

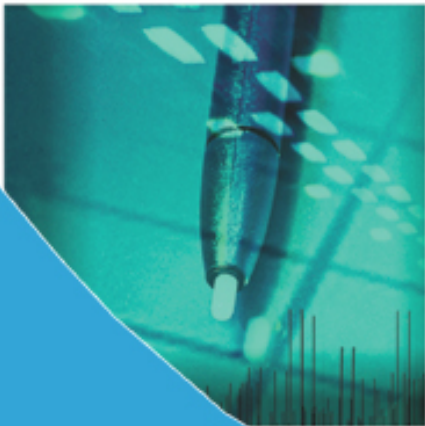
DRAFT



NATIONAL TECHNICAL AUTHORITY  
FOR INFORMATION ASSURANCE

# Accreditor Role Definitions

Part of the Information Assurance Competency  
Framework for use across the Public Sector



DRAFT

**DRAFT**



## Document status

### Document status

Title	Accreditor Role Definitions
Version	0.9
Status	Draft
Date	16th March 2010

Page 2

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on 01242 221491 x30306 (non-sec) or email [infoleg@gchq.gsi.gov.uk](mailto:infoleg@gchq.gsi.gov.uk)

**DRAFT**

# References

A.	HMG IA Standard No 2 – Risk Management & Accreditation of Information Systems, <a href="http://www.cesg.gsi.gov.uk">www.cesg.gsi.gov.uk</a>
B.	Government IT Profession, <a href="http://www.civilservice.gov.uk/it">www.civilservice.gov.uk/it</a>
C.	Institute of Information Security Professionals, <a href="http://www.instisp.org">www.instisp.org</a>
D.	HMG Security Policy Framework, <a href="http://www.cabinetoffice.gov.uk/spf.aspx">http://www.cabinetoffice.gov.uk/spf.aspx</a>
E.	HMG IA Standard No 1 – Technical Risk Assessment, <a href="http://www.cesg.gsi.gov.uk">www.cesg.gsi.gov.uk</a>



# Contents

Document status .....	1
References.....	3
Contents.....	4
Foreword.....	5
Introduction .....	6
Accreditor Role Description .....	7
The Institute of Information Security Professionals (IISP) Skill Set.....	8
Accreditor Role Levels.....	9
Accreditor Roles and Responsibilities.....	10
Accreditor Roles and Responsibilities (Senior Accreditor).....	11
Accreditor Roles and Responsibilities (Lead Accreditor).....	12
Minimum Recommended IISP Skill Levels.....	13
Assessment Process .....	15

## Foreword

Information Assurance has never been so important both to the public sector and to the public as a whole. Citizens expect to access many government services through the Internet and the government aims to use Information and Communications Technology (ICT) to deliver its services effectively. Neither of these is achievable if government cannot demonstrate that it properly protects the information entrusted to it, or if citizens do not have confidence in our ability to do so. To compound the challenge, as business becomes increasingly reliant on availability and accuracy of data and ICT, the sophistication of the threat from Foreign Intelligence Services and organised crime is increasing. The potential impacts of failures in Information Assurance are daunting, and this has been recognised in the UK's first National Cyber Security Strategy.

In this climate, effective accreditation of our Information Systems is vital, and we need accreditors to ensure that the risks to our information systems are understood and addressed so that Senior Information Risk Owners are able to take properly informed judgements about the risks they own. This represents a welcome opportunity to raise the standing of accreditors, but it is not without its obligations. We must demonstrate the usual attributes of a profession: well defined roles based upon defined skills and competencies; documented standards of knowledge and competence; a process to assess fitness for membership of the profession and conditions for retaining membership.

Production of these Accreditor Role Definitions is therefore simply a step on a journey to properly establishing Information Assurance and accreditation as a discipline within the IT Profession in the public sector. Whilst recognising that different organisations will have differing needs, our intention is for these definitions to provide improved consistency across organisations and

that they form the basis with which Senior Information Risk Owners specify the attributes required of their accreditors and for which accreditors are selected for posts and trained to develop their skills. Please embrace them as part of the national requirement for a professional community.

**Simon Kershaw**  
**Head of Accreditation Specialism**

# Introduction

Information Assurance (IA) professionalism is aligned with the Government IT Profession. IA is a prerequisite for the effective use of ICT systems, and just as IA is not a solely technical discipline, so ICT encompasses a wide range of competencies covering technical and non-technical areas. IA's relationship with the Government IT Profession reflects the complementary relationship between IA and IT.

The goal of the Government IT Profession is to enable organisations and individuals to build effective capacity and capability to deliver excellent IT. It aims to drive the development of a more professional government IT workforce by putting into place the right building blocks for the profession – setting the standards, policies and guidance required to ensure that the public sector has capable people and capable organisations, delivering and managing fit-for-purpose IT-enabled projects and services.

The first of these building blocks is the Government IT Profession competency and skills framework – the basis of which is the UK IT industry standard Skills Framework for the Information Age (SFIA). These provide a common language to describe the skills and attributes required of IT professionals.

Work is underway to align the draft IA Competency Framework with the existing Government IT Profession frameworks. However, for the purpose of this draft document we will continue to use the draft IA Competency Framework. One of the specialist skill areas within this is IA Risk Management and Accreditation. This document describes roles within Accreditation at five levels of responsibility. The middle three levels of responsibility are then defined further using a skill set and competency definitions developed by the Institute of Information Security Professionals.

## Purpose

The purpose of this document is to define the role of Accreditor, Senior Accreditor and Lead Accreditor in sufficient detail to:

- Enable reliable assessments of individuals' competence against the role definitions.
- Drive professionalism of accreditation as envisaged by the IA Competency Framework
- Enable greater mobility of accreditors between public sector organisations and to open up more career development opportunities

## Scope

The roles defined in this document are intended to be applicable to all areas of the public sector.

# Accreditor Role Description

Accreditors work on behalf of the Senior Information Risk Owner (SIRO) who is the member of the board of directors accountable for managing information risk. The SIRO will typically delegate some authority for accepting residual risks within the organisation's risk appetite to accreditors but the SIRO remains accountable for all accreditation decisions. In many organisations, accreditors will report to the SIRO through a line management chain which may include the Department Security Officer and/or the IT Security Officer. Whatever the line management chain, there should be an escalation process to ensure that the most contentious accreditation decisions can be escalated from the accreditor to the SIRO.

HMG IA Standard No 2 – Risk Management & Accreditation of Information Systems, reference A, describes accreditation and the role of the accreditor as follows:

*“Accreditation is an independent assessment that an information system meets its IA requirements and that the residual risks, in the context of the business requirement, are acceptable to the business.*

*The role of the accreditor is 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.*

*Although it is necessary for the accreditor to have an understanding of ICT related technology, deep technical knowledge may not be essential depending on the specific requirements of individual posts. It is necessary for the accreditor to consider risk management in the round to ensure the physical, personal, procedural and technical controls are balanced. It is important therefore, that although the accreditor will need to continually develop their technical knowledge, they may also need access to people who have a more professional technical understanding of the technologies involved, to support the accreditation process. To support this requirement, funding should be identified at the outset for any specialist technical advice and services required such as Technical and IA Consultants, IT Health Checks and assurance services.”*

# The Institute of Information Security Professionals (IISP) Skill Set

The IISP has defined a set of IA skills and competency levels<sup>1</sup>. These are available at [www.instisp.org](http://www.instisp.org), reference C. The competency levels are defined as shown below.

## ***Awareness – IISP Level 1***

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.

## ***Basic Application – IISP Level 2***

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.

## ***Skilful Application – IISP Level 3***

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.

## ***Expert – IISP Level 4***

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.

Accreditor roles can be defined in terms of these skills and competency levels. To encourage professionalism it is desirable to align accreditor role definitions with the competency levels expected for Associate and Full Membership of the IISP. This enables one assessment process to meet the needs of the HMG IA Competency Framework and IISP membership.

<sup>1</sup> 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 the express permission of the Institute. The skills and competency level titles, organising structure, and underlying skills description documents, are copyright © The Institute of Information Security Professionals. All rights reserved.

## Accreditor Role Levels

Accreditors operate at multiple levels. This document recognises that there are at least 5 levels and defines skill levels for the middle 3 levels:

- **Trainees** who only make accreditation decisions under close supervision. Trainees may enter the accreditation specialism from many different backgrounds so there are no pre-requisite IISP skills required to start training.
- **Accreditors** who are trusted to make routine accreditation decisions with little supervision.
- **Senior Accreditors** who are trusted to lead the accreditation of complex, high risk or precedent setting systems and to judge when to escalate accreditation decisions. Senior Accreditors may also supervise Accreditors, assist in policy development and improvement in accreditation processes.
- **Lead Accreditors** who have wide experience and are responsible for ensuring that the accreditation process in their organisation meets the standards detailed in HMG IA Standards Nos 1 & 2, references A and E.
- **The Head of Accreditation Specialism** who is responsible for driving improvement in the quality and effectiveness of accreditation across a large organisation or group of organisations. An overall Head of Accreditation Specialism is appointed by the Accreditors' Forum to lead for HMG as a whole. Within organisations this role will be filled only where there is a particularly strong focus on accreditation and a large team of accreditors.

The Accreditor role is expected to be mandated in the Security Policy Framework, reference D in spring 2010.

# Accreditor Roles and Responsibilities

Accreditor role definitions are detailed below for the middle 3 levels of responsibility. The minimum recommended IISP skill levels are detailed in Table 1.

We recognise that organisations differ in their needs: not all Accreditor roles may be used, and some individuals may have other responsibilities in addition to their accreditation role. However, it is vital for organisations to consider the responsibilities placed on their Accreditor and ensure that staff can operate at the appropriate level. In small organisations there may only be a single qualified accreditor whose level of responsibility depends upon the degree of autonomy from any parent organisation or the size of the organisation and its governance structure. In many organisations, Lead Accreditors will also fill the role of Senior Accreditor.

## Accreditor

An Accreditor typically operates at a basic competency level in line with the IISP Level 2 “Basic application” definition. An Accreditor is responsible to a Senior Accreditor or the Lead Accreditor (where these roles are filled) and:

- Is able to make routine accreditation decisions, accepting residual risk on behalf of their organisation where it is clearly within the normal risk appetite
- Has some supervision
- Is able to escalate accreditation judgements that have implications beyond their level of responsibility and experience

From the description of the role of an Accreditor at reference A it is assumed that the Accreditor has “access to people who have a professional technical understanding of the technologies involved, to support the accreditation process” and therefore it is not essential that the Accreditor has knowledge of Vulnerability Testing. It is also assumed that Accreditation does not include conducting investigations or use of forensic techniques and therefore the Accreditor does not need these skills.

# Accreditor Roles and Responsibilities (Senior Accreditor)

A Senior Accreditor typically operates at an advanced competency level in line with the IISP Level 3 “Skilful application” definition, and is able to lead accreditation activity for the most complex or risky information systems, judging when to escalate accreditation decisions based on a good understanding of the normal or local risk appetite where different. A Senior Accreditor is responsible to the Lead Accreditor (where this role is filled).

A Senior Accreditor also contributes to improving the performance of the organisation’s accreditation function through activities such as:

- Coaching or supervising less experienced accreditors.
- Refining the organisation’s accreditation process.
- Assisting development of IA policy that affects accreditation
- Acting as the subject matter expert for some aspect of accreditation

# Accreditor Roles and Responsibilities (Lead Accreditor)

The Lead Accreditor also typically operates at an advanced competency level in line with the IISP Level 3 “Skilful application” definition, and takes responsibility for the accreditation process across the whole organisation complying with HMG IA Standards No 1 (reference E) and No 2 (reference A). The Lead Accreditor will normally be responsible to the SIRO.

In smaller organisations Lead Accreditors may also fill the role of Accreditor or Senior Accreditor. Typical activities undertaken by the Lead Accreditor include:

- Taking advice from the SIRO on the level of risk appetite and advising accreditors accordingly.
- Ensuring that accreditation decisions are escalated to appropriate levels in the organisation.
- Ensuring that accreditors are appropriately trained and supervised and are tasked at a level commensurate with their experience and competence.
- Managing the team of accreditors to ensure they collectively meet any service level agreed with the SIRO.
- Managing the recruitment and selection of accreditors.
- Ensuring that the accreditation team produces regular reports on their activities to enable managerial oversight.

# Minimum Recommended IISP Skill Levels

Table indicates the minimum recommended IISP skill levels for Accreditor, Senior Accreditor and Lead Accreditor.

- Level 1 = Awareness;
- Level 2 = Basic Application;
- Level 3 = Skilful Application;
- = Not applicable

**Table of Minimum Recommended IISP Skill Levels**

IISP Skill	Minimum Recommended IISP Skill Level		
	Accreditor	Senior Accreditor	Lead Accreditor
A1 – Governance	1	2	3
A2 – Policy & Standards	2	3	3
A3 – Information Security Strategy	2	2	3
A4 – Innovation & Business Improvement	2	2	3
A5 – Information Security Awareness and Training	1	1	1
A6 – Legal & Regulatory Environment	2	2	3
A7 – Third Party Management	1	1	2
B1 – Risk Assessment	2	3	3
B2 – Risk Management	2	3	3
C1 – Security Architecture	2	2	2
C2 – Secure Developme	2	2	2
D1 – Information Assurance Methodologies	2	2	2
D2 – Security Testing	2	2	2

## DRAFT

IISP Skill	Minimum Recommended IISP Skill Level		
	Accreditor	Senior Accreditor	Lead Accreditor
<b>E1 – Secure Operations Management</b>	1	1	2
<b>E2 – Secure Operations &amp; Service Delivery</b>	1	1	2
<b>E3 – Vulnerability Assessment</b>	-	-	-
<b>F1 – Incident Management</b>	-	-	-
<b>F2 – Investigation</b>	-	-	-
<b>F3 – Forensics</b>	-	-	-
G1 – Audit and & Review	2	2	2
H1 - Business Continuity Planning	1	1	2
H2 - Business Continuity Management	1	1	2
I1 – Research	-	-	-
I2 – Academic Research	-	-	-
I3 – Applied Research	-	-	-
J1 – Teamwork and Leadership	2	2	3
J2 – Delivering	2	2	2
J3 – Managing Customer Relationships	2	2	3
J4 – Corporate Behaviour	2	2	3
J5 – Change and Innovation	2	2	2
J6 – Analysis and Decision Making	2	3	3
J7 – Communication and Knowledge Sharing	2	2	3
K1 – Contributions to the Community	-	-	-
K2 – Professional Contributions	-	-	-
K3 – Professional Development	-	-	-

# Assessment Process

The process for assessing whether an individual meets the standard expected of either the Accreditor, Senior Accreditor or Lead Accreditor has yet to be decided in detail. It is intended that the process be consistent with that being developed for other roles in the IA discipline and be recognised by IA professional bodies as a means to providing evidence for meeting membership requirements.

In the meantime it is recommended that organisations using these role definitions follow the normal practices for demonstrating fitness for fulfilling a role:

- Request written evidence of experience and skills
- Request past line managers to confirm past responsibilities held
- Assess skills and competency at interview

It is recommended that formal assessment is undertaken when individuals are appointed to the role of Accreditor, Senior Accreditor or Lead Accreditor. To encourage professionalism, it is recommended that posts should be advertised nationally with selection panels including an independent member.

## Maintaining Competency

The standards for maintaining recognition of the Accreditor, Senior or Lead Accreditor status shall be aligned with the IISP-ITPC standards for Continuous Professional Development.

## Mobility of Accreditors

Adoption of these role definitions is intended to enable greater mobility of accreditors across the public sector and to help offer broader options for career development. This is desirable because smaller organisations may not be able to provide a full development path from Trainee Accreditor to Lead Accreditor, and large organisations may not be able to offer promotion to all accreditors who are capable of filling the Senior or Lead Accreditor roles. Greater mobility of accreditors between organisations can ease both these problems and offer career development opportunities. This framework is intended to provide a common lexicon which, coupled with the forthcoming IA professionalism framework, is intended to help job advertisers to recruit across the public sector.

DRAFT

[www.cesg.gov.uk](http://www.cesg.gov.uk)

CESG  
A2j  
Hubble Road  
Cheltenham  
Gloucestershire  
GL51 0EX  
Tel: +44 (0)1242 709141  
Fax: +44 (0)1242 709193  
Email: [enquiries@cesg.gsi.gov.uk](mailto:enquiries@cesg.gsi.gov.uk)

© Crown Copyright 2010.

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on 01242 221491 x30306 (non-sec) or email [infoleg@gchq.gsi.gov.uk](mailto:infoleg@gchq.gsi.gov.uk)

DRAFT