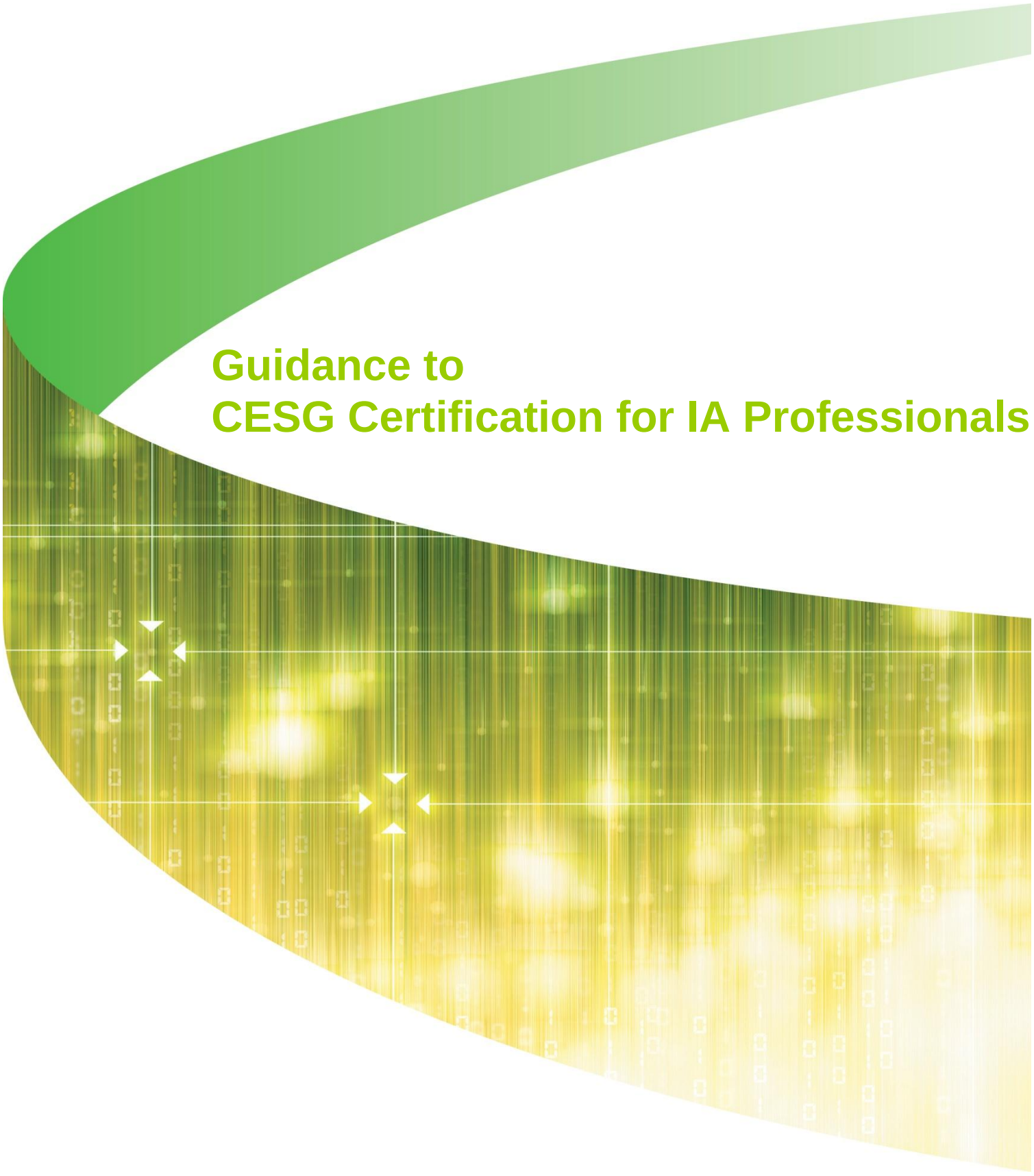
January 2015
Issue No: 2.1

Guidance to CESG Certification for IA Professionals



CESG

NATIONAL TECHNICAL AUTHORITY
FOR INFORMATION ASSURANCE

Guidance to CESG Certification for IA Professionals

Issue No: 2.1
January 2015

Document History

Version	Date	Comment
1.0	September 2012	First issue Comprises guidance chapters previously incorporated in CESG Certification for IA professionals, with various changes as listed. Change of role title from Security Architect to IA Architect Clarification of the differences between Practitioner, Senior Practitioner and Lead Practitioner – see Chapter 3 Incorporation of Bloom's revised taxonomy of knowledge into the skill assessments – see Chapters 4 and 5 Revision to good evidence requirement and progression (paras 25 and 26) – see Chapter 5 Option for Certification Bodies to use IISP Skill Group J in lieu of SFIA responsibility levels – see Chapter 5 Addition of guidance for applicants – see Chapter 6 Addition of guidance for employers and clients – see Chapter 7 Addition of code of conduct – see Chapter 8 Also includes changes made to the CESG Certification for IA professionals document made at issues 1.1 and 1.2 The IA role definitions and IISP skills supplements will be found in CESG Certification for IA professionals
2.0	March 2014	Second Issue Incorporates changes to reflect the introduction of the CESG for IA professionals (CCP) scheme to industry in September 2013. Introduction of the Penetration Tester role – see Chapter 3 Headline skill statements revised to include addition of the Applied Research skills ITPC discretionary migration paragraph removed from Guidance to Certification Bodies in Chapter 5 Additional paragraph in Chapter 6 – Guidance for Applicants, introducing the STAR method for presenting evidence
2.1	January 2015	Third Issue Incorporates a number of minor changes, providing a little further clarification of Practitioner, Senior and Lead levels. Provides more context on the four levels used for Penetration Tester role (paragraphs 12 and 13). Highlights the intention to encourage wider private sector take up. References the start of the CESG Certified Training (CCT) scheme. In Table 1, extends the COMSO role to individuals working to PCI/DSS.

Purpose & Intended Readership

This document contains guidance on CESG's Certification for Information Assurance (IA) Professionals (reference [a]). It is relevant to all IA professionals who work in, or for, the public sector and to those who recruit, select, train or manage them.

The framework is also relevant to IA professionals working in the private sector. The framework contributes to Objective 4 of the UK Cyber Security Strategy (reference [b]), building the UK's cross cutting knowledge, skills and capability to underpin all cyber security objectives.

It is planned that the scheme will be extended internationally in the future.

Executive Summary

CESG has developed a framework for certifying IA professionals who meet competency and skill requirements for specified IA roles. This will enable recruitment from a pool of certified security professionals.

The framework has been developed in consultation with Government departments, academia, industry, the certification bodies, and members of the CESG Listed Advisor Scheme (CLAS), (reference [c]) and CREST. The framework includes a set of IA role definitions and a certification process.

The set of role definitions:

- Covers the IA roles most commonly used across the public sector, many of which have equivalent roles in the private sector
- Typically defines each of the IA roles at three levels[1]
- Aligns each role level with responsibility levels defined by The Skills Framework for the Information Age (SFIA), (reference [d])[2]
- Describes each role in terms of its purpose and the skills required at each responsibility level
- Uses the set of skills defined by the Institute of Information Security Professionals (IISP), (reference [e])
- Supplements the IISP [3] skill definitions to aid assessment against them
- Is detailed in CESG Certification for IA Professionals

The certification process:

- Has been defined in detail and is operated by three Certification Bodies (CBs) appointed by CESG:
    - APM Group – www.apmg-ia.com
    - BCS, the Chartered Institute for IT Professionals – www.bcs.org
    - IISP, RHUL and CREST consortium – www.iisp.org
- Assesses applicants against the requirements of the role definitions, skills and SFIA levels

[1] The Penetration Tester role has been defined at four levels. At this time there is no intention to introduce this additional level for existing roles, although new roles may have a fourth level. See Chapter s 3 and 5.
[2] The Skills Framework for the Information Age is owned by the SFIA Foundation: www.SFIA.org.uk
[3] The IISP Skills Framework is copyright © The Institute of Information Security Professionals. All rights reserved. The Institute of Information Security Professionals ® IISP ® M.Inst.ISP ® and various IISP graphic logos are trademarks owned by The Institute of Information Security Professionals and may be used only with express permission of the Institute.

- Includes the issue of certificates endorsed by CESG stating the IA role and responsibility level at which the applicant has been assessed as having performed competently.

IA professionals working in or for the public and private sectors are encouraged to apply for certification to demonstrate their competence in their IA role.

Feedback

CESG Information Assurance Standards and Guidance welcomes feedback and encourage readers to inform CESG of their experiences, positive or otherwise in this document. Please email: enquiries@cesg.gsi.gov.uk

Contents:

Chapter 1 - Introduction

Key Principles

- Improving the level of professionalisation in IA is an objective of the UK Cyber Security Strategy
- Certification aims to improve the matching of requirements for IA expertise and the competence of those recruited or contracted to provide that expertise

1. The public sector is accountable to Parliament for protecting a vast array of sensitive data supporting many public services. The sophistication of the threats to that data, the complexity of the information systems and the high potential business impacts of data loss, leave the public sector increasingly dependent on Information Assurance (IA) specialists to manage information risks. The complexity of the skills and competencies required of these specialists continues to grow. The public sector cannot do this work alone and will rely on products, services and systems from the private and industry sectors to extend reach, effectiveness and capability. Consequently, improved IA professionalisation is an objective of the UK Cyber Security Strategy (reference [b]).

2. Whilst there is substantial overlap between public sector IA requirements and those of other sectors, the former are determined by a distinct combination of threats, business impacts and public expectations. The public sector therefore needs to articulate the competencies required of the IA professionals working within it, to formally recognise the IA skills of those who have them, and to encourage their continuous professional development. To meet this need, CESG has established a framework to certify the competence of IA professionals in performing common public sector IA roles. The framework is consistent with ISO 17024, 'Conformity assessment - General requirements for bodies operating certification of persons' (reference [f]) and aims to improve the matching between public sector requirements for IA expertise and the competence of those recruited or contracted to provide that expertise.

3. If you are an IA specialist working in or for either the public or private sectors, the certification process will give you the opportunity to have your competence to perform an IA role independently verified. The IA role definitions will also help you plan your professional development. Chapter 6 provides guidance for applicants for IA certification.

4. If you are involved in the recruitment, selection, management, development or promotion of IA professionals, the role definitions will provide template specifications of common IA roles. With refinements to meet any local requirements, these can form the basis for job specifications, promotion criteria or practitioner development requirements. The certification process gives you the option of setting certification as a requirement for job applicants or as an objective for jobholders. Recruiters should note that whilst the certifications offer significant assurance over competence of individuals that they will still need to perform a detailed review of the candidate's skills – as some of the

roles, particularly the SIRA role is extremely broad and covers a very wide range of experiences. Chapter 7 gives guidance for employers and clients of certified IA professionals.

5. Certification Bodies (CBs) assess competence in a variety of ways depending on the skills needed for a role. The assessment process will typically include review of written evidence, knowledge testing, input from referees, an interview, recommendation from assessors, and a final decision by a ratifying panel. The more senior the role, the more extensive the assessment is expected to be. Guidance for CBs and their assessors is at Chapter 5.

Chapter 2 - Concept of Operation

Key Principle

- IA professionals apply to Certification Bodies appointed by CESG for certification against a role at a specific level

6. The components of the framework are illustrated in Figure 1. CESG owns the set of IA roles and supplemented skills defined in the companion document, CESG Certification for IA Professionals. These have been, and will continue to be developed in consultation with advisory bodies drawn from Government departments, industry, academia and CLAS.

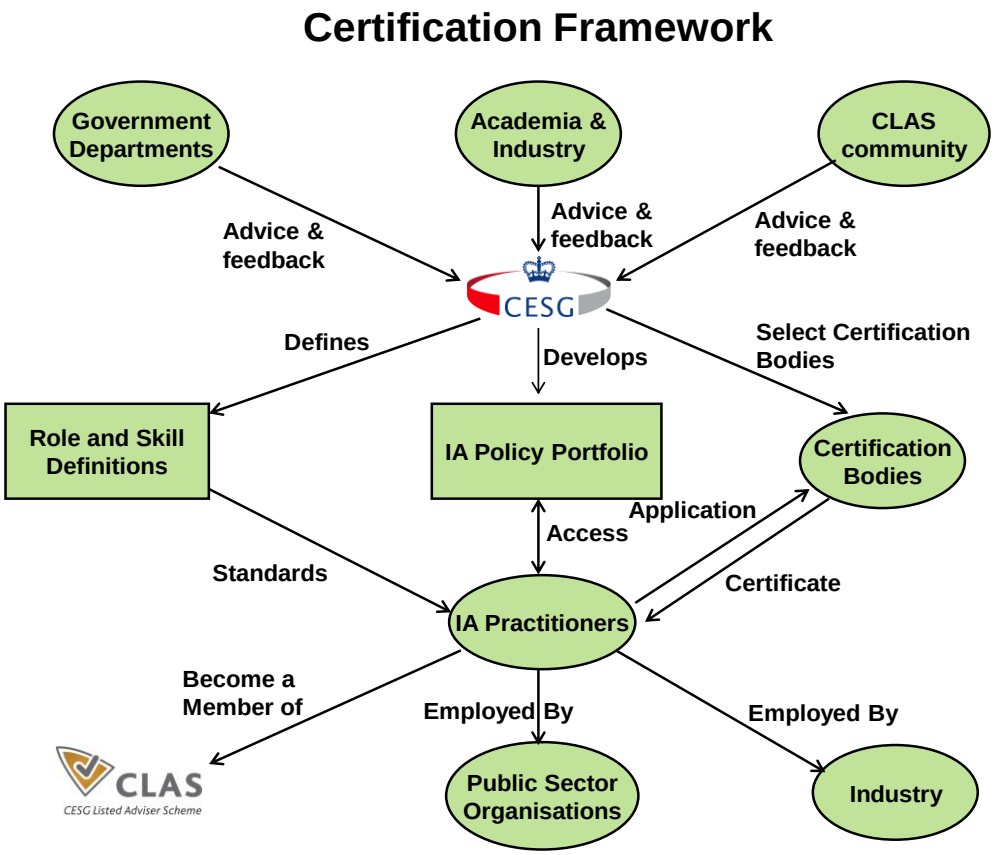


Figure 1: Certification Framework

7. CESG has appointed three CBs who will assess IA professionals against the requirements of the role definitions. IA professionals can use their certificates as evidence to prospective employers, clients or promotion panels of their competence to perform the defined role at the level to which they have been certified. CBs will charge IA professionals for their certification. It is expected that details of those certified will be available from the respective CB websites.

8. It is intended that the role and skill definitions will drive professional development of IA across both the public and private sectors.

9. The IA certification framework should:

   a. Improve matching between public and private sector requirements for IA expertise and the competence of employed and contracted IA professionals.

   b. Encourage IA practitioners to develop all the skills needed in order to become fully effective.

   c. Provide assurance that certified IA professionals meet the requirements of the IA role definitions.

   d. Provide clearer definitions of the skills required for IA roles.

   e. Facilitate the recruitment of staff from a growing community of cyber security professionals.

10. To assist the provision of training, CESG aspires to enable training providers to develop training courses that will be assessed against the IISP Skills Framework. The first CESG Certified Training (CCT) courses were launched in November 2014. Further details on the implementation of the certification and training schemes will be found at www.cesg.gov.uk (Awareness and Training).

Chapter 3 - Role Definitions

Key Principles

- Each IA role is typically defined at three levels of competence that are aligned with responsibility levels defined by The Skills Framework for the Information Age (SFIA)
- The Penetration Tester role is defined at four levels. At this time, there are no plans to extend this to other existing roles
- Each IA role is defined in terms of the IA skills required to perform it

11. Roles are defined at three levels, Practitioner, Senior Practitioner and Lead Practitioner, which are aligned with levels of responsibility defined by SFIA. The full set of SFIA levels of responsibility is[4]

    1 Follow
    2 Assist
    3 Apply
    4 Enable
    5 Ensure/Advise
    6 Initiate/Influence
    7 Set strategy/inspire

12. SFIA defines each level of responsibility in terms of autonomy, influence, complexity and business skills. These are referred to elsewhere in this document as the SFIA responsibility attributes. Most of the Practitioner, Senior Practitioner and Lead Practitioner role levels align with SFIA levels 2, 4 and 6 respectively. The Penetration Tester role aligns these levels at 3, 4 and 6 respectively, but does introduce a fourth (Principal level) with a SFIA level of 5. The baseline entry for certification to the scheme is set fairly high, and expects applicants to provide evidence of practical application of the skill/role. Having related qualifications, but with no practical experience will not gain certification. Practitioners typically support work on a single project, information system, service or business unit. They may have no experience as an IA Practitioner beyond their current client, assignment or business unit. They work with some supervision and can be trusted to deliver routine tasks. Experienced and competent Practitioners will generally develop into Senior Practitioners.

13. Senior Practitioners typically work with clients or service owners to contribute to the success of a programme or multiple projects. They have sufficient experience to handle significant complexity and require little supervision.

[4] Text from the Skills Framework for the Information Age quoted by kind permission of The SFIA Foundation: www.SFIA.org.uk

14. Lead Practitioners typically:

    a. Have influence across a Senior Information Risk Officer's (SIRO) area of responsibility.

    b. Influence the corporate investment portfolio or corporate governance to optimise the balance between security and other business objectives.

    c. Ensure that IA contributes to strategic business objectives.

    d. Provide 'thought leadership' for the profession/skill.

15. Lead Practitioners especially require strong SFIA responsibility attributes in addition to IA skills to meet the role requirements. Just being an experienced and competent Senior Practitioner is not sufficient to become a Lead Practitioner.[5] Additionally without some experience at Senior Practitioner level it would be difficult to demonstrate IA competence at the Lead Practitioner level.

16. The Penetration Tester is primarily an industry role. Unlike the other portfolio roles it has been developed at four levels to meet the needs of the profession and to raise standards. It includes a Principal level, acknowledging both the leadership and technical consultancy element of the role whilst retaining the specialist skills required at the Senior level.

17. Each role definition includes the role purpose and a headline statement of the responsibilities normally expected at each level. Illustrative duties consistent with the headline statement are given plus an indicative set of information security skills.

18. The scope of the certification framework is the set of IA roles that are in common use across the public sector, and of which CESG has some ownership, with the addition of industry facing roles. The current list is at Table 1 below. The roles are derived from three sources:

    a. Roles commonly undertaken by CLAS members.

    b. Roles recognised in the HMG Security Policy Framework (SPF), (reference [g]).

    c. Other roles believed to be widely used across industry and the public sector.

19. Some CCP roles may not match in name to those performed in some areas of the public sector and in industry. For example, the Auditor role as defined in the CCP portfolio might be similar to compliance roles elsewhere. Variations in job titles will be many, but when deciding if the CCP scheme is relevant it is important to understand the selected CCP role purpose and responsibilities and to be able to meet the headline statement for that specific role.

[5] Similarly, good project managers do not always make good programme managers and it is not essential for programme managers to have been project managers.

20. Some roles can be readily grouped together as different levels of a more generic role. For this reason the roles of IT Security Officer (ITSO, as mandated in the SPF), Information System Security Manager and Information System Security Officer have been grouped together. Similarly, the Crypto Custodian is a subset of the Communications Security Officer (ComSO) role and consequently these two roles have been grouped together. Some changes to the COMSO role have been introduced to reflect those who perform similar functions, but in accordance with PCI/DSS rather than government standards.

21. No hierarchy is intended among these roles. It is assumed that the ITSO and ComSO will typically report to the Department Security Officer (DSO). The DSO role is owned by Cabinet Office and currently outside the scope of the certification framework.

22. The Accreditor typically reports to the SIRO, sometimes through a management chain. The SIRO role is owned by Cabinet Office and is also outside the scope of the certification framework.

23. There is no prescribed career path through these roles. Much IA knowledge is common to multiple roles and it would be natural for many IA professionals to perform multiple roles in the course of a career. For small organisations, an IA specialist may perform multiple roles in one post.

24. It is expected that further roles will be defined according to demand for certification against them.

Table 1: List of Roles and their Purpose

IA Role	Purpose
Accreditor	To act as an impartial assessor of the risks that an information system may be exposed to in the course of meeting the business requirement and to formally accredit that system on behalf of the Board of Directors.
Communications Security Officer / Crypto Custodian and deputy/alternate custodian	To manage cryptographic systems as detailed in HMG IA Standard No. 4 (IS4), Management of Cryptographic Systems (reference [h]) and in relevant product specific Security Procedures. This role now encompasses those who perform similar functions albeit for PCI/DSS compliance, rather than in accordance with HMG standards.
IA Architect	To drive beneficial security change into the business through the development or review of architectures so that they: • fit business requirements for security • mitigate the risks and conform to the relevant security policies • balance information risk against cost of countermeasures
IA Auditor	To assess compliance with security objectives, policies, standards and processes.
IT Security Officer/ Information Security System Manager/ Information Security System Officer	To provide governance, management and control of IT security.
Penetration Tester	To provide an independent assessment of the different elements that comprise an information system or product with the aim of finding and documenting the vulnerabilities present.
Security & Information Risk Advisor	To provide business driven advice on the management of security and information risk consistent with HMG IA policy, standards and guidance or with relevant industry or commercial guidance.

Chapter 4 - Skill Definitions

Key Principles

- The IISP has defined a set of Information Security skills and skill levels
- These skill definitions have been supplemented to enable assessment against the skill levels
- The IA roles may be defined in terms of other suitable skill sets if they become available

25. CESG Certification for IA professionals supplements the Institute of Information Security Professional's (IISP) skill definitions in line with the IISP skill level definitions shown in the table below. The skill definitions are supplemented in two respects to aid assessment against each of the four IISP defined skill levels. These supplements have been developed in consultation with the advisory bodies drawn from Government departments, academia, industry and CLAS and other bodies.

    a. Each IISP skill group is supplemented with a statement of the knowledge most relevant to the skill.

    b. Each IISP skill is supplemented with a headline statement of what is expected at each skill level followed by examples of behaviour that is consistent with the headline statement.

26. The IA certification framework assumes a mapping between the knowledge requirements in the IISP skill level definitions and Bloom's revised taxonomy of knowledge (reference [i]). This mapping is shown in Table 2. The taxonomy is described further in Chapter 5.

27. For each skill, a headline statement is provided at each of the four skill levels. These are summarised at Table 3. The headline statements are intended to be consistent with the skill level definitions and the IISP principles and examples given for each skill in the IISP Full Member Application Guidance Notes.

28. Examples of the kinds of behaviour, knowledge, competence, experience, versatility, autonomy or influence that are consistent with the headline statement are given in the Annex on skill definitions. These examples do not form an exhaustive list; other examples may also meet the headline statement. Essential requirements to meet the headline statement are denoted with the term 'shall'.

29. The skill definitions are intended to be cumulative; i.e. to meet the requirements at levels 2, 3 or 4 entails meeting the requirements for lower levels. However, note that role definitions are not cumulative; see Chapter 5.

Table 2: IISP Skills Summary – Definitions for Levels

IISP Skill Level	Applicable Knowledge Level from Bloom's Revised Taxonomy (reference [i])
Level 1: (Awareness) Understands the skill and its application. Has acquired and can demonstrate basic knowledge associated with the skill. Understands how the skill should be applied but may have no practical experience of its application.	Remembering/ Understanding
Level 2: (Basic Application) Understands the skill and applies it to basic tasks under some supervision. Has acquired the basic knowledge associated with the skill, for example has acquired an academic or professional qualification in the skill. Understands how the skills should be applied. Has experience of applying the skill to a variety of basic tasks. Determines when problems should be escalated to a higher level. Contributes ideas in the application of the skill. Demonstrates awareness of recent developments in the skill.	Applying
Level 3: (Skilful Application) Understands the skill and applies it to complex tasks with no supervision. Has acquired a deep understanding of the knowledge associated with the skill. Understands how the skill should be applied. Has experience of applying the skill to a variety of complex tasks. Demonstrates significant personal responsibility or autonomy, with little need for escalation. Contributes ideas in the application of the skill. Demonstrates awareness of recent developments in the skill. Contributes ideas for technical development and new areas for application of the skill.	Evaluating/ Analysing
Level 4: (Expert) An authority who leads the development of the skill. Is an acknowledged expert by peers in the skill. Has experience of applying the skill in circumstances without precedence. Proposes, conducts, and/or leads innovative work to enhance the skill.	Creating

Table 3: Headline Skill Statements

IISP Skill	Level 1	Level 2	Level 3	Level 4
A1 – Governance	Understands local arrangements for Information Governance (IG)	Applies IG standards or processes to local area and to clients beyond it	Develops IG standards or processes; applies IG principles across the organisation	Leads development of IG at the organisation level or has influence at national or international standards level
A2 – Policy & Standards	Understands the need for policy and standards to achieve Information Security (IS)	With supervision and aligned with business objectives, authors or provides advice on IS policy or standards	Without supervision, advances business objectives through development or interpretation of a range of IS policies or standards	A recognised expert in IS policy and standard development
A3 – Information Security Strategy	Understands the purpose of IS strategy to realise business benefits	Contributes to development or implementation of IS strategy under supervision	Influences investment decisions or risk appetites through contribution to development or implementation of IS strategy	A recognised expert in IS strategy development or implementation
A4 – Innovation & Business Improvement	Is aware of the business benefits of good IS	Applies IS to achieve business objectives with some supervision	Supports realisation of strategic business benefits through innovative application of IS	Develops and promotes new concepts for business improvement through IS which are widely adopted across the public sector or an industry sector
A5 – IS Awareness and Training	Understands the role of security awareness and training in maintaining information security	Materially contributes to improving security awareness with some supervision	Delivers, or manages the delivery of training on multiple aspects of IS	A recognised authority on the development of IS Awareness & Training

IISP Skill	Level 1	Level 2	Level 3	Level 4
A6 – Legal & Regulatory Environment	Is aware of major pieces of legislation relevant to IS and of regulatory bodies relevant to the sector in which they work	Understands applicable legislation and regulations relating to IS in the context of own or client organisations	Influences business practices affecting IS through the application of legislation and regulations	Is an authority on an area of legislation or regulation relevant to IS
A7 – Third Party Management	Is aware of the need for organisations to manage the information security of third parties	With supervision, contributes to developing or maintaining compliance by third parties to contracting authority's IS policies and standards	Enhances organisational IS through broad influence on third party management	Advances best practice in third party management with respect to IS
B1 – Risk Assessment	Demonstrates awareness of the causes of information risk and their implications	Understands how to produce risk assessments	Produces complex risk assessments that influence senior risk owners, managers or other stakeholders	Influences development of risk assessment methodologies across and beyond an organisation
B2 – Risk Management	Demonstrates awareness of techniques to manage information risk	Contributes to management of risks to information systems with supervision	Advises management on information risk across a business unit or organisation	Advances the practice of information risk management across the public sector or an industry sector or internationally
C1 – Security Architecture	Is aware of the concept of architecture to reduce information risk	Applies architectural principles to security design with some supervision	Applies architectural principles to complex systems or to bring structure to disparate systems	Extends the influence of security architecture principles across the public sector or an industry sector

IISP Skill	Level 1	Level 2	Level 3	Level 4
C2 – Secure Development	Is aware of the benefits of addressing security during system development	Contributes to the development of secure systems with some supervision	Applies and improves secure development practices used across multiple projects, systems or products	Is an authority on the development of secure systems
D1 – IA Methodologies	Is aware of the existence of methodologies, processes and standards for providing Information Assurance	Applies an IA methodology or standard with some supervision	Verifies risk mitigation using IA methodologies	Enhances the capability of IA methodologies to realise business benefits across the public sector or an industry sector
D2 – Security Testing	Is aware of the role of testing to support IA	Effectively applies testing methodologies, tools or techniques with some supervision	Provides assurance on the security of a product or process through effective testing	Advances assurance standards across a product range, technology, or industry sector through rigorous security testing
E1 – Secure Operations Management	Is aware of the need for secure management of information systems	Monitors the application of SyOPS with some supervision	Manages the development of SyOPs for use across multiple information systems or manages compliance with them	An authority on Security Operations Management, working across the public sector or an industry sector

IISP Skill	Level 1	Level 2	Level 3	Level 4
E2 – Secure Ops & Service Delivery	Is aware of the need for information systems and services to be operated securely	Effectively applies SyOPs with some supervision	Develops SyOPs for use across multiple information systems or maintains compliance with them	Influences SyOPs used across the public sector or an industry sector
E3 – Vulnerability Assessment	Is aware of the need for vulnerability assessments to maintain Information Security	Obtains and acts on vulnerability information in accordance with Security Operations Procedures	Ensures that information risk managers respond appropriately to relevant vulnerability information	Is an authority on the use or impact of vulnerability assessments across the public sector or an industry sector
F1 – Incident Management	Is aware of the benefits of managing security incidents	Contributes to security incident management	Manages security incidents	Is an authority on security incident management across the public sector or an industry sector
F2 – Investigation	Is aware of the basic principles of investigations	Contributes to investigations into security incidents	Leads investigations into security incidents or manages a team of investigators or provides skilled support	Is an authority on security investigations
F3 – Forensics	Is aware of the capability of forensics to support investigations	Contributes to forensic activities, with some supervision	Manages forensic capability or provides skilled support	Is an authority on forensics
G1 – Audit, Assurance and Review	Understands basic techniques for testing compliance with security criteria (policies, standards, legal and regulatory)	Audits compliance with security criteria in accordance with an appropriate methodology	Influences Senior Information Risk Owners or business managers through information risk driven auditing	Advances the influence of security auditing across the public sector or across an industry sector

IISP Skill	Level 1	Level 2	Level 3	Level 4
H1&2 – Business Continuity Management	Understands how Business Continuity Planning and Management contributes to information security	Contributes to the definition or implementation of business continuity processes to maintain information security	Leads definition or implementation of business continuity processes to maintain information security across a business unit or organisation	Is an authority on the information security aspects of Business Continuity
I3 – Applied Research	Understands the fundamental concepts of applied research but does not yet have the knowledge needed to apply this skill in an operational context	Performs research activities under supervision	Leads research tasks, working independently and coaching others	Acknowledged as a leader in the research community

Chapter 5 - Guidance for Certification Bodies

Key Principles

- Certification Bodies have some discretion in how role definitions are interpreted
- Assessments against the role definitions must be based on good evidence

30. For certification against a particular role and level, CBs must assess whether a future employer or client of the applicant could have reasonable confidence that the applicant could repeat the level of competence claimed in similar circumstances. CBs should consider the position of a recruitment consultant who needs to decide whether to recommend an IA specialist to a client knowing that they are only likely to gain further business if the client is satisfied. Certification should give the recruitment consultant justifiable confidence to recommend the certified IA specialist to a range of clients.

31. The crux of any assessment should be whether the applicant has good evidence of meeting the relevant headline statement in the role definition. The evidence of meeting the SFIA responsibility attributes and IISP skill levels should be seen as a strong guide to help assess how well the role headline statement has been met rather than as prescriptive criteria in their own right. For this reason, CBs have some discretion in how much evidence is required.

32. As a guide, successful applicants should provide good evidence of meeting:

    a. The standard in the role definition headline statement for the applicable responsibility level.

    b. The entire core IISP skill levels defined in the role definition (these are in **bold** in the skill tables) except as defined under the Security and Information Risk Advisor and the Auditor role definitions.

    c. All mandatory requirements within core skill definitions (these are denoted by the term ‘shall’).

    d. Three-quarters of all skills required at level 1 or above.

    e. All of the SFIA attributes of responsibility (autonomy, influence, complexity and business skills). Good evidence of only 3 of the 4 attributes can be accepted if the candidate had limited opportunity to demonstrate the fourth attribute, or the assessor had limited time to probe claims made and there was no evidence that the applicant was actually weak in this attribute. However, see para 36 for an alternative to SFIA.

33. The required Bloom's (reference [i]) knowledge level for some of the knowledge listed in the knowledge statement applicable to each core IISP skill. This may be based on evidence from the applicant's work experience or through examination. Guidance on the meaning of Bloom's knowledge levels is given in Table 4.

Table 4: Bloom's Knowledge Levels

Bloom's Revised Level	Name	Ability	Typical Exam Question Style
1	Remembering	Recall or remember information but not necessarily able to use or explain	Define, duplicate, list, memorise, recall, repeat, reproduce, state
2	Understanding	Explain ideas or concepts	Classify, describe, discuss, explain, identify, locate, recognise, report, select, translate, paraphrase
3	Applying	Use the information in a new way	Choose, demonstrate, employ, illustrate, interpret, operate, schedule, sketch, solve, use, write
4	Analysing	Distinguish between different parts	Appraise, compare, contrast, criticise, differentiate, discriminate, distinguish, examiner, question, test
5	Evaluating	Justify a decision	Appraise, argue, defend, judge, select, support, value, evaluate
6	Creating	Provide a new point of view	Assemble, contract, create, design, develop, formulate, write

34. Good evidence of meeting the role headline statement requires at least two examples of how the applicant applied their IA expertise to address a business requirement and what the outcome was. One piece of work may be used as evidence to support multiple skills or SFIA attributes but a variety of work examples provides stronger evidence of deployability to a range of clients.

35. Good evidence will also withstand scrutiny, e.g.:

    a. Was the evidence claimed supported by a referee and was the validity of the reference checked?

    b. Was the candidate credible when probed at interview?

    c. Was knowledge tested in accordance with the IISP skill level and the associated knowledge level from Bloom's revised taxonomy?

    d. Were the example pieces of work sufficiently substantial to demonstrate the SFIA attributes at the claimed responsibility level?

    e. Was the client contacted to confirm the applicant's claims?

    f. Are the examples claimed consistent with the career history described in the application?

    g. Are the skills or knowledge claimed supported by relevant qualifications, training and experience?

36. Certification Bodies have the option of assessing applicants against the IISP Skill Group J instead of using the SFIA responsibility levels. The recommended translation between these two frameworks is given below.

Table 5: Translation between SFIA and IISP Frameworks

SFIA Responsibility Level	Average Skill Level for IISP Skill Group J
1	Not applicable
2	1.5
3	2.0
4	2.5
5	3.0
6	3.25
7	Not applicable

Except where stated otherwise, role definitions are **not** cumulative as one progresses from Practitioner to Lead Practitioner; i.e. it is possible to certify an individual as a Senior or Lead Practitioner without good evidence of the individual being able to fill the role at lower level(s). The rationale behind this is that it ought to be feasible to manage a team without having previously been a member of the team. CBs would need evidence that the applicant has acquired sufficient, additional and pertinent competencies for the required role – especially if technical rather than managerial in nature. However, skill definitions are cumulative; see Chapter 4.

Performance Monitoring

37. CBs are required to take reasonable opportunities to monitor the performance of those that they have certified in order to maintain the credibility of the certification process and their certificates.

Re-certification

38. CBs are required to state how long their certificates are valid for and what the process should be for re-certification. It is expected that some form of evidence of continuing professional development will be sufficient to avoid repeating the complete certification process.

Chapter 6 - Guidance for Applicants

Key Principles

- Applicants are assessed on whether the evidence presented demonstrates competence to perform the role at the level applied for
- Good evidence explains how the applicant applied their IA expertise to help achieve a business objective

39. CBs are tasked with assessing applicants against the role definitions based upon the evidence presented. They do not attempt to assess how effective you are in your current work. CBs frequently either fail applications or return them for further work because applicants have not presented adequate evidence. To avoid this, please note the points below.

40. Applicants should ensure that the evidence presented supports the role(s) and level(s) applied for. Study the role and skill definitions carefully and target your evidence accordingly. The crux is demonstrating work that meets the headline statement in the role definition at the responsibility level for which you are applying.

41. Good evidence typically outlines a business objective, how you personally applied IA expertise to help achieve it and the impact your contribution made. Lists of personal qualities, jobs held or qualifications gained are not, on their own, good evidence as they do not explain what you, as an IA practitioner, have actually achieved or how you personally added value. They may add useful context to actual evidence.

42. Candidates might consider the STAR method when compiling their evidence - Situation, Task, Action, and Result – as this will provide focus that gets to the crux of your work experience. Providing information in a structured manner is more likely to result in a more receptive response to the evidence you are presenting.

43. At Practitioner level, CBs will wish to see evidence of what you have actually done in the role and how you applied IA skills and the SFIA responsibility attributes to fill the role.

44. At Senior Practitioner level, CBs will look for evidence of the ability to analyse business objectives and the associated IA issues, then apply IA expertise to enable some form of business benefit to be achieved.

45. The Principal level has been introduced with and presently applies only to the Penetration Tester role. This level acknowledges both the leadership and technical consultancy breadth of IA knowledge, whilst retaining the specialist skills required at the Senior Practitioner level

46. At Lead Practitioner level, the CBs will look for evidence of applying IA expertise at the organisational level to support strategic business objectives; e.g.

reduced costs or risks, improved business agility or some form of competitive advantage. Lots of experience at Senior Practitioner level (Principal level for the Penetration Tester role) is not sufficient to reach Lead Practitioner level.

47. The level to which evidence may be scrutinised is described in Chapter 5 in the guidance for CBs.

48. CBs offer different approaches to assessment. In choosing a CB an applicant should consider the assessment process, the costs and effort associated with achieving and maintaining certification, support for continued professional development, and any benefits that a CB may offer.

49. CBs have some discretion in how much evidence they require. Details are in Chapter 5.

Chapter 7 - Guidance for Employers and Clients of Certified IA professionals

50. The CESG Certification Standard can support organisations in selecting IA professionals for assignments and it can also be used to guide the professional development of internal staff. Employers or clients who seek to select IA professionals for employment or contracts are advised to note the following:

    a. IA certification does not eliminate the need for care when selecting IA professionals. IA professionals of the same role and responsibility level are not all the same. You will still need to consider how relevant their experience, culture, skills and knowledge is to your needs. The bigger the difference, the longer it will typically take for them to be fully effective in your environment.

    b. Consider what profile of roles and responsibility levels you need. If you need a team, consider the mix of roles and responsibility levels that would best suit your requirements. For instance, one Senior Practitioner may be able to supervise a handful of Practitioners ensuring that the Senior Practitioner's experience is only applied where it is most needed. In this example the Senior Practitioner will also need team leadership skills in addition to their IA specialist skills.

    c. IA is a broad and rapidly evolving field. Even within specific roles, nobody has knowledge and experience across the full scope of the role. Be careful not to assume knowledge or experience that your employee or contractor does not have.

    d. The certification framework aims to identify IA professionals who have demonstrated the role requirements and are sufficiently versatile to apply them in a range of organisations. It still takes time to become effective in a new organisation and more time to become effective in a new sector.

    e. If you are engaging an IA specialist to help to upskill your existing staff then you should consider this skill and capability separately as this is not part of the CESG Certification for IA professionals although some CBs may identify this capability as part of their assessment.

    f. The CBs assess the IA professionals against a common standard but in slightly different ways. You might like to familiarise yourself with the different approaches to ensure that those attributes of the certification process most important to you are employed.

Chapter 8 - IA Practitioners' Code of Conduct

51. CESG expects all Practitioners undertaking work on the basis of its IA certification framework to comply with the following code of conduct in order to uphold the reputation and good standing of the framework.

Table 6: IA Practitioner's Code of Contact

Attribute	Expected Behaviour	Inappropriate Behaviour
Impartiality	• Act in the best interests of the client organisation at all times	• Proposing or undertaking unnecessary or excessive work • Suppressing findings that the client representative does not wish to hear • Recommending inappropriate products or services • Not declaring potential conflicts of interest
Objective	• Base advice on material knowledge, facts, professional experience and evidence	• Being influenced by personal relationships or short term objectives • Ignoring material facts
Confidentiality & Integrity	• Protect information received in the course of work for a client organisation	• Disclosing vulnerabilities in client information systems to third parties • Sharing client information with third parties without permission
Compliance	• Provide advice and ensure that conduct is consistent with applicable laws, regulations and the HMG Security Policy Framework (reference [g]) or other relevant security policies	• Recommending actions that knowingly contravene applicable laws, regulations or policies • Recommending actions which conflict with CESG guidance without drawing the client's attention to the conflict • Undertaking security testing without client permission
Competence	• Meet Certification Body requirements for Continuing Professional Development	• Undertaking work which you know you are not competent to undertake • Presenting yourself as having a higher level of competence than is actually the case

Attribute	Expected behaviour	Inappropriate Behaviour
Proportionate	• Ensure advice is proportionate with business objectives and the level of information risk	• Recommending work that is disproportionately large to business requirements • Recommending solutions that are grossly inadequate to meet the intended business requirements
Reputation	• Preserve the reputation of the IA certification framework	• Conduct that may bring the IA certification framework into disrepute • Using the IA certification brand outside its intended scope

References

[a] CESG Certification for IA Professionals - www.cesg.gov.uk/awarenesstraining/certified-professionals/Pages/index.aspx

[b] The UK Cyber Security Strategy – Protecting and promoting the UK in a digital world - www.cabinetoffice.gov.uk/resource-library/cyber-security-strategy

[c] CLAS - www.cesg.gov.uk

[d] SFIA - www.sfia.org.uk

[e] IISP - www.iisp.org

[f] ISO 17024 - www.iso.org/iso/catalogue_detail?csnumber=29346

[g] HMG Security Policy Framework - http://www.cabinetoffice.gov.uk/media/207318/hmg_security_policy.pdf

[h] HMG IA Standard No. 4, Management of Cryptographic Systems, Issue 6.0, April 2014 (OFFICIAL)

[i] Anderson, L.W. & Krathwohl, D. R. (Eds) (2001). A taxonomy for Learning, teaching and assessing: A revision of Bloom's taxonomy of educational objectives. New York: Addison Wesley Longman. April 2001

Glossary

CB	Certification Body
CCT	CESG Certified Training
CLAS	CESG Listed Advisor Scheme
DSO	Departmental Security Officer
IA	Information Assurance
IISP	Institute of Information Security Professionals
IS	Information System
ITSO	Information Technology Security Officer
SFIA	Skills Framework for the Information Age
SIRO	Senior Information Risk Owner
SyOPs	Security Operating Procedures

IA
CESG
A2i
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX

Tel: +44 (0)1242 709141
Fax: +44 (0)1242 709193
Email: enquiries@cesg.gsi.gov.uk