only documents that do not require protective marking. However, we recognise that this may not always be possible. Where submissions are protectively marked, the ITPC secretariat within Cabinet Office CSIA fulfils the handling role: in such cases the references to the NSG in the following paragraphs would apply instead to CSIA.

When a certificate submission is received from a candidate, the NSG will first check all the required components are present. Wherever possible, submissions will be matched with examiners who have some expertise in the dissertation subject area. To ensure anonymity, the cover sheet of the dissertation will be removed and the only identifier used will be the candidate's scheme reference number.

Confidentiality

To maintain the integrity of the assessment procedure, examiners and candidates are not identified to each other. Therefore you should not seek to identify the candidate, nor make your identity known to him. All communication between the examiner and the candidate must be conducted through the NSG, and all feedback on the dissertation should be given on the assessment form supplied by the NSG with the submission and using your examiner reference number.

If upon receipt of a submission from the NSG you realise that the candidate's identity is known to you, for example through the context of the dissertation, then you should contact the National School at once so that they can forward it to another examiner.

Processing successful submissions

If your assessment is that the candidate has met the Scheme's criteria, return the dissertation to the NSG together with the assessment form confirming that the submission has passed. The NSG will endorse your pass to the scheme secretariat, who will in turn issue the Certificate Of Infosec Competency to the candidate.

Processing failed submissions

If your assessment is that the submission has failed to meet the scheme's criteria, return it to the NSG, together with clear and detailed feedback on the assessment form. You are required to give the candidate unambiguous instruction on how to amend or otherwise raise the level of the submission to achieve a pass when resubmitting.

Candidates are permitted two resubmissions, each of which must be made within three months of receiving feedback on the previous submission. A second submission will normally be sent to the same examiner, so that you can decide whether the candidate has successfully met the requirements you previously stipulated in your feedback to them. Third certificate submissions will be referred to a different examiner.

Appeals

If a candidate has had three unsuccessful certificate submissions, and has been declared failed, they may appeal directly to the scheme secretariat to review the decision. In such cases, the secretariat would review the three submissions and the examiners' comments, and consult with the examiners. If the secretariat disagrees with the decision, they may overrule the examiners and award the certificate.

Key information for examiners

This section outlines the key points of the scheme which you need to know when assessing certificate submissions. They apply equally to the Government Practitioner and specialist certificates. More detailed guidance for candidates is contained in the scheme's Candidate Handbook, available on our website.

Candidate's supporter

The scheme requires all candidates to have a supporter or mentor. Normally, this will be a line manager but there are circumstances where someone else may be more appropriate. The key requirement for a supporter is that they have sufficient knowledge of information security or local business security requirements to judge whether the candidate has correctly identified and, later, achieved their target competencies.

The candidate's supporter is required to:

- agree with the candidate their Target Competencies and endorse these to the scheme;
- provide opportunities for the candidate to put their formal learning into practice;
- monitor the candidate's progress toward achieving their Target Competencies; and
- endorse the candidate's dissertation to the scheme.

Target competencies

The booklet **The Infosec Competencies** (available on our website) contains the matrix of Infosec core competencies for all ITPC certificate training paths.

The core competencies are expressed in generic terms. Candidates are required to take each core competency in turn and add to it some detail which is both relevant to their work and can be measured in some way by their supporter and by you, the scheme's examiner.

Registration with the scheme

Before the candidate can begin work towards the certificate, they must register with the scheme by submitting their target competencies, accompanied by an endorsement from their supporter. If the secretariat approve the target competencies, they confirm registration with the candidate and allocate an ITPC reference number.

Attending the courses

Ideally candidates will first attend an induction level course then, three to six months later, a practitioner level course. However, those who first learn of the scheme during a practitioner level course must also complete an induction level course. The two courses do not need to be taken with the same training provider, but both must be accredited for the certificate.

Candidates must complete simple learning logs, noting the main points that were of relevance to them each day. These logs form part of the certificate submission, and examiners should assess from these whether the candidate has understood the points taught on the courses.

Candidates are also required to retain the certificate of attendance given to them by the training provider on completing each course, and include these as part of their certificate submission.

The project

The candidate's project should, wherever possible, be work-based and must be agreed with their line manager and/or supporter. For Government Practitioner submissions, there is virtually no constraint on subject matter, other than that it addresses an aspect of information security as it is practised in Government. It may be entirely technical in nature, entirely strategic, or a mix of those. It may be about implementing Infosec, developing policy or providing consultancy. For specialist submissions, however, the project and dissertation must be about active involvement in the specialist area, for example a project and dissertation for the Accreditor certificate should cover active involvement in an accreditation exercise; preferably as an Accreditor or perhaps a member of an Accreditation Panel.

The project must provide the candidate with the opportunity to achieve their target competencies and demonstrate that they:

- understand the concepts and terminology of Infosec as managed within government;
- appreciate the implications their own Infosec role has within their organisation; and
- bring a risk management approach to Infosec that integrates with business needs.

Making an assessment

This section describes the scheme's assessment criteria, and offers some guidance on how to go about making your assessment. It also covers the actions you are required to take when passing or failing a candidate's certificate submission.

Certificate submission

The National School of Government will forward you certificate submissions comprising all of the following elements, each labelled with the candidate's scheme reference number:

- table of target competencies;
- certificates of attendance;
- learning logs;
- supporter's letter; and
- project dissertation.

The National School of Government will check the candidate has provided all the required documents. If this is not the case, the NSG will return the certificate submission to the candidate and request a full set of documents be resubmitted. The NSG will also ensure the cover sheet provided with the certificate submission is removed so that the candidate's personal details are not known to you: to maintain the integrity of the assessment procedure, examiners and candidates are not identified to each other.

Table of target competencies

Check the target competencies submitted by the candidate are the same as those originally submitted to the scheme. In exceptional circumstances (change of job/role or work targets outside the candidate's control), ITPC allows that some target competencies may be changed during the period of study toward the certificate award. If this is the case, the candidate must document these and explain to your satisfaction that such changes were unavoidable. If you are not satisfied that these claims are reasonable you may fail the certificate submission.

Certificates of attendance

Check the candidate's certificates of attendance for both induction and practitioner level courses fall within two years of the certificate submission date. Photocopies of certificates are acceptable: because candidates must remain anonymous to examiners, personal details should have been removed.

In addition, the candidate may submit certificates of attendance from other, non-scheme, courses. These should be taken into account only if you feel the dissertation is borderline and want to be satisfied the candidate has a good technical knowledge of Infosec issues.

Learning logs

Check the candidate's learning logs (from scheme induction and practitioner level courses only) show an understanding of the teaching points they record. Candidates are required to note only those which are of relevance to them. Learning logs can be brief, even bulleted, notes, and quality of presentation should not be a factor in your assessment of the certificate submission. You should only be concerned about failing a submission where the dissertation falls below standard and the learning logs show clear misinterpretation of Infosec issues.

Supporter's letter

Check the supporter has provided a brief statement to verify the account the candidate gives in their dissertation. They should also confirm they are satisfied the candidate has achieved their target competencies to a satisfactory level. This part of the certificate submission is required more to ensure the candidate's supporter provides mentoring than to aid in your assessment.

Project dissertation

Check the dissertation comprises around 3,500-5,000 words, excluding supporting information such as cover notes, references, glossaries and the like. If the dissertation is substantially shorter than required (say, 2,500 words) then it should be failed; allow slight shortfalls – the content, and proof of target competency achievement, are the primary criteria for the award.

Check that each target competency is referenced in the text and that the candidate has provided evidence of achieving it. Candidates are expected to define key Infosec concepts covered in the induction level course, such as risk management, defence-in-depth and system accreditation. Where these are mentioned, check the candidate gives a definition which complies with the Government stance. Candidates are also required to illustrate that they understand how their Infosec activities relate to other internal and external business activities. Check there is evidence of this.

Most of all, candidates are required to illustrate a risk management approach to Infosec: they must provide a reasoned account of a particular issue or piece of work they have undertaken, provide evidence of the options and constraints that they encountered and give good reason for taking the course of action they followed to achieve an Infosec objective.

Judgement calls

The certificate requirements have been designed to make assessment as simple as possible. In the majority of cases, you should be able to determine easily whether the submission is worthy of a pass. However, there will inevitably be times when you will need to exercise judgement. These notes may help.

Remember that the certificate award is for basic competency. However, candidates must give persuasive evidence of meeting their target competencies and must convince you of three things:

- That they recognise and understand the concepts and fundamentals of Infosec. Key points here include the risk management principle, the meaning of 'defence-in-depth' and its benefits, the accreditation process and its components.
- That they understand the implications of their work and how it affects local business requirements. For example, how does their role interface with others in the organisation and who are their key contacts inside and outside the business? For Accreditor certificate candidates, do they show the ability to make sound judgements irrespective of any business or 'political' pressures brought to bear?
- That they have brought a pragmatic, risk-management approach to Infosec, which recognises and accommodates business requirements. For example, if they have faced a scenario where the security requirement appeared in direct opposition to the business need, how did they resolve that? If they have been in a situation where it appeared that organisational or national policy would prevent the business achieving its goals, again, how did they resolve this? For Accreditor certificate candidates, if they allowed conditional accreditation of a system, what were their reasons and how did they manage that situation?

When assessing the dissertation, ask yourself, "Does this candidate broadly know what Infosec is about?" In other words, does the text persuade you that the author could be entrusted with Infosec responsibility at the level at which they currently work? If you are in any doubt about how to proceed, contact the secretariat for advice.

Poorly completed learning logs should not in themselves constitute a failure; we all learn in different ways and some are better note-takers than others. As long as what has been entered is not factually wrong or misleading (suggesting some basic misunderstanding), then they should be considered adequate.

The line manager's supporting letter should not significantly influence your deliberations. It is principally required to ensure the integrity of the dissertation. If, however, you feel the statement lacks an understanding of the project, you may wish to query this aspect via the secretariat.

The following checklist may be useful: failure to answer two or more questions satisfactorily will normally mean that the submission should be failed.

Certificate submission component	Assessment check
Table of target competencies	<ul style="list-style-type: none"> • Does the candidate's copy match the set of target competencies submitted on entry to the scheme? If not, does the candidate provide adequate reasons (for example, changes in work circumstances outside their control) for any changes?
Certificates of attendance	<ul style="list-style-type: none"> • Do the certificates come from accredited training providers? • Do the dates of attendance fall within the 2-year time limit for completing the certificate syllabus?
Learning logs	<ul style="list-style-type: none"> • Do the logs show an understanding of the points noted?
Supporter's letter	<ul style="list-style-type: none"> • Does the supporter agree with the candidate's description of their achievement of target competencies?
Project dissertation	<ul style="list-style-type: none"> • Does the text amount to 3500-5000 words? • Are all the candidate's target competencies (or, for waiver candidates, the core competencies) referenced, and enough explanation of their achievement given in each case? • Does the candidate define core concepts such as risk management, defence-in-depth and accreditation? • Does the candidate show they appreciate how their Infosec activities relate to other internal or external business functions? • Does the candidate give detailed illustration of a risk management approach to an Infosec issue they encountered in the workplace?
Overall	<ul style="list-style-type: none"> • Does the certificate submission as a whole demonstrate that the candidate understands the need for information security and could be entrusted to manage systems that process sensitive assets?

The waiver path route

ITPC recognises that candidates with adequate work experience should not be required to undertake the formal training components of its syllabus. However, it exercises due rigour in assessing applications for waivers from the standard training route.

To qualify for a waiver, the candidate must submit:

1. A CV outlining their career to date, and concentrating in depth on their current role. This must satisfy you, the examiner that the Candidate has:
 - a minimum three years' experience of Infosec, relevant to their sphere of work;
 - a good knowledge of government Infosec policy and implementation implications; and
 - an in-depth understanding of at least one particular aspect of Infosec
2. Supporting statements from two referees; these should preferably be involved in Infosec work themselves, though line manager references will also be acceptable.
3. A dissertation in a similar format to that for training path candidates, reflecting some recent piece of work or research. ITPC allows some flexibility in the size and nature of the dissertation, but it must convince you, the examiner, that the candidate:
 - understands the concepts and terminology of Infosec as managed within government;
 - knows the requirements and implications of the information security work that they undertake; and
 - can apply a risk-based, risk management approach to securing information in a way that addresses the business needs without compromising the security requirement

In making your assessment of waiver submissions you should therefore apply the same basic criteria as for training path submissions. However you should also be satisfied that the candidate meets or exceeds the relevant Infosec core competencies as listed in the Infosec Competencies booklet. The referees' statements replace that of the supporter, and the certificates of attendance and learning logs obviously do not apply in the case of waiver candidates.

Scheme contacts

**ITPC scheme
secretariat**

Cabinet Office CSIA
6th Floor
Stockley House
130 Wilton Road
London
SW1V 1LQ

www.seriousaboutinfosec.gov.uk
itpc@cabinet-office.x.gsi.gov.uk

**National School of
Government**

Sunningdale Park
Larch Avenue
ASCOT
SL5 0QE

www.nationalschool.gov.uk

01344 634575

CESG

Course Administration
Room A2J
CESG
Hubble Road
Cheltenham
GL51 0EX

www.cesg.gov.uk

01242 221491 ext 34954