June 2013
Issue No: 3.0

CESG Certification for IA Professionals

CESG

NATIONAL TECHNICAL AUTHORITY
FOR INFORMATION ASSURANCE

CESG Certification for IA Professionals

Issue No: 3.0
June 2013

Document History

Issue	Date	Comment
1.0	March 2011	First definitive version
1.1	September 2012	Certification Bodies may, at their discretion, accept the Infosec Training Paths Competency scheme qualification as sufficient evidence for meeting the requirements of the Security & Information Risk Advisor role at responsibility level 2.
1.2	May 2012	Removal of FOIA footer throughout the document. Addition to both the role purpose and the responsibilities for both the Comsec Practitioner and the ComSO roles. Updates to reflect revised mapping of Mandatory Requirements (MR) in HMG SPF v7.0, October 11.
1.3	May 2012	Minor update to Table 7.
2.0	September 2012	Second definitive version. Removal of guidance chapters and their incorporation with CESG 'Awareness & Training' web pages. Removal of statements in Accreditor role definition requiring Senior & Lead Accreditors to meet responsibility requirements of Practitioner and Senior Accreditors respectively. Change of role title from Security Architect to IA Architect. Additional bullet point to the S&IRA Lead Practioner role: 'Leads development of IA training, guidance or professional standards in widespread use across the public sector'. Addition of knowledge statements to skill group definitions – see Annex A.
3.0	June 2013	Third definitive version. Incorporating HM Treasury GPG on role of internal audit in IA. Additional bullets to IA Senior & Lead Auditor roles Introduction of flexibility in core skills for IA Auditor role. Refinement to role definition headline statement for Lead S & IRA.

Purpose & Intended Readership

This document describes CESG's certification framework for Information Assurance (IA) Professionals. 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.

Parts of the framework may be relevant to IA Professionals working for the private sector. The framework contributes to Objective 4 of the UK Cyber Security Strategy (reference [a]), building the UK's cross cutting knowledge, skills and capability to underpin all cyber security objectives. This document is complemented by Guidance to CESG Certification for IA Professionals (reference [b]), which provides supporting information on the use and application of this framework.

Executive Summary

CESG has developed a framework for certifying IA Professionals who meet competency and skill requirements for specified IA roles. The purpose of certification is to enable better matching between public sector requirements for IA Professionals and the competencies of the staff or contractors undertaking common IA roles. 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]). 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
- Defines each of the IA roles at 3 levels
- Aligns each role level with responsibility levels defined by The Skills Framework for the Information Age (SFIA), (reference [d])[1]
- 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 [2] skill definitions to aid assessment against them

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

[1] The Skills Framework for the Information Age is owned by the SFIA Foundation: www.SFIA.org.uk

[2] 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.

    - IISP, RHUL & CREST consortium – www.iisp.org

- Assesses applicants against the requirements of the role definitions
- Includes the issue of certificates endorsed by CESG stating the IA role and responsibility level at which the applicant has been assessed as being competent to perform

IA Professionals working in, or for, the public sector are encouraged to apply for certification to demonstrate their competence in their IA role.

Contents:

THIS PAGE IS INTENTIONALLY LEFT BLANK

Accreditor Role Definition

Role Purpose

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 (reference [f])

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 (reference [f])
- To ensure the accreditation process meets the HMG Security Policy Framework (SPF) (reference [g]) and HMG IA Standards Nos 1 and 2 (IS1 & IS2) (reference [h])

Responsibilities

To achieve a particular responsibility level the candidate should meet the standard in the headline statement.

Accreditor – SFIA Responsibility Level 3

Headline statement

Makes routine accreditation decisions, accepting residual risk on behalf of their organisation where it is clearly within the normal risk appetite as declared by the Senior Information Risk Owner (SIRO)

Accreditors meeting the headline statement above will normally demonstrate all of the attributes below:

- Follows HMG SPF (reference [g]), IS1 & IS2 (reference [h]) and their local interpretations
- Reviews Risk Management Accreditation Document Sets (reference [h]) to confirm that risk assessments and risk treatment plans are consistent with business requirements
- Recognises accreditation decisions that have implications beyond their level of responsibility, experience or delegated risk tolerance and escalates them accordingly
- Builds constructive relationships with clients to build accreditation into business and project plans

- Is able to justify their accreditation decisions to stakeholders in terms of the business objectives, threats, risks, vulnerabilities, controls and likelihood of business impacts
- Provides constructive and timely advice to system developers on whether proposed solutions are likely to gain accreditation
- Understands the normal risk appetite and the potential business impact of accepting risks either above or below it

Senior Accreditor - SFIA Responsibility Level 4

Headline statement

Leads accreditation decision making for complex or risky information systems

Is capable[3] of undertaking the role of Accreditor, meets the headline statement above and performs the majority of the activities below:

- Accredits information systems which require risk mitigation measures in addition to the default measures applied across the organisation or domain
- Manages, coaches or supervises less experienced accreditors
- Contributes to development of the organisation's accreditation process
- Contributes to the development of IA policy that affects accreditation
- Acts as the subject matter expert for some aspect of accreditation

Lead Accreditor – SFIA Responsibility Level 6

Headline statement

Ensures that the accreditation process across the SIRO's area of responsibility is driven by business objectives and complies with HMG IA Standards

Is capable of undertaking the role of Senior Accreditor, meets the headline statement above and performs the majority of the activities below:

- Influences the SIRO on the level of risk appetite and advises accreditors accordingly
- Initiates changes to Accreditation Policies to balance accreditation resources with business objectives
- Influences Information Asset Owners and other stakeholders to support accreditation processes

[3] Subject to allowances for familiarisation with the local practicalities of the role.

- Ensures that accreditors are appropriately trained and supervised and are tasked at a level commensurate with their experience and competence
- Manages the team of accreditors to ensure they collectively meet any service level or Accreditation Policy agreed with the SIRO
- Manages the recruitment and selection of accreditors
- Ensures that the accreditation team produces regular reports on their activities to enable SIRO and managerial oversight

Table of Indicative IISP Skill Levels

Core skill: A6, B1, B2, D1	Indicative IISP Skill Level		
IISP Skill	**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 – IS Awareness and Training	1	1	1
A6 – Legal & Regulatory Environment	**2**	**2**	**3**
A7 – Third Party Management[4]	1	1	2
B1 – Risk Assessment	**2**	**3**	**3**
B2 – Risk Management	**2**	**3**	**3**
C1 – Security Architecture	2	2	2
C2 – Secure Development	1	1	1
D1 – IA Methodologies	**2**	**2**	**3**
D2 – Security Testing	2	2	2
E1 – Secure Operations Management	1	1	2
E2 – Secure Ops & Service Delivery	1	1	2
E3 – Vulnerability Assessment	1	2	2
F1 – Incident Management	1	2	2
F2 – Investigation	1	1	1
F3 – Forensics	1	1	1
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	-	-	-

[4] Skill only required if information systems or services are provided by a third party

IA Auditor Role Definition

Role Purpose

The following activities are within the scope of the role:

- To assess an organisation's compliance with security objectives, policies, standards and processes in accordance with HM Treasury: Good Practice Guide; The internal audit role in information assurance; https://www.gov.uk/government/publications/public-sector-internal-audit-standards-good-practice-guidance
- To provide impartial assessment and reports covering security investigations, information risk management and investment decisions to improve an organisation's information risk management
- To provide an independent opinion on whether IA control objectives are being met within an organisation
- To identify an organisation's systemic trends and weaknesses in security
- To recommend responses to audit findings

Responsibilities

To achieve a particular responsibility level the candidate should meet the standard in the headline statement. The supporting bullet points provide examples of activities, behaviours or responsibility consistent with the standard. Other examples may also meet the standard.

IA Auditor – SFIA Level 2

Headline statement

Undertakes assigned routine or ad hoc audits to test compliance with IA policies or standards

- Tests compliance with local security policies and procedures, Codes of Connection or security requirements mandated in the Security Policy Framework (SPF) (reference [g])
- Meets the HM Treasury Code of Ethics for Internal Auditors detailed in Public Sector Internal Audit Standards, June 2013; https://www.gov.uk/government/publications/public-sector-internal-audit-standards
- Assists with the development of audit plans
- Works under the supervision of a Senior or Lead Auditor

IA Senior Auditor - SFIA Responsibility Level 4

Headline statement

Leads audit activity to meet complex audit objectives and takes responsibility for the audit findings

- Leads audits assessing compliance with IA policies or standards across an organisation or business unit; e.g. IA maturity assessments, compliance with ISO 27001 or departmental standards
- Identifies opportunities for greater business benefits through improvements to detective controls
- Provides supervision and guidance to IA auditors they are assigned to lead and takes responsibility for their audit findings
- Develops audit plans to meet audit objectives and takes responsibility for their delivery
- Leads audits to assess the management of information risk across the organisation or business unit
- Reports and justifies audit findings to clients with minimal supervision
- For auditors in the third line of defence[5], reviews the effectiveness of information risk management

IA Lead Auditor – SFIA Responsibility Level 6

Headline statement

Proposes and delivers information risk driven audit programmes to senior information risk owners or an IA Board

Is responsible, and accountable to a Senior Information Risk Owner or an IA Board, for the operation, delivery and quality of the IA audit function across the SIRO's area of responsibility

- Audit findings influence SIRO plans for managing information risk
- Sets standards for training and performance of subordinate IA auditors and takes responsibility for their performance and development as IA Auditors
- Objectively assesses the maturity of an existing information auditing function using cross-government benchmark standards for auditing

[5] As defined in HMT Good Practice Guide; The internal audit role in information assurance

- Adds value by recommending efficiencies and cost-effective options to address the non-compliance issues and information assurance gaps that have been identified during the audit process
- Develops audit regimes to enable greater business flexibility at an acceptable risk level

Table of Indicative IISP Skill Levels

Due to the breadth of work undertaken in this role, 6 core skills are identified. All IA Auditors are required to meet skill G1 and 3 of the remaining 5 core skills.

Core skills: A1, A2, A6, D1, F2, G1	Indicative IISP Skill Level		
IISP Skill	**Auditor**	**Senior Auditor**	**Lead Auditor**
A1 – Governance	2	3	3
A2 – Policy & Standards	2	2	3
A3 – Information Security Strategy	2	2	3
A4 – Innovation & Business Improvement	2	2	3
A5 – IS Awareness and Training	1	1	1
A6 – Legal & Regulatory Environment	**2**	**2**	**3**
A7 – Third Party Management[7]	1	2	3
B1 – Risk Assessment	2	3	3
B2 – Risk Management	2	2	2
C1 – Security Architecture	1	2	2
C2 – Secure Development	1	1	1
D1 – IA Methodologies	**2**	**2**	**3**
D2 – Security Testing	1	2	2
E1 – Secure Operations Management	1	2	2
E2 – Secure Ops & Service Delivery	1	1	2
E3 – Vulnerability Assessment	1	1	1
F1 – Incident Management	1	2	2
F2 – Investigation	**1**	**2**	**3**
F3 – Forensics	1	2	2
G1 – Audit and Review	**2**	**3**	**3**
H1 – Business Continuity Planning	1	2	2
H2 – Business Continuity Management	1	1	1
I1 – Research	-	-	-
I2 – Academic Research	-	-	-
I3 – Applied Research	-	-	-

[7] Skill only required if information systems or services are provided by a third party.

IA Architect Role Definition

Role Purpose

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

Responsibilities

To achieve a particular responsibility level the candidate should meet the standard in the headline statement. The supporting bullet points provide examples of activities, behaviours or responsibility consistent with the standard. Other examples may also meet the standard.

IA Architect – SFIA Responsibility Level 2

Headline statement

Represents security requirements in the design and implementation of IS architectures

Is responsible to a Senior Security Architect to:

- Understand the business environment and the information risks that systems of interest are subject to
- Assist Senior Security Architects identify information risks that arise from potential solution architectures
- Propose alternate architectures or countermeasures to mitigate risks from initial solution architectures
- Assists with the secure configuration of ICT systems in compliance with the intended architecture

Senior IA Architect – SFIA Responsibility Level 4

Headline statement

Enables the design and implementation of secure[8] IS architectures

Is responsible to a Lead Security Architect for all the responsibilities of a Security Architect plus:

- Identifies information risks that arise from potential solution architectures
- Designs alternate solutions to mitigate identified information risks
- Ensures that alternate solutions or countermeasures mitigate identified information risks
- Applies 'standard' security techniques and architectures to mitigate security risks.
- Develops new architectures that mitigate the risks posed by new technologies and business practices
- Provides consultancy and advice to customers on IA and architectural problems
- Supervises Security Architects reporting to them

Lead IA Architect – SFIA Responsibility Level 6

Headline statement

Influences the security of enterprise or solution architectures across the public sector or across the whole of a public sector organisation

Is typically responsible to an Enterprise Architect, Chief Information Officer, Chief Technology Officer, Departmental Security Officer or SIRO for all the responsibilities of a Senior IA Architect and:

- Initiates development of new security architectures to mitigate emerging information risks
- Influences senior stakeholders to comply with architectural principles and objectives
- Presents the business case to directors for strategic security investment in enterprise or solution architectures
- Establishes training programmes for security architects

[8] In this context 'secure' means that when subsequently tested by a CHECK penetration test, no unexpected vulnerabilities are found that require design changes.

- Mentors, supervises or takes responsibility for the work of less experienced security architects
- Influences security architecture practices in widespread use across the public sector

Table of Indicative IISP Skill Levels

Core skills: A4, C1, C2, D1	Indicative IISP Skill Levels		
IISP Skill	**IA Architect**	**Senior IA Architect**	**Lead IA Architect**
A1 – Governance	1	2	3
A2 – Policy & Standards	2	3	3
A3 – Information Security Strategy	1	2	2
A4 – Innovation & Business Improvement	**1**	**2**	**3**
A5 – Information Security Awareness and Training	1	1	2
A6 – Legal & Regulatory Environment	1	2	2
A7 – Third Party Management[9]	1	1	2
B1 – Risk Assessment	2	3	3
B2 – Risk Management	2	3	3
C1 – Security Architecture	**2**	**3**	**3**
C2 – Secure Development	**1**	**1**	**2**
D1 – Information Assurance Methodologies	**1**	**2**	**2**
D2 – Security Testing	1	2	2
E1 – Secure Operations Management	1	2	2
E2 – Secure Operations & Service Delivery	1	1	2
E3 – Vulnerability Assessment	1	2	2
F1 – Incident Management	1	2	2
F2 – Investigation	1	1	2
F3 – Forensics	1	1	1
G1 – Audit and Review	1	1	2
H1 – Business Continuity Planning	1	1	2
H2 – Business Continuity Management	1	1	2
I1 – Research	1	1	1
I2 – Academic Research	-	1	1
I3 – Applied Research	-	1	2

SFIA defines IT skills, some of which are relevant to the IA Architect role. The table below shows the relevant skills and the indicative SFIA level for IA Architect, Senior IA Architect and Lead IA Architect. Where the skill is not defined at a SFIA level applicable to IA Architect or Senior IA Architect, the table cell is marked as 'Undefined'.

[9] Skill only required if information systems or services are provided by a third party

SFIA Skill	Indicative SFIA Level		
http://www.sfia.org.uk/cgi-bin/4gdocs.pl/sfia4G.xls	**IA Architect**	**Senior IA Architect**	**Lead IA Architect**
STPL – Enterprise Architecture	Undefined	Undefined	5
ARCH – Solution Architecture	Undefined	Undefined	5
EMRG – Emerging Technology Monitoring	Undefined	Undefined	5
BSMO – Business Modelling	2	3	4
REQM – Requirements definition and Management	2	3	4
DESN – Systems Design	2	4	5
NTDS – Network Design	Undefined	Undefined	5

THIS PAGE IS INTENTIONALLY LEFT BLANK

Security & Information Risk Advisor Role Definition

Role Purpose

To provide business driven advice on the management of security and information risk consistent with HMG IA policy, standards and guidance:

- To provide a focal point for resolution of security and information risk matters
- To identify, analyse and evaluate information risks
- To explain to risk owners and other stakeholders the causes, likelihood and potential business impacts of information risks throughout the information system lifecycle
- To assist checking compliance with applicable regulations, standards, policies and guidance on information risk management
- To present options for treating or transferring information risks
- To support the development of Risk Management Accreditation Document Sets (RMADS) in accordance with IS1 & IS2 (reference [h])
- To investigate security incidents
- To promote security awareness

Responsibilities

To achieve a particular responsibility level the candidate should meet the standard in the headline statement. The supporting bullet points provide examples of activities, behaviours or responsibility consistent with the standard. Other examples may also meet the standard.

Security and Information Risk Advisor – SFIA Responsibility Level 2

Headline statement

Assists customers in the routine application and interpretation of security or IA policies and practices

- Uses prescribed risk assessment technique to identify emerging information risks early in the development cycle of assigned new information systems
- Co-ordinates the identification of suitable risk treatment using standard IA controls where appropriate
- Authors security documents to demonstrate compliance with applicable policies and standards; e.g. RMADS

- Liaises with an accreditor to gain timely accreditation
- Undertakes preliminary or fact finding enquiries into security incidents
- Checks or reports compliance with applicable security standards and procedures
- Presents security briefings to users or local management
- Contributes to security communications
- Drafts requirements for IT Health Checks and assists in remediating findings

Senior Security and Information Risk Advisor – SFIA Responsibility Level 4

Headline statement

Enables provision of the Security and Information Risk Advisor service across a range of business units, sites, projects or other change activities

- Selects appropriate risk assessment techniques for use across the client programme
- Identifies information risks which are systemic across the programme
- Recommends implementation of new IA controls across the programme or enterprise to provide more cost effective risk mitigation in the long term
- Contributes to the development of IA strategies, policies, guidance and awareness
- Integrates information risk management into programme risk management
- Manages security incidents escalated from a Security and Information Risk Advisor in accordance with applicable policies and standards
- Provides specialist information security advice requiring at least one IISP skill at skill level 3
- Plans and manages delivery of a security work programme
- Manages or supervises Security & Information Risk Advisors

Lead Security and Information Risk Advisor – SFIA Responsibility Level 6

Headline statement

Influences[10] management of security and information risk across a large[11] organisation or across multiple client organisations

Ensures provision of the Security and Information Risk Advisor service across the organisation

- Integrates information risk management into enterprise risk management
- Influences the SIRO and other senior stakeholders on business driven information risk management strategies, policies and practices
- Initiates the development of new IA controls or policies
- Leads the development of organisation wide information risk assessment techniques, reporting frameworks or processes
- Ensures consistent delivery of security training across the organisation
- Ensures compliance with applicable security and IA standards and policies is monitored across the organisation
- Leads development of IA training, guidance or professional standards in widespread use across the public sector
- Ensures effective management of security incidents
- Manages or supervises Senior Security and Information Risk Advisors

[10] By influencing across an organisation we mean influencing policies or controls that by default are applicable throughout the organisation.

[11] By 'large' we mean typically more than 1,000 employees and requiring a S&IRA service well beyond the remit of a senior practitioner operating at SFIA level 4.

Due to the breadth of work undertaken in this role, 8 core skills are identified. Security and Information Risk Advisors are required to meet the skill requirements for any 4 of these, Senior S & IR Advisors meet the requirements for any 5 and Lead S and IR Advisors to meet the requirements for any 6.

Table of Indicative IISP Skill Levels

Core Skills: A2, A3, A4, A6, B1, B2, F1, F2	Indicative IISP Skill Level		
IISP Skill	**S & IR Advisor**	**Senior S & IR Advisor**	**Lead S & IR Advisor**
A1 – Governance	1	2	3
A2 – Policy & Standards	**2**	**3**	**3**
A3 – Information Security Strategy	**1**	**2**	**3**
A4 – Innovation & Business Improvement	**1**	**2**	**3**
A5 – IS Awareness and Training	1	1	2
A6 – Legal & Regulatory Environment	**1**	**2**	**2**
A7 – Third Party Management[12]	1	1	2
B1 – Risk Assessment	**2**	**3**	**3**
B2 – Risk Management	**2**	**3**	**3**
C1 – Security Architecture	1	2	3
C2 – Secure Development	1	1	2
D1 – IA Methodologies	1	2	3
D2 – Security Testing	1	2	2
E1 – Secure Operations Management	1	2	2
E2 – Secure Ops & Service Delivery	1	1	2
E3 – Vulnerability Assessment	1	2	2
F1 – Incident Management	**2**	**3**	**3**
F2 – Investigation	**2**	**2**	**2**
F3 – Forensics	1	1	1
G1 – Audit and Review	1	1	2
H1 – Business Continuity Planning	1	1	2
H2 – Business Continuity Management	1	1	2
I1 – Research	1	1	1
I2 – Academic Research	-	1	1
I3 – Applied Research	-	1	1

[12] Skill only required if information systems or services are provided by a third party.

IT Security Officer Family of Roles

Role Purpose

Provides governance, management and control of IT security.

Responsibilities

To achieve a particular responsibility level the candidate should meet the standard in the headline statement. The supporting bullet points provide examples of activities, behaviours or responsibility consistent with the standard. Other examples may also meet the standard.

Information System Security Officer (ISSO) – SFIA Responsibility Level 2

Responsible to an ISSM or ITSO

Headline statement

Assists implementation of effective IT security in accordance with local policy

- Contributes to development of Security Operating Procedures (SyOPs) for new IT systems
- Review requests for change; rejecting or escalating requests that breach SyOPs
- Provides advice on compliance with IT security policy and procedures
- Alerts the accreditor to changes in system use that might affect the level of residual risk
- Reviews the effectiveness of IT security controls in accordance with accreditation conditions and corporate security policies
- Reports security incidents or breaches of security policy in accordance with local procedures
- Assists investigations into IT security incidents

Information System Security Manager (ISSM) – SFIA Responsibility Level 4

Responsible to the ITSO

Headline statement

Enables effective IT security across a wide portfolio of IS

- Manages a team of ISSOs
- Develops terms of reference for ISSOs
- Identifies and reports systemic weaknesses in control effectiveness

- Specifies requirements for IT Health Checks to ensure identification of vulnerabilities and testing of IT security controls, and to protect other IT systems
- Reports security incidents or breaches of security policy in accordance with local procedures and guidance from GovCertUK (www.govcertuk.gov.uk) or local Warning, Advice and Reporting Point (WARP) (reference [i])
- Assesses the significance of security advice from WARPs or other sources to own area of responsibility and makes appropriate recommendations
- Chairs IT system security working groups
- Represents IT security on Change Advisory Board
- Manages compliance in area of responsibility with organisational commitments to codes of connection with partners
- Contributes to development of IT security policy
- Leads investigations into IT security incidents

IT Security Officer – SFIA Responsibility Level 6

Responsible to the DSO and/or SIRO for the security of information in electronic form (HMG Security Policy Framework (reference [g]), Mandatory Requirement 1)

Headline statement

Influences corporate IT security

- Agrees with the DSO and SIRO the IT security policy for their area of responsibility
- Ensures that IT security policy is updated as IT security threats evolve
- Defines target end state for IT security controls in IT systems across the DSO's area of responsibility
- Reports the effectiveness of IT security controls to the DSO
- Advises stakeholders on compliance with IT security policy and controls
- Contributes to IT service level definitions
- Promotes a security aware culture
- Contributes to IA maturity assessments for the organisation
- Supports the IA programme manager in developing the business case for investment to improve IT security controls
- Initiates investigations into IT security incidents in accordance with their organisation's forensic readiness policy.

- Factors lessons learnt from security incidents into IT security policies and processes
- Maintains the organisation's relationship with GovCertUK or local WARP; ensures that IT security incidents are reported where appropriate and ensures that GovCertUK warnings and advisory notices are acted upon within their organisation
- Ensures compliance with organisational commitments to codes of connection with partner organisations
- Manages relationships with key stakeholder groups such as users, project managers, IT service providers, Information Asset Owners, enterprise architects and procurement staff to gain compliance with policy
- Ensures the maintenance of information risks on corporate risk register

Table of Indicative IISP Skill Levels

Core skills: A6, E1, E2, E3, F1	Indicative IISP Skill Level		
IISP Skill	**ISSO**	**ISSM**	**ITSO**
A1 – Governance	2	2	3
A2 – Policy & Standards	2	2	3
A3 – Information Security Strategy	1	2	3
A4 – Innovation & Business Improvement	2	2	3
A5 – IS Awareness and Training	1	2	2
A6 – Legal & Regulatory Environment	**2**	**2**	**3**
A7 – Third Party Management	1	2	2
B1 – Risk Assessment	1	2	2
B2 – Risk Management	1	2	3
C1 – Security Architecture	1	2	2
C2 – Secure Development	1	1	2
D1 – IA Methodologies	1	2	2
D2 – Security Testing	1	2	2
E1 – Secure Operations Management	**1**	**2**	**3**
E2 – Secure Ops & Service Delivery	**2**	**3**	**3**
E3 – Vulnerability Assessment	**1**	**2**	**3**
F1 – Incident Management	**1**	**2**	**2**
F2 – Investigation	1	2	2
F3 – Forensics	1	2	2
G1 – Audit and Review	1	2	2
H1 – Business Continuity Planning	1	2	2
H2 – Business Continuity Management	1	2	2
I1 – Research	-	-	1
I2 – Academic Research	-	-	1
I3 – Applied Research	-	-	1

Communications Security Family of Roles

Role Purpose

To manage cryptographic systems as detailed in HMG IA Standard No 4 (IS4), Management of Cryptographic Systems (reference [j]), and in relevant product specific security procedures.

Electro-magnetic security is outside the scope of this role.

Responsibilities

To achieve a particular responsibility level the candidate should meet the standard in the headline statement. The supporting bullet points provide examples of activities, behaviours or responsibility consistent with the standard. Other examples may also meet the standard.

Comsec Practitioner – SFIA Responsibility Level 2

Is responsible to a Comsec Manager or Communications Security Officer (ComSO)

Headline statement

Assists in the implementation of Comsec policy or monitoring compliance with it

- Fills the role of Comsec Inspector, Controlling Authority, Cryptonet Controller, Closed User Group Controller, Custodian or deputy/alternate custodian as detailed in IS4 Supplement 1, Roles and Responsibilities (reference [k]) including undertaking any mandatory training courses
- Performs routine Comsec duties
- Contributes to development of local Comsec procedures
- Recognises breaches of Comsec policy and reports accordingly to the Comsec Incident Notification, Reporting and Alerting Scheme (CINRAS)
- Manages organisation's holdings of cryptographic systems and key materials in accordance with IS4 (reference [j]) Similarly, manages allocation of these materials to sub accounts coordinating approval/order/receipt/despatch and final return and /or destruction of key material and cryptographic systems
- Performs internal musters and check of holdings

Comsec Manager – SFIA Responsibility Level 4

Is responsible to the ComSO

Headline statement

Manages compliance with Comsec policy

- Manages Comsec Practitioners
- Produces local Comsec procedures
- Manages configuration control for cryptographic equipment
- Reports Comsec incidents to the ComSO
- Manages local Comsec training and awareness

ComSO – SFIA Responsibility Level 5

Is responsible to the DSO

Headline statement

Ensures compliance with IS4 across the DSO's area of responsibility

- Ensures that the Comsec functions described in IS4 (reference [j]) are fulfilled
- Ensures that the organisation is audited annually for compliance with IS4 (reference [j])
- Leads development and implementation of local Comsec policy
- Leads development and promulgation of communications and cryptographic security education, training and awareness across the organisation
- Represents cryptographic system security on internal and interdepartmental security committees
- Manages cryptographic system related security investigations and reporting of incidents in conjunction with the DSO to CINRAS
- Provides strategic level cryptographic system security advice
- Responsible for performing annual internal audit of organisation's compliance against IS4 (reference [j])

Table of Indicative IISP Skill Levels

Core skills: A6, E1, E2, F1	Indicative IISP Skill Level		
IISP Skill	**Comsec Practitioner**	**Comsec Manager**	**ComSO**
A1 – Governance	1	2	3
A2 – Policy & Standards	2	2	3
A3 – Information Security Strategy	1	2	3
A4 – Innovation & Business Improvement	1	1	2
A5 – IS Awareness and Training	1	2	2
A6 – Legal & Regulatory Environment	**2**	**2**	**2**
A7 – Third Party Management	1	2	2
B1 – Risk Assessment	1	2	2
B2 – Risk Management	1	2	3
C1 – Security Architecture	1	1	2
C2 – Secure Development	1	1	2
D1 – IA Methodologies	1	2	2
D2 – Security Testing	1	2	2
E1 – Secure Operations Management	**1**	**2**	**3**
E2 – Secure Ops & Service Delivery	**2**	**3**	**3**
E3 – Vulnerability Assessment	1	2	3
F1 – Incident Management	**1**	**2**	**2**
F2 – Investigation	1	2	2
F3 – Forensics	1	2	2
G1 – Audit and Review	1	2	2
H1 – Business Continuity Planning	1	2	2
H2 – Business Continuity Management	1	2	2
I1 – Research	-	-	1
I2 – Academic Research	-	-	1
I3 – Applied Research	-	-	1

THIS PAGE IS INTENTIONALLY LEFT BLANK

Annex A - Skill Definitions

Skill Section A – Information Security Management

IISP Principle

Capable of determining, establishing and maintaining appropriate governance of (including processes, roles, awareness strategies, legal environment and responsibilities), delivery of (including policies, standards and guidelines), and cost-effective solutions for (including impact of third parties) information security within a given organisation.

Knowledge Requirements

Information Security Management skills are based upon knowledge, understanding and proficiency in key specialisms such as, but not necessarily limited to, the following:

- Management frameworks directly relevant to information security such as ISO 27000 series – Information Security Management Systems. For the public sector these also include:
  - HMG Security Policy Framework (reference [g])
  - HMG IA Maturity Model and Assessment Framework (reference [l])
- Legislation directly relevant to information security including:
  - Data Protection Act
  - Computer Misuse Act
  - Freedom of Information Act
- Common management frameworks that support the governance, delivery and cost-effectiveness of information security such as:
  - ISO 9000
  - PRINCE2
  - Managing Successful Programmes
  - IT Infrastructure Library
  - Investors in People

A1 - Governance

IISP Example Skills

- Establishing frameworks to develop and maintain appropriate information security expertise within an organisation

- Gaining management commitment and resources to support the governance structure
- Incorporating physical, personnel and procedural issues into the overall security governance process
- Relating an organisation's business needs to their requirements for information security
- Encouraging an information risk awareness culture within an organisation. For example, raising awareness of how the various forms of social engineering can be used to compromise information
- Establishing frameworks for maintaining the security of information throughout its lifecycle

CESG Supplementation

Skill Level 1: Understands local arrangements for Information Governance (IG)

- Shall be able to explain their understanding of the term 'Information Governance'
- Is aware of the IG regime in own organisation including aspects such as:
  - the key IG bodies and their membership in their own organisation
  - the applicability of IG processes and standards to their own work
- For those working in the public sector: is aware of the HMG Security Policy Framework (reference [g]) and the Mandatory Requirements relevant to their own work
- Understands the potential business impact of inadequate Information Governance

Skill Level 2: Applies IG standards or processes to local area and to clients beyond it

- Shall be able to describe how information is governed in at least one organisation
- Is able to apply IG standards or processes beyond immediate work area, e.g.
  - Recording of information assets
  - Application of IA controls
  - Escalation of accreditation decisions to management
- Recognises non-compliance with IG standards in own area of responsibility and responds appropriately

- For those working in the public sector: is aware of the HMG IA Maturity Model (IAMM) and the Assessment Framework and their applicability to their own work
- Raises awareness in local area of IG
- Can offer suggestions for improvement to local practices to improve compliance with the IG regime
- Has received some training relevant to IG eg. ISO 27001 course, ISACA Certified Information Security Manager or Certified in the Governance of Enterprise IT. For those working in the public sector: IAO training course, accreditation modules

Skill Level 3 – Develops IG standards or processes; applies IG principles across the organisation

- Shall be able to describe and contrast different styles of IG
- Regularly applies IG standards or processes beyond the local business area
- Is able to apply IG standards or processes in complex cases without supervision. Shows good judgement on when to escalate IG issues to seniors
- Influences corporate resourcing of IG
- Interprets IG principles or policies for other business units, developing practical guidance tailored to their needs
- Takes responsibility for improving aspects of IG in response to internal or external audits
- Makes IG decisions that set organisational precedents

Skill Level 4 – Leads development of IG at the organisation level or has influence at national or international standards level

- Initiates changes to IG frameworks at departmental or national level
- Authors guidance on the application of IG principles at departmental or national level
- Provides guidance on IG across their own organisation
- Influences government, industry sector or public IG standards

A2 – Policy and Standards

IISP Example Skills

- Developing and maintaining organisational security policies, standards and processes using recognised standards (such as the ISO 27000 family) where appropriate
- Developing and maintaining standards for appropriate personnel screening
- Developing and maintaining standards for appropriate physical storage of information
- Providing advice on the interpretation of policy
- Undertaking a gap analysis against relevant external policies, standards and guidelines, and initiating remedial action where appropriate

CESG Supplementation

Skill Level 1: Understands the need for policy and standards to achieve Information Security (IS)

- Shall be able to list major sources of applicable IS policies and standards. For the public sector this shall include the HMG Security Policy Framework (reference [g]), the CESG Policy Portfolio and departmental IS policies and standards
- Updates local policies to reflect changes in policies from higher authorities
- Understands local requirements for consultation, review and approval of policies and standards

Skill Level 2: With supervision and aligned with business objectives, authors or provides advice on IS policy or standards

- Shall be able to describe at least one IS policy or standard in detail and justify its content
- Develops new policies and standards in response to authorised tasks
- Is aware of, and takes into account, relevant business objectives when formulating policy and standards. In the public sector this will include departmental strategic objectives, public service agreements and the HMG Security Policy Framework (reference [g])
- Writing is clear, succinct, unambiguous and in a language appropriate to the intended reader
- Incorporates review comments effectively

- Complies with local processes for consultation, review and approval
- Answers questions on policies and standards that they have authored
- Provides advice on the interpretation of IS policy or standards

Skill Level 3: Without supervision, advances business objectives through development or interpretation of a range of IS policies or standards

- Can describe and contrast various approaches to IS policy or standard development
- Initiates development of new policies and standards in own organisation
- Is capable of co-ordinating development of effective policies and standards in information security fields with which they are not previously expert
- Contributes to development of national or international policies or standards
- Supervises other policy developers
- Advances local practices for policy and standard development
- Incorporates recent advances in information security into existing policies and standards
- Co-ordinates policy and standard development on behalf of an organisation
- Interprets IS policy or standards to support important or complex decisions or decisions that set new precedents
- Expresses findings from penetration testing as non-compliances with applicable policy and guidance

Skill Level 4: A recognised expert in IS policy and standard development

- Leads development of policy of standards in emerging IS issues or to provide national direction
- Advances the practice of policy or standard development
- Is recognised as a thought leader by peers in the field
- Chairs ISO working committees

A3 – Information Security Strategy

IISP Example Skills

- Balancing cost against security risk for the business
- Interpreting external requirements and standards in terms relevant to an organisation
- Balancing technical, physical, personnel and procedural controls to address information risks in the most effective way

CESG Supplementation

Skill Level 1 – Understands the purpose of IS strategy to realise business benefits

- Is aware of the IS strategy of at least one organisation
- Applies local IS strategy to own work
- Understands how IS can support or hinder business objectives

Skill Level 2 – Contributes to development or implementation of IS strategy under supervision

- Shall be able to describe the IS strategy of at least one organisation and how it contributes to business benefits
- Can describe factors to be taken into account during IS strategy development
- Participates in IS strategy development workshops
- Drafts or reviews components of IS strategy
- Implements components of IS strategy

Skill Level 3 – Influences investment decisions or risk appetites through contribution to development or implementation of IS strategy

- Shall be able to describe and contrast alternative IS strategies for realising business benefits
- Can describe techniques to gain adoption of IS strategy
- Develops or refines corporate IS strategy to deliver business benefits
- Influences corporate strategies to reflect the needs of IS
- Leads workshops or teams to develop IS strategy

- Achieves consensus among key stakeholders
- Drives business change to implement IS strategy

Skill Level 4 – A recognised expert in IS strategy development or implementation

- Shall have developed or implemented an IS strategy that gave business advantage or made new markets accessible
- Is consulted by directors and senior business managers. In the public sector this includes the CIO, CTO, SIRO, DSO, ITSO and IAOs
- Authorises corporate IS strategy
- Leads development of corporate IS strategy
- Is able to co-ordinate many factors in the development of new strategy and gain widespread support for the strategy
- Advances the practice of developing and implementing IS strategy

A4 – Innovation and Business Improvement

IISP Example Skills

- Recognises potential strategic application of information security and initiates investigation and development of innovative methods of protecting information assets, to the benefit of the organisation and the interface between business and information security
- Exploits opportunities for introducing more effective secure business and operational processes

CESG Supplementation

Skill Level 1 – Is aware of the business benefits of good IS

- Shall be able to explain that the ultimate purpose of IS is to enhance business prospects in the long term through reduced information risk, reduced costs or enabling value adding capabilities that would otherwise exceed the risk appetite or risk tolerance
- Understands the potential impacts in their own business of poor IS
- Is aware of the constraints that IS policies place upon their own business
- Produces data to enable others to make business improvements; e.g protective monitoring, IT Health Checks, audits of IS controls

Skill Level 2 – Applies IS to achieve business objectives with some supervision

- Shall be able to describe how IS improved an organisation's ability to meet business objectives
- With some supervision, provides IS advice on the design, implementation, configuration or operation of information systems to balance IS with business objectives
- Identifies opportunities for IS to enable business improvement in their own area
- Identifies opportunities for cost-effective IS improvements in information systems or services
- Pro-actively finds data that changes perceptions on information risk or the effectiveness of IS controls
- Monitors developments in IS tools or technologies and makes recommendations on those that are most applicable to their business unit, organisation or client

Skill Level 3 – Supports realisation of strategic business benefits through innovative application of IS

- Shall be able to describe how they conceived and delivered a business improvement through application of IS; e.g. reduced cost or risk, greater business agility
- Identifies opportunities for IS to enable strategic business benefits
- Is able to persuade senior stakeholders to invest in IS to make business benefits; e.g. improved IS controls to enable consolidation of IT infrastructure
- Is able to resolve challenging conflicts between security and other business objectives; e.g. balancing need to know with need to share
- Applies deep knowledge of IS and business activities to identify information risks of concern at board level; e.g. specific increased threat that could exploit vulnerabilities causing high business impact
- Appraises senior managers and directors of the IS implications of strategic business objectives; e.g. risks of information sharing with new partners, increased use of on-line services, increased remote working
- Influences the implementation of IS in Enterprise Architectures

Skill Level 4 – Develops and promotes new concepts for business improvement through IS which are widely adopted across the public sector or an industry sector

- Develops guidance on the application of IS to deliver business benefits that is used across the public or industry sectors
- Influences IS professional development to ensure IS enables as well as protects businesses
- Identifies the IS implications of government or regulator policies and strategies and takes actions to influence public or industry sector IS policy, standards or guidance accordingly
- Is sought for key note speeches at IS conferences

A5 – Information Security Awareness and Training

IISP Example Skills

- Identifying security awareness and training needs in line with security strategy, business needs and strategic direction
- Gaining management commitment and resources to support awareness and training in information security
- Identifying the education and delivery mechanisms needed to grow staff in information security awareness and competence
- Managing the development or delivery of information security awareness and training programmes

CESG Supplementation

Skill Level 1: Understands the role of security awareness and training in maintaining Information Security

- Shall be able to give examples of risks to information caused by poor security awareness
- Can describe a variety of methods for improving security awareness
- Can describe security weaknesses in security practices in own area
- Can describe the business benefits to own area of good security awareness
- Is aware of policy and standards relevant to security awareness and training; for the public sector this includes HMG Security Policy Framework (reference [g]) Mandatory Requirements 6 and 10.

Skill Level 2: Materially contributes to improving security awareness with some supervision

- Presents effective training sessions on IS awareness
- Materially contributes to the content of security awareness initiatives
- Understands the information security aspects of the material they promote
- Adapts the style of delivery to the IS awareness needs of the audience

Skill Level 3: Delivers, or manages the delivery of training on multiple aspects of IS

- Develops or delivers effective information security training courses based on up to date IS knowledge
- Identifies gaps in organisational security awareness
- Designs or modifies awareness programmes to meet organisational needs
- Initiates new ways for enhancing IS awareness
- Persuades management of the need to resource IS awareness and training

Skill Level 4: A recognised authority on the development of IS Awareness and Training

- Drives cultural change enabling strategic business objectives through the design and implementation of organisational IS awareness programmes
- Establishes career development frameworks to maximise staff potential
- Influences professional bodies to incorporate IS within their training programmes
- Develops training standards for IS trainers
- Authors articles, papers or books on IS that are published following peer review

A6 – Legal and Regulatory Environment

IISP Example Skills

- Familiar with legal and regulatory requirements that could affect organisation security policies, and where to turn for specific detail as needed
- Relating the legal and regulatory environment within which the business operates to the risk management and security strategy tasks
- Ensuring security policies comply with all personal data protection laws and regulations relevant to the business
- Ensuring security policies support compliance with corporate governance practices
- Identifying where security can provide business advantage by addressing specific legal or regulatory needs

CESG Supplementation

Skill Level 1 – Is aware of major pieces of legislation relevant to Information Security and of regulatory bodies relevant to the sector in which they work

- Is aware of legislation relevant to IS: e.g. Official Secrets Act, Data Protection Act, Computer Misuse Act, and Freedom of Information Act
- Is aware of relevant regulatory bodies and key pieces of regulatory frameworks; for the public sector, shall be aware of the HMG Security Policy Framework (reference [g]) and CESG IA Policy Portfolio (reference [f])
- Own work complies with applicable legislation and regulation relating to IS
- Knows who to consult in own area with respect to legislation and regulation

Skill Level 2 – Understands applicable legislation and regulations relating to IS in the context of own or client organisations

- With supervision, advises whether business practices comply with relevant legislation and regulation based on an understanding of business requirements
- Recognises major non-compliances with applicable legislation and regulations
- Recognises when their advice is precedent setting and knows where to gain more expert advice if required

- Proposes updates to IS policies or standards to comply with legislation or regulations
- Is aware of major recent changes to legislation and regulations relevant to IS and considers their implications for own or client organisations
- For those working in the public sector, monitors updates to the CESG IA Policy Portfolio

Skill Level 3 – Influences business practices affecting IS through the application of legislation and regulations

- Analyses new and forthcoming legislation or regulations for their impact on own or client organisations
- Persuades management of the need to change Information Security practices to comply with legislation and regulations
- Authors IS policy or standards for own area of influence to comply with legislation and regulations
- Identifies need to change working practices in area of influence in response to new legislation or regulation
- Provides advice on the implications of export control regulations, in consultation with legal advisors if appropriate

Skill Level 4 – Is an authority on an area of legislation or regulation relevant to IS[13]

- Contributes to the development of legislation or regulation based on detailed understanding of the issues it aims to resolve
- Has an in-depth understanding of the reasoning behind legislation and regulations and its intended consequences
- Advises on the interpretation of legislation or regulation in circumstances that were not anticipated at the time of its creation; e.g. due to emerging technologies
- Provides authoritative guidance on the application of legislation or regulation for all those subject to it

[13] People at this skill level may be lawyers specialising in IA or IA specialists providing the subject matter expertise upon which legislation or regulation is based.

A7 – Third Party[14] Management

IISP Example Skills

- Identifying and advising on the technical, physical, personnel and procedural risks associated with third party relationships
- Assessing the level of confidence that third party security capabilities/services operate as defined

CESG Supplementation

Skill Level 1 – Is aware of the need for organisations to manage the information security of third parties

- Shall be able to explain the potential IS consequences to an organisation of failing to manage third parties effectively
- Is aware of an organisation's obligations to its data owners to ensure third parties protect data entrusted to them
- Is aware of the use of contract terms and conditions to protect information entrusted to third parties
- Is aware of policies and standards relevant to third party IS management; e.g. ISO27001 – Requirements for an Information Security Management System, Office of Government Commerce model terms and conditions for ICT

Skill Level 2 – With supervision, contributes to developing or maintaining compliance by third parties to the contracting authority's IS policies and standards

- Advises procurement or legal staff on the requirements for contracts to protect information entrusted to third parties based on a good understanding of the supporting IS requirements
- Specifies technical, physical, personnel or procedural security requirements expected from third parties
- Assesses the potential risks of entrusting third parties to protect information or to deliver services upon which the information security of the first party depends
- Assesses compliance by third parties to agreed information security policies and standards

[14] By 'Third Party' we mean an organisation's external suppliers or delivery partners as used in ISO 27001

Skill Level 3 – Enhances organisational information security through broad influence on third party management

- Develops organisational IS policies for sharing information with third parties
- Negotiates frameworks for managing third party protection of shared information
- Advises information risk owners or managers of the risks of supply chains including third parties that are not subject to EU legislation protecting personal data or privacy such as the EU Charter of Fundamental Human Rights
- Leads complex negotiations with third parties on standards for protecting shared information whether through transfer of data or access to a shared repository

Skill Level 4 – Advances best practice in third party management with respect to information security

- Authors guidance on third party management which influences the public sector or an industry sector
- Establishes new models for managing the risks of sharing information with third parties
- Develops IS techniques enabling wider use of less trusted suppliers

Skill Section B – Information Risk Management

IISP Principle

Capable of articulating the different forms of threat to, and vulnerabilities of, information systems and assets. Comprehending and managing the risks relating to information systems and assets.

Knowledge Requirements

Information risk management skills are based upon knowledge, understanding and proficiency in key specialisms such as, but not necessarily limited to, the following:

- Information risk management methodologies such as:
  - ISO 27005 - Information Security Risk Management
  - HMG IA Standard No 1 & 2, Information Risk Management (reference [h])
- Generic risk management methodologies such as:
  - ISO 31000 – Risk Management; Principles & Guidelines
  - HM Treasury Orange Book (reference [m])
  - CCTA Risk Analysis & Management Method (CRAMM) (reference [n])
  - Risk Management Standard, The Institute of Risk Management (reference [o])
- Key concepts
  - Threats, threat actors, vulnerabilities, likelihood, business impacts
  - Aggregation
  - Information assets and asset values
  - Risk appetite
  - Risk tolerance

B1 – Risk Assessment

IISP Example Skills

- Identification of assets that require protection
- Identification of relevant threats to the assets
- Identification of exploitable vulnerabilities
- Assessing the level of threat posed by potential threat agents
- Producing an information security risk assessment
- Determining the business impact of a risk being realised

CESG Supplementation

Skill Level 1 – Demonstrates awareness of the causes of information risk and their implications

- Shall be able to describe the components that determine information risk; asset, threat, threat actors, vulnerability, impact and likelihood
- Shall be able to identify at least one risk assessment methodology
- Is aware of sources of information on threats and vulnerabilities
- Is aware of the concept of protective markings and business impact levels
- For staff working in the public sector: shall be aware of HMG IA Standards Nos 1 & 2 (reference [h]) and the concepts contained within them
- Behaviour is consistent with an understanding of the causes of information risk and its implications

Skill Level 2 – Understands how to produce information risk assessments

- Can produce information risk assessments for Information Systems with basic supervision taking into account information assets, threats, threat actors, vulnerabilities, business impacts and likelihood
- Liaises effectively with stakeholders to collate relevant information and to explain risk assessments
- Assists risk owners or risk managers to identify appropriate business impact levels or protective markings taking into account the effects of aggregation
- For those working in the public sector: is able to author a Risk Management Accreditation Document Set in accordance with IS1 & IS2 (reference [h])

- For those working in the public sector: can use the HMG IA Standard No 1 technical risk assessment tool
- Can judge whether their risk assessments are within risk appetite or local risk tolerance and decide whether or not to escalate the decision
- For those working in the public sector: has undertaken courses on the use of IS1 & IS2 (reference [h])
- Follows guidance from ISO 31010

Skill Level 3 – Produces complex information risk assessments that influence senior risk owners, managers or other stakeholders

- Is able to produce credible risk assessments for complex and unusual systems without supervision
- Risk assessments are trusted by senior risk owners and risk managers
- Is able to apply findings from threat assessments, IT Health Checks and vulnerability testing tools into risk assessments
- Is able to tailor corporate risk assessment processes to meet specific business requirements to the satisfaction of the accreditor or other stakeholder
- Is able to suggest improvements to the risk assessment process and/or methodology
- Mentors risk assessors with less expertise and/or experience
- Is able to clearly articulate risk assessments to non IA practitioners
- Understands how information risk management fits within wider risk management strategies

Skill Level 4 – Influences development of information risk assessment methodologies across and beyond an organisation

- Influences departmental or national development of information risk assessment practices; e.g. in the context of shared services or using new technologies
- Information risk assessments have sufficient credibility to change major client, organisational or national priorities for risk mitigation
- Authors departmental or national guidance on information risk assessment practices
- Influences generic risk management strategies

- Influences professional development of risk assessors
- Is credible at main board level
- Recognises situations for which previous approaches are inadequate and develops innovative alternatives or novel solutions with widespread applicability

B2 – Risk Management

IISP Example Skills

- Developing information risk management strategies to reduce the risk
- Including information risk management strategies in business risk processes
- Gaining management commitment to the support of the information risk elements of business risk management
- Adapting the risk management strategy to address changes in the threat environment and in business risk
- Selecting the most appropriate tools and techniques for auditing effectiveness of mitigation measures in place

CESG Supplementation

Skill Level 1 – Demonstrates awareness of techniques to manage information risk

- Shall be able to describe different types of controls to mitigate risks (e.g. preventive, detective, corrective) and give examples of them
- Shall be able to describe the use of Business Impact Levels in information risk management
- Is aware of the requirements for an Information Security Management System (ISMS) as detailed in ISO 27001
- For those working in the public sector: shall be aware of HMG SPF (reference [g]), IS1 & IS2 (reference [h]) and CESG Good Practice Guide No 19 (GPG 19), Managing Accreditation – Governance, structure and Culture (reference [p])
- Is aware of sources of assurance; e.g. intrinsic, extrinsic, operational
- Is aware of the concepts of risk appetite and risk tolerance

Skill Level 2 – Contributes to management of risks to information systems with supervision

- Shall be able to describe and justify a risk treatment plan for at least one information system based upon stated risk appetite and a risk assessment
- Contributes to the design, review, approval or implementation of risk treatment plans for information systems with some supervision

- For those working in the public sector: shall be familiar with IS1 & IS2 (reference [h])
- For those working in the public sector: is able to author a Risk Management Accreditation Document Set (RMADS) or review a RMADS and assess whether it meets business requirements
- Understands the level of risk appetite or risk tolerance in usual area of work
- Is cognisant of and has appreciation of applicable legislation and regulations relating to IS in the context of own or client organisations (A6)

Skill Level 3 – Advises management on information risk across a business unit or organisation

- Designs, approves or implements risk treatment plans for information systems without supervision
- Maintains consistency in information risk management across an organisation
- Prioritises the allocation of information risk management resources across an organisation
- Contributes to the development of organisation information risk management frameworks that enhance the business in the long term
- Identifies value adding business activities that can be enabled by improved information risk management and advises how to achieve this
- Identifies IS controls upon which the organisation is most dependent
- Influences the level of resources allocated to information risk management
- Peer reviews risk management plans

Skill Level 4 – Advances the practice of information risk management across the public sector or an industry sector or internationally

- Authors risk management policy, standards or guidance that are used across the public sector or an industry sector
- Develops new methods for managing risks across an organisation
- Is widely consulted of the effectiveness of enterprise risk management frameworks
- Has influenced the body of knowledge on information risk management

Skill Section C – Implementing Secure Systems

IISP Principle

Comprehends the common technical security controls available to prevent, detect and recover from security incidents and to mitigate risk. Capable of articulating security architectures relating to business needs and commercial product development that can be realised using available tools, products, standards and protocols, delivering systems assured to have met their security profile using accepted methods.

Knowledge Requirements

Information Security Management skills are based upon knowledge, understanding and proficiency in key specialisms such as, but not necessarily limited to, the following:

- Security Architectures and Patterns
- Secure Development processes
- Life cycle activities
- Management responsibilities
- Business requirements
- Skills frameworks, e.g. SFIA
- Architectural frameworks, e.g.
  - The Open Group Architecture Framework (TOGAF), (reference [q])
  - MoD Architecture Framework (MODAF), (reference [r])
  - Zachman (reference [s])
- Range of core security technologies, e.g.
  - Access control models
  - Public and private encryption
  - Authentication techniques
  - Intrusion detection techniques and how to apply them
  - Common design patterns for mitigating against information risks

C1 – Security Architecture

IISP Example Skills

- Interpreting relevant security policies and risk profiles into secure architectural solutions that mitigate the risks and conform to legislation
- Presenting security architecture solutions as a view within broader IT architectures
- Relating security architectures to business needs and risks
- Working with recognised security architecture
- Devising standard solutions that address requirements delivering specific security functionality whether for a business solution or for a product
- Minimising the risk to an asset or product through “standard” security architecture practices
- Delivering the security architecture that supports the risk management strategy using current security technologies and techniques
- Maintain awareness of the security advantages and vulnerabilities of common products and technologies
- Minimising the risk to an asset or product through the use of “standard” security technologies and products
- Designing and developing processes for maintaining the security of an asset or product through its full life cycle
- Designing robust and fault-tolerant security mechanisms and components appropriate to the perceived risks
- Selecting the appropriate security products, components and technologies to meet a security requirement
- Selecting the most appropriate information interchange protocols that meet the security requirements

CESG Supplementation

Skill Level 1 – Is aware of the concept of architecture to reduce information risk

- Shall be able to explain how architecture can contribute to secure designs
- Understands design patterns or architecture relevant to their work
- Can explain some applications of architecture to manage information risk
- Understands that security architecture is one aspect of IT and enterprise architectures

Skill Level 2 – Applies architectural principles to security design with some supervision

- Provides advice on information system design to incorporate security architecture
- Recognises whether IS designs are compliant with key features of relevant security architectures
- Recognises major security weaknesses in enterprise architectures or IS architectures
- Has knowledge of architectural frameworks commonly used in a public or industry sector; e.g. TOGAF (reference [q]), Zachman (reference [s])
- Has knowledge of a range of core security technologies; e.g. access control models, public and private encryption, authentication techniques, intrusion detection
- Is familiar with system engineering techniques for developing coherent solutions to complex problems
- Has knowledge of some common design patterns for mitigating information risks

Skill Level 3 – Applies architectural principles to complex systems or to bring structure to disparate systems

- Designs security architectures for complex new information systems
- Influences IT or Enterprise Architectures to enable legacy applications to be migrated to a secure architecture or to enable secure integration of existing systems
- Influences senior managers to adopt architectural principles to reduce information risk
- Develops security architecture standards for application across an organisation
- Recommends changes to information systems to make them compliant with existing architectures
- Recommends changes to enterprise architectures to improve security
- Adapts existing architectures to accommodate new technologies or business requirements
- Has a broad knowledge of security vulnerabilities and techniques for defending against them

- Leads workshops to develop security architectures
- Supervises less experienced practitioners
- Has good knowledge of sources of up to date information relevant to security architecture design; e.g. CPNI, CESG, ISO standards

Skill Level 4 – Extends the influence of security architecture principles across the public sector or an industry sector

- Influences the security architecture of systems connecting multiple organisations
- Develops novel security architectures to meet new business requirements
- Persuades major organisations to adopt new security architecture standards
- Develops and communicates new security architecture ideas which are used across the public sector or an industry sector
- Provides intellectual leadership in a security practice influencing secure architectures of major information systems across multiple organisations

C2 – Secure Development

IISP Example Skills

- Implementing secure systems, products and components using an appropriate methodology
- Defining and implementing secure development standards and practices including, where relevant, formal methods
- Selecting and implementing appropriate test strategies to demonstrate security requirements are met
- Defining and implementing appropriate processes for transfer of a product/system to operation/sale/live use
- Defining and implementing appropriate secure change and fault management processes
- Minimising the risk to an asset or product through the 'standard' design and development processes
- Verifying that a developed component, product or system meets its security criteria (requirements and/or policy, standards and procedures)
- Analysing problem reports for signs of anomalous security issues, coordinating research into vulnerabilities and instigating corrective action where necessary
- Specifying and/or implementing processes that maintain the required level of security of a component, product, or system through its lifecycle
- Managing a system or component through a formal security assessment

CESG Supplementation

Skill Level 1 – Is aware of the benefits of addressing security during system development

- Shall be able to describe the benefits of designing security into systems early in the development lifecycle
- Can describe a system development lifecycle and the opportunities to influence its security during each stage
- Is aware of the existence of tools to test system security
- Is aware of the existence of systems engineering and product development practices
- Is aware of the potential need to satisfy the requirements of external CBs

Skill Level 2 – Contributes to the development of secure systems with some supervision

- Proposes security requirements for information systems
- Follows local processes for implementing secure systems
- Applies secure design patterns to system development
- Produces security artefacts required by CBs
- Contributes to the development or improvement of security techniques; e.g. authentication mechanisms, protective monitoring, malware defences, secure protocols, cryptographic algorithms
- Effectively uses tools to assist secure development

Skill Level 3 – Applies and improves secure development practices used across multiple projects, systems or products

- Supervises developers of secure systems
- Produces secure development processes, standards or guidance for local use
- Applies secure development practices to complex security requirements without supervision
- Adapts system development lifecycles to improve security
- Selects appropriate tools to enable secure development
- Improves secure design patterns
- Reviews information system designs to assess their security
- Develops or enhances security techniques; eg. authentication mechanisms, protective monitoring, malware defences, secure protocols, cryptographic algorithms
- Factors the security requirements of CBs into development plans

Skill Level 4 – Is an authority on the development of secure systems

- Develops new techniques for secure development which are widely adopted
- Provides assurance that systems operating at business impact levels 5 & 6 will meet their security requirements
- Provides a competitive advantage to major IT service providers by advancing their secure development capability
- Creates new tools enabling major improvements to secure development

Skill Section D – Information Assurance Methodologies and Testing

IISP Principle

Develops and applies standards and strategies for verifying that measures taken mitigate identified risks.

Knowledge Requirements

Information Security Management skills are based upon knowledge, understanding and proficiency in key specialisms such as, but not necessarily limited to, the following:

- Assessment Methodologies such as the ISO 27000 series and Common Criteria
- Information Risk Management Frameworks. For the public sector these also include:
  - IS1 & IS2 (reference [h])
- Assessment services or standards. For the public sector these also include:
  - HMG IA Standards
  - CHECK (reference [t])
- FIPS (reference [u])
  - CESG Claims Tested Mark
  - CESG Assisted Products Service
- Mitigation Measures, including keeping current with threats. For the public sector these include CESG Good Practice Guides
- Governance, as exemplified in the ISO 27000 series
- Management responsibilities
- Testing strategies
- Testing methodologies, such as required for EMC and Comsec testing. For the public sector these would include:
  - TEMPEST testing
  - CESG Implementation Guide No. 18, Forensic Readiness Planning (reference [v])

D1 – Information Assurance Methodologies

IISP Example Skills

- Developing methodologies for assessing the correct implementation of mitigation measures
- Assessing the level of assurance provided by a security mechanism, system or product in accordance with one or more recognised methodologies and standards
- Assessing whether a process is “fit for purpose” and meets the security requirements

CESG Supplementation

Skill Level 1 – Is aware of the existence of methodologies, processes and standards for providing Information Assurance

- Shall be aware of the fundamentals of IA; ie Confidentiality, Integrity, Availability, non-repudiation
- Shall be able to describe and demonstrate understanding of at least one IA standard or methodology
- Is aware of major security assessment services or standards; e.g. ISO 27000 series. For the public sector use this includes HMG IA Standards, CHECK (reference [t]), FIPS (reference [u]), CESG Claims Tested Mark, Common Criteria, CESG Assisted Products Service
- Understands what an Information Security Management System is and why it can be useful

Skill Level 2 – Applies an IA methodology or standard with some supervision

- Drafts components of an Information Security Management System in accordance with ISO 27001
- Drafts risk assessment and risk treatment plans in accordance with IS1 & IS2 (reference [h]) for review by an accreditor
- Interprets findings from IA methodologies in the business environment
- Recognises the limitations of an IA methodology to meet the business requirement

Skill Level 3 – Verifies risk mitigation using IA methodologies

- Applies recognised IA methodologies to verify that risks are mitigated to levels acceptable to risk owners and managers, taking into account the business environment and objectives
- Appropriately refines or interprets IA methodologies for use on complex tasks to meet the needs of risk owners or managers
- Advises whether a methodology is appropriate to identify or mitigate risks to information systems
- Supervises the use of IA methodologies
- Reviews the effective application of IA methodologies
- Justifies the choice of IA methodology to stakeholders or explains its limitations
- Applies IA methodologies proportionately to the potential business benefits or impacts

Skill Level 4 – Enhances the capability of IA methodologies to realise business benefits across the public sector or an industry sector

- Develops new IA methodologies to meet emerging IA requirements that are adopted across the public sector or an industry sector
- Authors new regulatory standards for IA methodologies to meet
- Expands the use of IA methodologies to new industry sectors or on a larger scale or to provide new business benefits
- Is an authority on the application of a widely recognised IA methodology
- Mentors experienced users of an IA methodology

D2 – Security Testing

IISP Example Skills

- Testing processes for vulnerabilities, highlighting those that are not addressed by security policies, standards and procedures and advising on corrective measures
- Applying recognised testing methodologies, tools and techniques, developing new ones where appropriate
- Assessing the robustness of a system, product or technology against attack
- Applying commonly accepted governance practices and standards when testing in an operational environment

CESG Supplementation

Skill Level 1 – Is aware of the role of testing to support IA

- Shall be able to describe and demonstrate understanding of how testing provides confidence of a system's security
- Shall be able to describe at least one security testing framework or process
- Understands why security testing cannot guarantee security

Skill Level 2 – Effectively applies testing methodologies, tools or techniques with some supervision

- Under supervision, develops test schedules or implements them
- Develops product test plans under supervision
- Drafts security requirements
- Assesses and interprets test results and proposes reasonable actions in response
- Contributes to end customer test reports
- Understands the difference between vulnerability testing and penetration testing

Skill Level 3 – Provides assurance on the security of a product or process through effective testing

- Shall be able to design an effective test programme for a product or process and is trusted to implement it effectively based on qualifications, training, experience and track record in identifying vulnerabilities
- Shall be aware of a wide range of vulnerabilities and exploits in their field of work
- Tailors the scope of testing to meet business requirements
- Knows where to find the latest information on vulnerabilities or exploits and can design tests to identify them
- Sets security testing standards or procedures for a category of products or processes
- Refines security testing standards or procedures in response to requirements for corrective measures
- Skilfully uses tools for systematic identification of vulnerabilities across multiple information systems
- Can explain to clients the implications of test findings
- Can prioritise the business importance of test findings
- Justifies to clients why their product/system subject to test failed to meet required standards
- Can explain the business implications of the limitations of test programmes
- Develops through life test programmes to assess whether security is maintained

Skill Level 4 – Advances assurance standards across a product range, technology, or industry sector through rigorous security testing

- Devises more thorough testing strategies or techniques that enable greater trust to be placed in a class of secure products or processes
- Is trusted to authorise a security product as fit to defend business critical systems against sophisticated and targeted attacks. In the public sector this means that a successful attack against systems would result in a Business Impact at Llevel 5 or 6
- Advances security testing practices across the public sector or an industry sector

- Develops new tools that are widely used to improve the effectiveness of security testing
- Through security testing, is able to persuade the public sector or an industry sector of significant new information risks
- Leads conferences or seminars on security testing
- Influences vendors of leading IT products to improve security

Skill Section E - Security Discipline - Operational Security Management

IISP Principle

Capable of managing all aspects of a security programme, including reacting to new threats and vulnerabilities, secure operational and service delivery consistent with security polices, standards and procedures, and handling security incidents of all types according to common principles and practices, consistent with legal constraints and obligations.

Knowledge Requirements

Information Security Management skills are based upon knowledge, understanding and proficiency in key specialisms such as, but not necessarily limited to, the following:

- Governance
- Management responsibilities
- Information Security Management Systems, such as ISO 27001
- IT Service Management processes, such as ITIL (reference [w])
- Existing and Emerging Vulnerabilities
- Use of penetration testing and vulnerability testing
- Risk Assessment and Monitoring
- Business Engagement
- Business Continuity Planning
  - Business Continuity Institute Good Practice Guidelines
- Operating Procedures
  - Operational accountability
- Communications
- Continuous improvement

E1 - Secure Operations Management

IISP Example Skills

- Establishing processes for maintaining the security of information throughout its existence
- Establishes and maintains SyOPs in accordance with security policies, standards and procedures
- Coordinating penetration testing on information processes against relevant policies
- Assessing and responding to new technical, physical, personnel or procedural vulnerabilities
- Managing implementation of information security programmes, and co-ordinating security activities across the organisation

CESG Supplementation

Skill Level 1 – Is aware of the need for secure management of information systems

- Shall be able to explain the potential for security incidents if information systems are not managed securely
- Shall be aware of common causes of security incidents; e.g. lost removable media, failure to scan files for viruses, weak or compromised passwords
- Is aware of sources of corporate security processes and procedures for maintaining operational security
- Is aware of incident reporting procedures in own area of work
- Is aware of tools commonly used to detect vulnerabilities and how they are used; e.g. port scanning, security checklists, protective monitoring, audits

Skill Level 2 – Monitors the application of Security Operating Procedures (SyOPs) with some supervision

- Drafts changes to SyOPs in response to newly identified vulnerabilities
- Monitors that SyOPs for introducing information systems into operational use have been followed
- Monitors compliance with routine SyOPs such as patching, updating anti-virus signatures or vulnerability testing
- Monitors the output of protective monitoring systems and alerts supervisors to suspicious events

- Monitors that SyOPs for decommissioning information systems and disposing of storage media are followed
- Provides advice on accepted practice for compliance with policies

Skill Level 3 – Manages the development of SyOPs for use across multiple information systems or manages compliance with them

- Leads development of the set of SyOPs used across multiple information systems
- Ensures coherence between SyOPs such that they combine to deliver cost-effective security
- Provides the information security content to security awareness campaigns
- Influences business managers to resource compliance with SyOPs
- Manages the review cycle for SyOPs, taking into account information from incidents, vulnerability assessments, penetration tests, threat assessments and changes to relevant legislation and regulations
- Interprets the meaning of relevant policies and implements appropriate Security Operations Procedures

Skill Level 4 – An authority on Security Operations Management, working across the public sector or an industry sector

- Reviews the adequacy of organisational security operations management
- Leads programmes to make major business driven improvements to security operations management across an organisation
- Develops effective cultural change programmes to improve organisational compliance with security procedures
- Contributes to the body of knowledge on effective security operations management

E2 - Secure Operations and Service Delivery

IISP Example Skills

- Configuring information and communications equipments in accordance with relevant security policies, standards and guidelines
- Maintaining security records and documentation in accordance with SyOPs
- Administering logical and physical user access rights
- Monitoring processes for violations of relevant security policies (e.g. acceptable use, security, etc.)

CESG Supplementation

Skill Level 1 – Is aware of the need for information systems and services to be operated securely

- Shall be able to describe the potential business impact of failure to operate information systems securely
- Can describe common causes of security incidents
- Can describe typical SyOPs for mitigating the risks of incidents
- Is aware of sources of corporate security processes and procedures for maintaining operational security
- Is aware of incident reporting procedures in own area of work

Skill Level 2 – Effectively applies SyOPs with some supervision

- Follows routine security procedures such as patching, updating anti-virus signatures or vulnerability testing
- Records security related activities to provide assurance to risk owners and managers that these activities have been completed
- Grants access rights in accordance with SyOPs
- Maintains secure configurations of equipment such as firewalls, routers, operating systems, applications, databases, cryptographic equipment, authentication systems
- Handles cryptographic key material or equipment in accordance with SyOPs

Skill Level 3 - Develops SyOPs for use across multiple information systems or maintains compliance with them

- Authors new SyOPs and gains support for their introduction
- Develops secure configuration or lockdown standards used across multiple information systems
- Maintains secure configuration of assets supporting multiple information systems; e.g. firewalls, routers, operating systems or applications
- Monitors compliance with SyOPs used across multiple information systems or services
- Takes responsibility for holdings of cryptographic key material or equipment

Skill Level 4 – Influences SyOPs used across the public sector or an industry sector

- Authors guidance on SyOPs used across the public sector or an industry sector
- Leads development of SyOPs used by a large service provider supporting multiple clients

E3 – Vulnerability Assessment

IISP Example Skills

- Analysing internal problem reports for signs of anomalous security issues
- Monitoring, collating and filtering external vulnerability reports for organisational relevance, ensuring that relevant vulnerabilities are rectified through formal change processes
- Engaging with the Change Management process to ensure that vulnerabilities are mediated
- Ensuring that disclosure processes are put in place to restrict the knowledge of new vulnerabilities until appropriate remediation or mitigation is available
- Producing warning material in a manner that is both timely and intelligible to the target audience(s)

CESG Supplementation

Skill Level 1 – Is aware of the need for vulnerability assessments to maintain Information Security

- Shall be able to explain why vulnerability assessments are required to maintain Information Security
- Can describe sources of vulnerability information; e.g. Common Vulnerabilities and Exposures; Warning, Advice and Reporting Points internal check lists
- Is aware of processes for responding to vulnerability assessments in own area of work

Skill Level 2 – Obtains and acts on vulnerability information in accordance with Security Operations Procedures

- Informs Change Management staff and other stakeholders of the need to respond to new vulnerabilities
- Identifies systems which are most vulnerable to attack and prioritises their work accordingly
- With supervision, studies information on recently identified vulnerabilities and assesses which are important or relevant to their area of influence
- Studies output from protective monitoring systems to identify potential exploitation of vulnerabilities
- Monitors corrective actions in response to vulnerability assessments

Skill Level 3 – Ensures that information risk managers respond appropriately to relevant vulnerability information

- Manages processes across multiple information systems for acquiring current vulnerability assessments and taking appropriate corrective action
- Prioritises actions to mitigate risks from vulnerabilities, taking into account threats and potential business impacts
- Influences senior management to resource vulnerability detection and mediation
- Devises metrics for monitoring the level of vulnerabilities
- Identifies potential business impacts if vulnerabilities are exploited
- Maintains lists of authorised or banned applications or devices for use on protective monitoring systems
- Co-ordinates corporate responses to vulnerability assessments

Skill Level 4 – Is an authority on the use or impact of vulnerability assessments across the public sector or an industry sector

- Sets policy for the collation of vulnerability assessments across the public sector or an industry sector
- Develops new techniques for systematically identifying the key risks to information systems from vulnerability assessments
- Uses trends on vulnerabilities to influence Information Security policy across the public sector or an industry sector
- Improves the use of tools to identify vulnerabilities across the public sector or an industry sector
- Recognises the business impact across a sector of exploitation of diverse combinations of vulnerabilities
- Convincingly explains to directors the potential business impact if vulnerabilities are exploited

Skill Section F - Security Discipline - Incident Management[15]

IISP Principle

Capable of managing or investigating an information security incident[16] at all levels.

Knowledge Requirements

Information Security Management skills are based upon knowledge, understanding and proficiency in key specialisms such as, but not necessarily limited to, the following:

- Secure Information Management (stakeholder management within organisational context)
- Incident detection techniques
- Incident response management (internal and external)
- Management responsibilities, e.g. ITIL (reference [w])
- Audit log management
- Forensics
  - Evidential standards - admissibility of evidence (adequate collecting and preserving) to a legal standard
  - Tools – disk imaging
  - Artificial Intelligence tools
  - ISO 27001
  - Impact assessment

[15] Incident Management is assumed to mean Security Incident Management in this context.

[16] Although ITIL defines incidents as service effecting, we do not assume that security incidents always affect information services.

F1 – Incident Management

IISP Example Skills

- Engaging with the overall organisation Incident Management process to ensure that security incidents are handled appropriately
- Defining and implementing processes and procedures for detecting breaches of security policy
- Defining and implementing processes for carrying out investigations into breaches of security policy
- Establishing and maintaining a Computer Security Emergency Response Team or similar to deal with breaches of security policy
- Co-ordinating the response to a breach of security policy
- Providing a full security response where third parties, managed service providers, etc. are involved

CESG Supplementation

Skill Level 1 – Is aware of the benefits of managing security incidents

- Shall be able to describe how security incident management can mitigate the consequences of security incidents
- Is aware of the main stages of incident management; e.g. identify, contain, cleanse, recovery, close
- Knows how to report a security incident within their own work area
- Is aware of the potential business impacts of security incidents upon Confidentiality, Integrity, Availability and reputation in their area of work
- Understands the need to preserve evidence to support formal proceedings

Skill Level 2 – Contributes to security incident management

- Provides input to new procedures for handling security incidents or for learning from them
- Provides an initial response to reported security incidents, escalating decisions where appropriate
- Maintains records of security incidents and produces summary reports
- Provides advice on how to respond to security incidents
- Manages security incidents under supervision
- Uses incident management tools effectively

Skill Level 3 – Manages security incidents

- Takes responsibility for managing assigned security incidents
- Ensures that security incident management is aligned with more general incident management
- Authors or authorises procedures for handling security incidents
- Improves organisational ability to manage security incidents in terms of detection or reporting processes, training for incident handlers and investigators or organisational procedures for damage limitation
- Provides input to the press office for handling media interest in security incidents
- Arranges separation of duties to avoid conflicts of interest
- Manages lessons learnt from security incidents within an organisation, ensuring that root causes have been identified and appropriate corrective measures implemented

Skill Level 4 – Is an authority on security incident management across the public sector or an industry sector

- Is experienced at handling major security incidents of direct concern to directors, regulatory bodies or ministers
- Is sought by the media for independent comment on major security incidents
- Co-ordinates responses to security incidents across multiple organisations
- Represents the organisation or sector in response to media interest
- Acts as an external reviewer of security incident procedures on behalf of a regulator
- Advances the body of knowledge on security incident management
- Promotes lessons learnt from security incidents across relevant sectors

F2 – Investigation

IISP Example Skills

- Working within the legal constraints imposed by the jurisdictions in which an organisation operates
- Carrying out an investigation into a breach of information security using all relevant sources of information including access logs, systems logs, camera footage, etc
- Assessing the need for Forensic activity, and coordinating the activities of specialist Forensic personnel within the overall response activities
- Engaging with the organisational Problem Management processes to ensure that Forensic services are deployed appropriately
- Providing a full security investigation capability where third parties, managed service providers, etc are involved

CESG Supplementation

Skill Level 1 – Is aware of basic principles of investigations

- Shall be able to describe common sources of information to support investigations into security incidents; e.g. people, CCTV, documents, computer files,
- Is aware of the need to preserve evidence for use in formal proceedings
- Is aware of local policies for investigations

Skill Level 2 – Contributes to investigations into security incidents

- Collects and records evidence to support security investigations; e.g. through interviews, studying documentation, analysing protective monitoring systems or impounding equipment, with some supervision
- Identifies potential sources of evidence
- Reporting initial findings from investigative work
- Knows how to record and preserve evidence such that it may be used to support formal proceedings
- Suggests ideas for improving team investigative capability

Skill Level 3 – Leads investigations into security incidents or manages a team of investigators or provides skilled support

- Shall have proven skills for investigating security incidents

- Takes responsibility for leading investigations into security incidents
- Manages a team of investigators; allocates individuals to tasks appropriate to their skills and experience, enables skill development, engages experts from beyond own team when required
- Presents evidence to support formal proceedings in response to investigations
- Co-ordinates investigations across multiple organisations

Skill Level 4 – Is an authority on security investigations

- Shall have a successful track record in leading investigations
- Leads investigations into serious criminal activity
- Provides independent subject matter expertise to support investigations run by other organisations
- Advances the body of knowledge on investigations

F3 – Forensics

IISP Example Skills

- Seizing evidence in accordance with legal guidelines and in the most effective manner to minimise disruption to the business and maintaining evidential weight
- Deploying specialist equipment to monitor for attempted system compromise
- Analysing system information (e.g. system logs, network traffic, hard disks, virtual memory, etc.) for evidence of breaches of security policy or laws
- Analysing software for malicious intent (malware)

CESG Supplementation

Skill Level 1 – Is aware of the capability of forensics to support investigations

- Shall be able to describe examples of information recoverable through forensics
- Is able to describe capabilities of some forensics tools
- Is aware of some forensic techniques
- Is aware of requirements to preserve forensic evidence
- Is aware of the existence of relevant legislation; e.g. principles in Data Protection Act, Regulations of Investigatory Powers Act

Skill Level 2 – Contributes to forensic activities, with some supervision

- Recovers or preserves data from storage media using forensic tools
- Seizes equipment as tasked whilst maintaining evidential weight
- Analyses data from protective monitoring sources for malicious intent
- Analyses software for malicious intent
- Deploys specialist tools to monitor for attempted system compromise
- Has knowledge of legal requirements for preservation of forensic evidence

Skill Level 3 – Manages forensic capability or provides skilled support

- Shall have experience of multiple forensic techniques and tools
- Shall have a track record of recovering evidence through forensics
- Has in depth experience of at least one forensic technique

- Knows which forensic techniques are most appropriate to support investigations and how to apply them with minimum business disruption
- Manages a team of forensic investigators
- Supervises less experienced forensics investigators
- Has an in-depth understanding of relevant laws and their application to forensics

Skill Level 4 – Is an authority on forensics

- Shall have a track record of recovering evidence through forensics which has been beyond the capabilities of forensic investigators at Level 2 or 3
- Develops new forensic techniques
- Advances forensic capabilities across the public sector or an industry sector
- Finds new business applications for forensic techniques
- Drafts new standards or guidance of widespread applicability

Skill Section G – Security Discipline – Audit, Assurance and Review

IISP Principle

Capable of defining and implementing the processes and techniques used in verifying compliance against security policies, standards, legal and regulatory requirements.

Knowledge Requirements

Audit skills are based upon knowledge, understanding and proficiency in key specialisms such as, but not necessarily limited to, the following:

- Audit methodologies
  - ISACA/Certified Information Systems Auditor (CISA)
  - ISO 27001
- Vertical/horizontal auditing techniques
- Audit processes. For the public sector these could include:
  - HMG IA Maturity Model (reference [l])
  - HMG SPF (reference [g])
- Audit techniques

G1 – Audit and Review

IISP Example Skills

- Verifying that information processes meet the security criteria (requirements or policy, standards and procedures)
- Defining and implementing processes to verify on-going conformance to security requirements
- Carrying out security compliance audits in accordance with an appropriate methodology

CESG Supplementation

Skill Level 1 – Understands basic techniques for testing compliance with security criteria (policies, standards, legal and regulatory requirements)

- Understands local processes for testing compliance with security criteria
- Understands the principles and rules of conduct in the practice of auditing; e.g. integrity, objectivity, confidentiality and competency
- Has received basic training in audit techniques

- Understands the benefits of auditing
- Is aware of at least one audit methodology

Skill Level 2 – Audits compliance with security criteria in accordance with an appropriate methodology

- Tests compliance with security criteria under supervision
- Supports a lead auditor to carry out audit assignments. In the public sector this includes auditing compliance with codes of connection, with HMG IA standards and with the requirements of the assessment framework of the HMG IA Maturity Model (reference [l])
- Audit findings influence information risk owners or managers. In the public sector this means influencing accreditors or Information Asset Owners
- Recommends or implements processes to verify on-going conformance to security requirements
- Assesses compliance with a code of connection
- Maintains current knowledge of relevant policies, standards, legal and regulatory requirements
- Is familiar with the professional practices expected by at least one audit body; e.g. Institute of Internal Auditors code of ethics, HM Treasury Guide on Internal Audit Standards, Information Systems Audit and Control Association code of professional ethics

Skill Level 3 – Influences senior information risk owners or business managers through information risk driven auditing

- Leads a team of auditors to conduct internal or external audits. In the public sector this could include assessments against the HMG IA Maturity Model,or checks for compliance with the HMG Security Policy Framework (reference [g]) or code of connection to public sector networks.
- Ensures audit plans and compliance testing activities are information risk driven based upon an understanding of threats, vulnerabilities and business impacts
- Has broad experience of conducting security audits
- Develops audit plans to meet audit assignments
- Effectively communicates credible audit findings to clients based on impartial, objective evidence and clear reasoning
- Identifies the security risks to the organisation from audit findings

- Identifies opportunities for improving audit techniques
- Audit findings influence senior information risk owners or business managers
- IRCA certificated ISMS Lead or Principal Auditor
- Able to conduct complex audits; e.g. involving multiple stakeholders, testing compliance against novel requirements or objectives, or whose findings set new precedents

Skill Level 4 – Advances the influence of security auditing across the public sector or across an industry sector

- Advances audit techniques and processes to test achievement of security objectives17
- Leads audits instigated by directors, ministers or regulatory bodies to identify root causes of security incidents of widespread interest
- Drives improvement in security audit regimes that enable strategic business benefits
- Audit findings influence development of public or industry sector security regulation, policies or standards

Relevant Qualifications and Training

- ISO 27001 Lead Auditor
- Member of Institute of Internal Auditors
- Certificated Information Security Management System (ISMS) Internal Auditor by International Register of Certificated Auditors (IRCA)

[17] By 'security objectives' we mean the business objectives that security policies, standards and requirements are intended to achieve. Security objectives could include meeting the security requirements to access externally owned data, ensuring the business is compliant with the Data Protection Act, compliance with ISO 27001 or keeping the risks of a business activity within agreed limits.

Skill Section H – Security Discipline – Business Continuity Management

CESG has produced a single supplementation for this skill section as none of the currently envisaged IA role definitions required separate supplementation of business continuity planning and management.

IISP Principle

Capable of defining the need for and of implementing processes for establishing business continuity.

Knowledge Requirements

Business Continuity Management skills are based upon knowledge, understanding and proficiency in key specialisms such as, but not necessarily limited to, the following:

- ISO 22301
- BS 25999
- Business continuity management lifecycle
- BCI Good Practice Guidelines
- Business Impact Analysis process
- HMG IA Maturity Model (reference [l])
- COBIT 4.1 (reference [x])
- ISO 27001
- BS 27031

H1 – Business Continuity Planning

IISP Example Skills

- Establishing the need for a Business Continuity Management (BCM) process or function
- Determining the events and external surroundings that can adversely affect an organisation
- Providing cost-benefit analysis to justify investment in controls to mitigate risks
- Determining and guiding the selection of possible business operating strategies for minimising disruption
- Designing, developing and implementing Business Continuity and Crisis Management plans
- Preparing a programme to create and maintain corporate awareness and enhance the skills required to develop and implement the Business Continuity Management programme
- Developing processes that maintain the currency of continuity capabilities and plan documents in accordance with the organisation's strategic direction
- Developing, co-ordinating and evaluating plans to communicate with internal stakeholders, external stakeholders and the media

H2 – Business Continuity Management

IISP Example Skills

- Developing and implementing procedures for responding to and stabilising the situation following an incident or event
- Establishing and managing an Emergency Operations Centre to be used as a command centre during the emergency
- Mounting pre-plan and co-ordinate plan exercises, and evaluating and documenting plan exercise results
- Verifying that the plan will prove effective by comparison with a suitable standard and of reporting results in a clear and concise manner
- Establishing applicable procedures and policies for co-ordinating continuity and restoration activities with external agencies while ensuring compliance with applicable statutes or regulations
- Co-ordinating, evaluating and exercising plans to communicate with internal stakeholders, external stakeholders and the media

CESG Supplementation

Skill Level 1 – Understands how Business Continuity Planning & Management contributes to information security

- Can describe the business continuity management lifecycle
- Understands the relationship between business continuity and information security
- Can describe how business continuity planning and management contributes to information security objectives
- Is aware of ISO standards relating to business continuity

Skill Level 2 – Contributes to the definition or implementation of business continuity processes to maintain information security

- Evaluates threats to information services through risk assessment
- Undertakes business impact analysis for information services
- Performs continuity requirements analysis for information services
- Identifies potential BCM strategies to achieve the maximum tolerable period of disruption for an information service
- Authors business continuity plans
- Exercises business continuity plans for information services, including in crisis situations
- Understands and can apply guidance from the Business Continuity Institute or other authoritative bodies
- Contributes to identification of Recovery Time Objectives and Recovery Point Objectives

Skill Level 3 – Leads definition or implementation of business continuity processes to maintain information security across a business unit or organisation

- Influences top management to support business continuity management
- Ensures business continuity management policy reflects an organisation's information risk appetite
- Leads activities to embed business continuity management across a business unit or organisation
- Validates analysis supporting business continuity strategies

- Selects business continuity strategies consistent with the organisation's information risk appetite and maximum tolerable period of disruption
- Endorses business continuity plans as being fit to meet business continuity strategies
- Leads definition or implementation of business continuity exercise programmes to assess the adequacy of business continuity plans
- Provides Key Performance Indicators for the BCM programme and provides assessments against them
- Leads corporate BCM exercises to provide assurance to the business
- Provides information security advice in crisis situations

Skill Level 4 – Is an authority on the information security aspects of Business Continuity

- Develops policies to improve resilience of information systems across the public sector or an industry sector
- Influences the level of investment to avert high impact but low probability scenarios across the public sector or an industry sector
- Provides expert consultancy on business continuity and information security at a senior level to multiple organisations
- Influences the design of major commercial products or services to reduce the risks of loss of information services
- Contributes to the public body of knowledge on the information security aspects of business continuity

Relevant Qualifications and Training

- Membership of the Business Continuity Institute
- ISEB Practitioner Certificate in Business Continuity Management

References

[a] The UK Cyber Security Strategy - www.cabinetoffice.gov.uk/resource-library/cyber-security-strategy

[b] Guidance to CESG Certification for IA Professionals - www.cesg.gov.uk/awarenesstraining/PET/pages/IA-certification.aspx

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

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

[e] IISP - www.instisp.org.uk

[f] CESG IA Policy Portfolio, http://cesgiap.gsi.gov.uk

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

[h] HMG IA Standard No 1 and 2, Information Risk Management , Issue 4.0, April 2012 (UNCLASSIFIED)

[i] WARP - http://www.govcertuk.gov.uk/warps.shtml

[j] HMG IA Standard No. 4, Management of Cryptographic Systems, Issue 5.1, April 2012. (UNCLASSIFIED)

[k] HMG IA Standard No.4, Supplement No.1, Roles and Responsibilities, Issue 1.0, April 2011 (UNCLASSIFIED)

[l] HMG IA Maturity Model and Assessment Framework - http://www.cesg.gov.uk/products_services/iacs/iamm/index.shtml

[m] HM Treasury – Orange Book: Management of Risk-Principles and Concepts, - http://hm-treasury.gov.uk/orange_book.htm

[n] CRAMM - http://www.cramm.com/

[o] Risk Management Standard, The Institute of Risk Management - http://www.theirm.org/publications/PUstandard.html

[p] CESG Good Practice Guide 19; Managing Accreditation – Governance, Structure & Culture - http://cesgiap.gsi.gov.uk/ia-policy-portfolio/good-practice-guides.html

[q] TOGAF, www.togaf.info

[r] MODAF - http://www/mod.uk/DefenceInternet/AboutDefence/WhatWeDo/InformationManagement/MODAF/

[s] Zachman Framework - www.zifa.com/framework.html

[t] CHECK - www.cesg.gov.uk

[u] FIPS - http://www.itl.nist.gov/fipspubs/

[v] CESG Implementation Guide No. 18 , Forensic Readiness Planning, Issue 1.0, June 2011 (UNCLASSIFIED)

[w] ITIL - www.itil-officialsite.com)

[x] COBIT - http://www.isaca.org/knowledge-Center/Cobit/Pages/Overview.aspx

Glossary

CB	Certification Body
CHECK	IT Health Check Service
CINRAS	Comsec Incident Notification, Reporting and Alerting Scheme
CIO	Chief Information Officer
CLAS	CESG Listed Advisor Scheme
COBIT	Control Objectives for Information and Related Technology
CPNI	Centre for Protection of National Infrastructure
CRAMM	CCTA Risk Analysis and Management Method
CTO	Chief Technology Officer
DSO	Departmental Security Officer
EA	Enterprise Architecture
FIPS	Federal Information Processing Standard
IA	Information Assurance
IAO	Information Asset Owner
ICT	Information Communications and Technology
IISP	Institute of Information Security Professionals
IS	Information Security
ISEB	Information Systems Examination Board
ITIL	Information Technology Infrastructure Library
ITSO	Information Technology Security Officer
MODAF	MoD Architecture Framework
RMADS	Risk Management Accreditation Document Sets
SFIA	Skills Framework for the Information Age
S&IRA	Security and Information Risk Advisor
SIRO	Senior Information Risk Owner
SyOPs	Security Operating Procedures
TOGAF	The Open Group Architecture Framework
WARP	Warning, Advice and Reporting Point

THIS PAGE IS INTENTIONALLY LEFT BLANK

Customer Feedback

CESG Information Assurance Guidance and Standards welcomes feedback and encourages readers to comment on the Role and Skill definition concept of operations outlined in this document. Please use this page to send your comments to:

Customer Support
CESG
A2j
Hubble Road
Cheltenham GL51 0EX

Fax: (01242) 709193 (for UNCLASSIFIED FAXES ONLY)
Email: enquiries@cesg.gsi.gov.uk

PLEASE PRINT

Your Name:

Department/Company Name and Address:

Phone number:
Email address:

Comments:

THIS PAGE IS INTENTIONALLY LEFT BLANK

IA
CESG
A3e
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX

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