

UNCLASSIFIED



2011 - IA Maturity Model Supported Self-Assessment Guide

(Version 2.1 dated 14 April 2011)

© Crown Copyright 2011 – All Rights Reserved

UNCLASSIFIED

UNCLASSIFIED

Document History

Version	Date	Description
0.1	24 Nov 09	Initial draft
0.2	25 Nov 09	Incorporating CESH & IS&A input
0.3	25 Nov 09	Final CESH & IS&A input
1.0	26 Nov 09	Agreed Version
1.1	27 Nov 09	Modification to formatting
2.0.1	15 Nov 2010	Draft revision for 2011 SSA
2.0.2	26 Nov 2010	Comments on previous draft
2.0.3	30 Nov 2010	Revised team involvement in evidence assessment and incorporation of screen shots
2.0	14 Dec 2010	Final draft for publication
2.1	14 April 2011	Modification to content (references, and typographical)

This document is issued by CESH

For additional copies of this document or for general queries please contact:

CESG Document Manager
CESG
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX

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

CONTENTS

Document History ii

Contents iii

References iv

Introduction 1

Cabinet Office Security Risk Management Overview..... 2

Using the Assessment Tool 5

SSA Planning Meeting 6

Establishing Evidence of IA Maturity 7

Support Available from CESC 8

Feedback to CESC 8

Conclusion 8

Annex A – Suggested List of Documents for Assessment A-1

Annex B – 2011 Assessment Tool – Example Results B-1

UNCLASSIFIED

References

1. HMG Information Assurance Maturity Model and Assessment Framework Version 4.0 dated 27 May 2010¹ (http://www.cesg.gov.uk/products_services/iacs/iamm/index.shtml)
2. HMG Security Policy Framework (HMG SPF) Version 5.0 dated February 2011 (<http://www.cabinetoffice.gov.uk/resource-library/security-policy-framework>)
3. Cabinet Office Data Handling Review Report dated June 2008 (<http://www.cabinetoffice.gov.uk/resource-library/data-handling-procedures-government>)
4. HMG IA Standard No 6 Protecting Personal Data and Managing Information Risk (from CIAP [information that led to IS6 is also available from <http://www.cabinetoffice.gov.uk/resource-library/data-handling-procedures-government> {e.g. Cross Government Actions: Mandatory Minimum Measures}})
5. BS ISO/IEC 27001:2005 dated 15 October 2005 (<http://www.iso.org>)
6. National Information Assurance Strategy (NIAS) dated June 2007 (http://webarchive.nationalarchives.gov.uk/20090707073435/http://cabinetoffice.gov.uk/csi/a/national_IA_strategy.aspx)
7. 2010/11 Cabinet Office Security Risk Management Overview (SRMO) dated January 2011 (Where appropriate, this may be specifically requested from the Cabinet Office [e.g. datareview@cabinet-office.x.gsi.gov.uk])

(Note: Where a document's information provides hyperlink references, these are for convenience, and were valid at the time of publishing. Hence, they cannot be guaranteed to work at a later date. If these hyperlinks do go out of date, then the use of appropriate search tools, on the appropriate web sites, may help in finding any relocated documents. In relation to Cabinet Office documents, please contact the Cabinet Office).

¹ IAMM v5 will be issued as a CESG Good Practice Guide (GPG) in 2011, and should be referred to once published in preference to this reference.

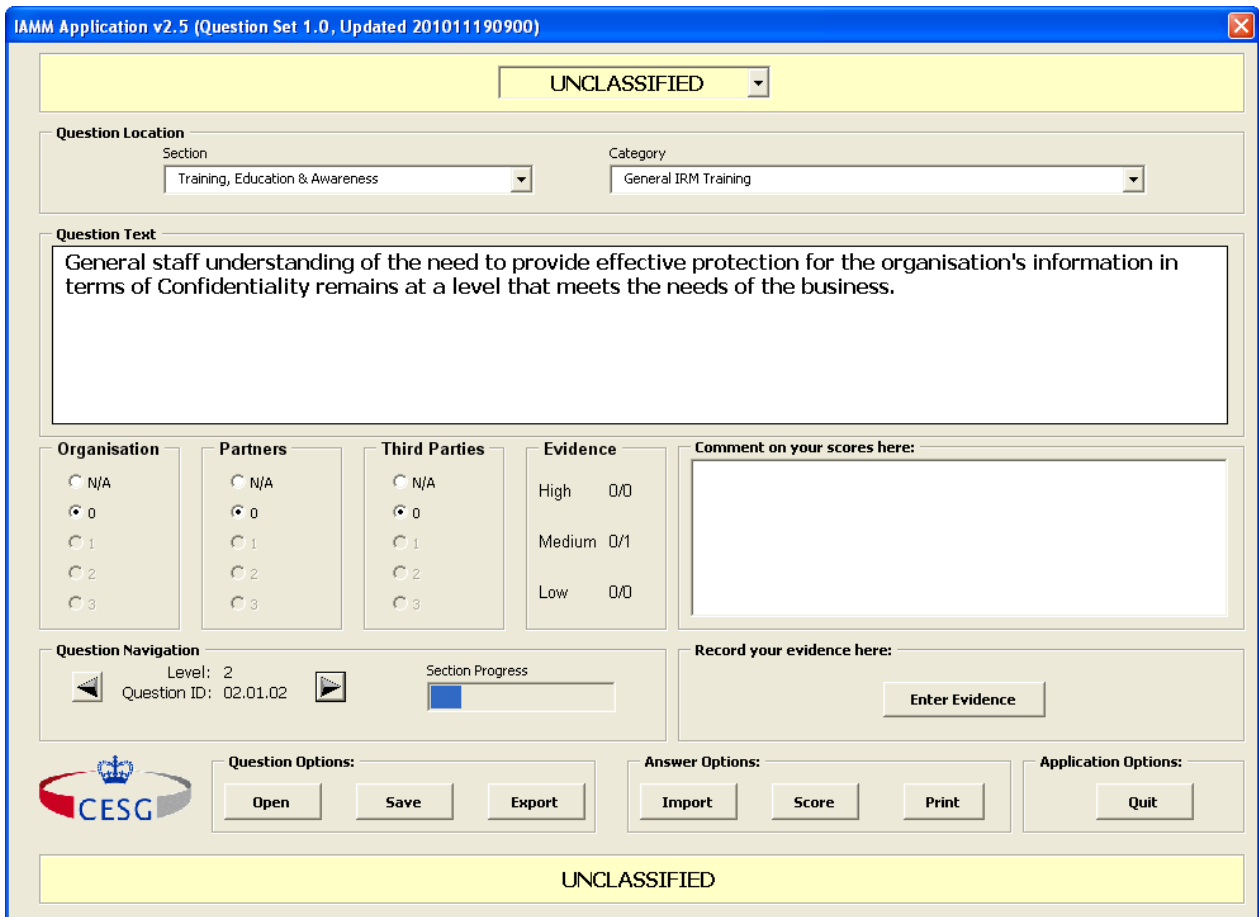
INTRODUCTION

1. On 30 September 2008 the Cabinet Office and CESA published the HMG Information Assurance (IA) Maturity Model (IAMM) and IA Assessment Framework to assist Senior Information Risk Owners (SIROs) in the task of developing IA maturity within their Departments.
2. The latest version of the IAMM[1] incorporates the mandatory Information Security and Assurance requirements of the HMG Security Policy Framework (HMG SPF)[2], which includes the requirement to apply the 2008 Data Handling Review (DHR)[3], (also available as IAS6[4]) and is aligned with both the ISO/IEC27001:2005 Standard[5] and the broader outcomes sought by the National IA Strategy[6]. The IAMM is underpinned by an IA Assessment Framework (IAAF)[1] which gives considerably more detail of the measures required to deliver the specific levels of maturity on which the Model is based.
3. In 2011 Ministerial and non-Ministerial Departments are required to provide an annual report to Cabinet Office using the Security Risk Management Overview (SRMO). Should the Cabinet Office be required to provide a report to Parliament on the progress being made by Central Government Departments on this issue as a whole, as it has in the past, then these departmental reports will be used to inform the process of completing this Report to Parliament. As in previous years, Departments may take advantage of the IAMM[1] and associated CESA Supported Self-Assessment procedure to establish the evidence to support the SRMO.
4. The Aim of this document is to give details of how the Supported Self-Assessment (SSA) procedure and the associated Tool may be used to assist the reporting requirement to the Cabinet Office, and provide guidance on the CESA IA Supported Self-Assessment Service which is designed to provide limited support from CESA staff to assist the SIRO in making the necessary assessments. It is anticipated that Departments will draw heavily on this assessment for their annual report and for aspects of their Statement on Internal Control. Note that this document does not cover all aspects of the content of the SRMO, which is covered in full within the Guidance produced by Government Security Secretariat (GSS)[7].

CABINET OFFICE SECURITY RISK MANAGEMENT OVERVIEW

5. The 2011 Cabinet Office SRMO is required to be completed by each Department and submitted by the SIRO to the GSS by 13 June 2011. The results from Departments may then be collated by GSS to form the basis of evidence on which a report to Parliament may be prepared. A Supported Self-Assessment using the associated Tool will provide a Department with details of what it has done to implement effective IA, which will constitute supportive evidence for the SRMO. The use of such an evidence-based process should provide a reliable indicator of year-on-year progress.

6. The SSA Tool is based on a Microsoft Excel Application containing detail derived from the IAAF in the form of a series of outcome orientated Information risk Management (IRM) requirements. Each of these Requirements is underpinned by a set of Evidence Statements, which enable the Department to determine whether they have completed the activity judged to be needed to deliver the Requirement. An example from the Tool is as follows:



UNCLASSIFIED

IAMM Application v2.5 - Evidence ✖

General staff understanding of the need to provide effective protection for the organisation's information in terms of Confidentiality remains at a level that meets the needs of the business.

No	Evidence	Importance	Available	Notes
1	Evidence exists that staff within the organisation and within its supply chains are taking appropriate action to protect the organisation's information. The general understanding of the staff of the need to protect the Confidentiality of the organisation's information is sufficient to meet the needs of the business.	Medium	<input type="radio"/> Yes <input checked="" type="radio"/> No	

UNCLASSIFIED

7. Each piece of evidence within the Evidence Statement is rated as being of High, Medium or Low importance and those completing the assessment use the radio buttons within the Tool to record the presence of satisfactory evidence. A notes column is also provided to enable details of the evidence to be recorded, which might prove useful in any subsequent analysis of the results generated by the Tool. Based on the availability of the evidence a score is derived using the scoring regime which follows. It should be noted that there is no automatic mechanism in the Tool to calculate a score from the record of evidence importance. The latter is recorded purely to assist the Department in gathering and assessing evidence, it is then up to the Department to interpret a score using the guidance in the table below.

N/A	Not applicable. A formal decision has been taken by the organisation that the required measure is not applicable in the context of managing information risk.
0	Hardly any of the Important (High), Medium Importance (Medium) or Low Importance (Low) evidence is available and that which is provided is not satisfactory.
1	Only some of the Important (High) and hardly any of the Medium importance (Medium) and Low importance (Low) evidence is available and is satisfactory.
2	The majority of the Important evidence (High) and some of the Medium importance (Medium) and Low importance (Low) evidence is available and is satisfactory.
3	All of the Important evidence (High) and the majority of the Medium importance (Medium) and Low importance (Low) evidence is available and is satisfactory.

8. Where the Department has an obligation to ensure that its Delivery Partners and 3rd Party Suppliers (these categories are defined in Appendix 3 of the guidance provided with Reference 7) meet the specified requirement, it is required that separate scores be entered.

9. The application also allows the user to establish the organisation's target IA maturity compliance levels prior to completing the assessment. This is then used in the presentation of the results, which is done in two ways:-

- a. As an overall assessment of compliance against the organisation's target IA Maturity Model levels, at each of the first three levels of the Model. An example of how the results are provided is at Annex B.
- b. As a detailed breakdown of the scores recorded, against each requirement, at each level, for the Department, its delivery partners and its 3rd party suppliers.

10. Throughout the Tool there is the opportunity for users to enter commentary, where this would be helpful in describing the Department's assessments.

USING THE ASSESSMENT TOOL

11. Whilst a significant amount of detailed information is required to complete the entries required by the Tool, it is anticipated that much of the data should already be available as a result of Departments having been required by the DHR to establish a regime in which the SIRO is presented with evidence from across the Department, its delivery partners and 3rd Party Suppliers, about how effective IRM is being delivered.

12. The DHR recognised that the implementation of the measures would be phased, with progress being fastest in respect of a Department's own activity and the activity of those bodies where Departments are in a position to mandate certain ways of working. Departments should identify any major differences in progress between themselves and bodies they control directly and with partners over whom they can only influence.

13. It is recommended that the SIRO brings together an Assessment Team consisting of between four and seven people who have sufficient experience and knowledge of how the Department is delivering effective IRM across the broad range of IA related disciplines from security to information management, Internal Audit (where appropriate) and data protection. But in all cases, it is imperative that the individuals chosen can take a business orientated view of IA. Additionally, it is strongly advised that a trained CESG Team Leader should be engaged to facilitate the assessment process and provide challenge. This is a cost recovery service.

14. The selected Assessment Team Members will need to be free to:

- a. Meet with the other Team members at an Assessment Planning Meeting
- b. Set aside sufficient time to read the IA documentation of which they are unfamiliar (See Annex A for a list of recommended documents)
- c. Optionally and in advance of the one day workshop, record in the tool the evidence available to satisfy a particular requirement
- d. Devote one day to a workshop with the other Team members during which the IRM Assessment is made and the Tool populated with data.

15. Experience gained from running these assessments in the past is that those members of the Department who form the Assessment Team learn a lot about how IA implementation within the Department can be improved, but to gain best value from the assessment prior knowledge of the HMG IA Maturity Model and the IAAF is essential. As a minimum, it is essential that staff have had the opportunity to read this Guide and understand the make-up of the Tool, prior to the Assessment Planning Meeting, so that they are aware of the breadth and depth of the task they are to undertake.

SSA PLANNING MEETING

16. The Planning Meeting is an essential part of the Assessment process as it is likely to be the first time that the Assessment Team will have come together to discuss the Assessment and clarify any issues they might have.
17. One of the key outputs of the Planning Meeting is the production of an agreed document reading list and a timetable detailing precisely when the documents can be made available to the Assessment Team Members and when the SSA Workshop is to be held. A suggested list of the documents which need to be made available to the Assessment Team is at Annex A. This list will need to be adapted to match the target level of IRM maturity within the Department, together with the terminology which is normally used.
18. Another key output of the Planning Meeting is to determine how evidence of IA maturity in delivery partners and 3rd party suppliers is to be presented at the Assessment Workshop. Cabinet Office Guidance [7] includes an extract from the Information Risk Return (IRR) guidance detailing the requirements that are applicable to delivery partners and 3rd party suppliers and the Department will need to have done preparatory work collecting the required assessment data prior to the Assessment Workshop.

ESTABLISHING EVIDENCE OF IA MATURITY

19. The design of the tool allows for the presence of satisfactory evidence to be recorded prior to the workshop, and by different members of the team. One way of achieving this would be for the Departmental administration support to send copies of the Tool to various appropriate parties in the Department, to populate different Evidence Sheets and giving details of the documentary references that apply (or where the evidence does not exist, recording notes to that effect). For example, the Leadership & Governance evidence sheets might be completed by one person, and the Training, Education & Awareness sheets by another, etc.. These could then be integrated into a single instantiation of the tool for the workshop.

20. The Assessment Team should then meet for a workshop during which evidence against the Requirements set out in the Tool should be considered and a score for compliance against each measure agreed. It may be necessary during the course of the workshop for a team member to break out to contact other members of the Department for additional information or to gain clarification of evidence gained from the documentation. The output of the workshop will be a completed Assessment showing the organisation's compliance status against the various IAMM derived requirements and against the Department's target level of maturity, with a commentary where considered applicable.

21. The Assessment should be evidence based. It is therefore essential that the Assessment Team Members allow sufficient time to read the IA documentation. The existence of a document alone is insufficient to meet the requirements of the assessment. The Assessment Team will be required to exercise judgement in determining the effectiveness of a particular document in delivering the required intent, and this can be recorded as an Importance level (e.g. see paragraph 7 above) against each piece of evidence. Other documents may help in this regard, but it is likely that those conducting the Assessment will have to exercise their subjective judgement based on their knowledge of how the Department operates.

SUPPORT AVAILABLE FROM CESH

22. Support to Departments is available from CESH. Members of CESH have been trained in the use of the IA Maturity Model and IAAF, and the Assessment Tool, to enable them to form independent IA Reviews Teams. One of these members of staff will be made available to each Department to facilitate and lead Departmental staff in populating the Tool. The person allocated to the Department should co-chair the Assessment Planning Meeting, they will set time aside to read the material on the agreed reading list, and will lead and facilitate the Assessment Workshop.

23. To engage the services of a member of CESH to assist in the completion of the Assessment, a member of the Department should complete the IAMM Assessment Services and Application Form available from the CESH website and submit this to the Enquiries team at CESH. On receipt, the appropriate CESH Service Manager will make contact with the Department with a view to determining the availability of CESH staff to meet the Department's requirements.

FEEDBACK TO CESH

24. The materials to support the use of the HMG IA Maturity Model are regularly updated. If you have any comments on how this Guide to completing the SSA (or any of the other information relating to the use of the IA Maturity Model), could be improved, then please pass your comments to the CESH Enquiries desk, who will send these to the appropriate area of CESH for consideration.

CONCLUSION

25. This Guide to the Supported Self-Assessment procedure has been prepared to assist SIROs in setting up and running an Assessment within their Departments and to provide details of the CESH Supported IA Self-Assessment Service, which will provide them with some independent professional assistance. It is based on experience gained in delivering the fully independent IA Reviews provided by the CESH Benchmarking Service.

26. An IA Supported Self-Assessment, designed to complement the SRMO, by its very nature cannot replicate the fully independent IA Review provided by CESH, but following the practice and procedure within this Guide will help to ensure that the effort devoted to this activity will produce something of meaningful use to the Department.

Annex A - Suggested List of Documents for Assessment

1. The precise list of documents that will need to be read by the Assessment Team is likely to depend on the Department and its IA maturity. However, the following list, should give an indication of the documentation which may be required.

2. This may seem an enormous list, but the reading task is split between Team members depending on their experience and expertise. In addition, since this includes evidence to support the achievement of higher levels of IA maturity within the Maturity Model, it is highly likely that some of these documents do not exist, or the information to cover off several of the requirements can be found in one document. For clarity, some items are repeated in more than one section.

- **Leadership & Governance**

- Main Board Policy Statement on IA
- Main Board minutes
- TORs for SIRO, IAO, DSO, ITSO, and COMSO if applicable
- Information Security Policy
- Organisational Risk Appetite
- Departmental Information Risk Assessment
- Departmental Information Risk Policy
- Information Charter and details of how staff and the public are made aware of its contents
- IA Strategy endorsed by Main Board (possibly part of Information Management Strategy)
- Details of IA Governance and whether this has been critically reviewed for its efficacy
- Details of how IAOs are discharging their mandatory responsibilities
- Information Asset Register, showing business critical assets
- IA programme details
- Written Assessment by SIRO to AO of how DHR recommendations are delivering the required change.
- Reports from SIRO to the Main Board
- Departmental SIC incorporating IRM
- Departmental Annual Report incorporating IRM

- **Training, Education & Awareness**

- Details of annual Information Risk Awareness Training given to all staff handling personal data in the Department, its arm's length bodies and its delivery partners, and details of how this is validated
- Information Risk Cultural Change Plan to include HR arrangements to reward positive approaches to IRM, mechanisms to capture staff concerns and how staff attitude is to be measured
- Details of Training Needs Analysis work
- Details of targeted IA education and training
- Details of how staff behaviours are measured and trends analysed
- Details of pre-appointment IA training and effectiveness
- Details of disciplinary action taken on IA related matters
- Details of collated training information provided to SIRO.

- **Information Risk Management**

- Information Risk Policy (possibly part of Departmental Risk Policy)
- Statement of Main Board IA risk appetite and how this is promulgated
- Evidence that a Departmental list of all information assets exists and that this is annotated to show the relevant IAO
- Annual Departmental Information Risk Assessment
- Organisational Threat Assessment
- Board Level Departmental Risk Register
- Departmental IA Risk Register
- Details of how all new IS are subject to accreditation
- Details of how PIAs are used for new IS
- Details of direction given to commercial staff mandating use of OGC Model Contract Clauses covering Information Risk
- Details of how Department's approach to IRM is agreed with external stakeholders including details of operations and data located off-shore
- Details of the accreditation status of all IS used by the Department
- Details of the application of Risk Appetite to accreditation decisions
- Details of IRM governance arrangements showing how IA risks are escalated to include the Department, its arm's length bodies, its delivery partners and its external stakeholders
- List of Business critical IS endorsed by SIRO
- Details of the risk based programme of work to tackle accreditation shortfalls
- Details of residual risks accepted for IS and systemic IA risks that impact on the delivery of the Department's business, including Digital Continuity arrangements
- RMADS for main Departmental IS
- Sy Ops for main Departmental IS
- Internal documents relating to those elements of the Manual of Protective Security, or the newly published Security Policy Framework, that have a direct bearing on the management of information risk within the Department

- **Through-Life IA Measures**

- Details of plans to determine the IA status of all Departmental IS
- Information Security Policy (may form part of Departmental Security Policy or Instructions), together with any security policy audit reports.
- Details of the arrangements to safeguard unencrypted personal information
- Details of use of encryption standards
- Details of how physical security measures are implemented and assured
- Details of Departmental security checking and vetting process and how it is assured
- Details of the risk based programme of work to tackle IA weaknesses
- Details of technical and operational risk reviews undertaken and work that has been undertaken as a result
- Representative Security Operating Procedures (SyOps)
- Departmental Acceptable Use Policy
- Remote Working Policy including controls on removable media
- Supply chain contractual arrangements covering IA/IRM/NDA's
- IA Incident management Policy including Incident Reporting Policy
- Forensic Readiness Plan, and details of how it has been validated
- Departmental incident management arrangements and metrics for IA related incidents and problems
- Business Continuity (BC) and Disaster Management (DM) Plan(s) including details of how they are validated
- BC & DM Test Report relating to IS
- Details of Departmental Access Management policy and practice, including arrangements with HR
- Details of Departmental Vulnerability Detection policy and practice
- Details of Departmental Patching policy and practice
- Details of Departmental Lock-Down policy and practice
- Details of Departmental Anti-Malware policy and practice
- Details of Departmental Controlled Disposal policy and practice

- **Assured Information Sharing**

- Information sharing policies
- Details of how the Department works with external stakeholders to achieve shared IA objectives
- Details of how the Department plans to implement IA control mechanisms to understand and control how IS interact internally and externally to the Department
- Network Management Board arrangements
- Network Security Policy
- Details of network boundaries and information sharing policies
- Details of agreements to Codes of Connection and how they are policed
- Details of any Enterprise Security Architecture Work.
- Details of Departmental Protective Monitoring policy and practice, including situational awareness, to include how it shares the data with external stakeholders.
- Details of system and network incidents and problems and what information is provided to the SIRO

- **Compliance**

- Details of the Department's IA compliance regime.
- Audit Committee reports relating to IRM
- Audit Unit reports relating to IRM
- Departmental Annual Report to CO on IRM
- Details of any external IA review undertaken
- A representative RMADS
- Organisational Risk Assessment
- Statement of Internal Control (SIC)
- IA improvement reports

Annex B – 2011 Assessment Tool – Example Results

