

UNCLASSIFIED



Guide to Assisted IA Assessment Service Using the HMG IA Maturity Model and Assessment Framework

(Version 0.3 dated 6 October 2008)

© Crown Copyright 2008 – All Rights Reserved

UNCLASSIFIED

UNCLASSIFIED

Document History

Version	Date	Description
0.2	30 Sep 08	Initial draft
0.3	6 Oct 08	Incorporating amendments from PJH

This document is authorised by:

P J Hooper
IA Maturity Model Benchmarking Team Leader

This document is issued by CESG

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

Approach to Assisted IA Assessment 1

Setting Up an Assisted IA Assessment 2

SIRO'S Responsibilities 2

Appointment of an IA Assessment Coordinator 2

Requesting Assistance from CESH 2

Selecting IA Assessment Team Members 2

The IA Assessment Planning Meeting 3

Establishing Evidence of IA Maturity 3

Conducting IA Assessment Interviews 4

The IA Assessment Report 4

Feedback to CESH 5

Conclusion 5

Annex A – Generic Agenda for the Planning Meeting A-1

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

Annex C – Suggested List of Interviewees C-1

Annex D – Suggested Format for IA Assessment Report D-1

References

1. HMG Information Assurance Maturity Model and Assessment Framework dated 30 September 2008
2. HMG Security Policy Framework (SPF) - Replaces the Manual of Protective Security in November 2008
2. Cabinet Office data Handling Review Report dated June 2008
3. BS ISO/IEC 27001:2005 dated 15 October 2005
4. National Information Assurance Strategy (NIAS) dated June 2007

DRAFT

INTRODUCTION

1. On 30 September 2008 the Cabinet Office and CESC published the HMG Information Assurance (IA) Maturity Model and Assessment Framework¹ to assist Senior Information Risk Owners (SIROs) in the task of developing IA maturity within their Departments.
2. The IA Model incorporates the IA requirements of the HMG Security Policy Framework (HMG SPF)² and the 2008 Data Handling Review³ and is aligned with both the ISO27001 Standard⁴ and the broader outcomes sought by the National IA Strategy⁵. The Model is underpinned by an IA Assessment Framework (IAAF) which gives considerably more detail of the measures required to deliver the specific levels of maturity on which the Model is based and is designed to be used as part of an IA Review process.
3. CESC has designed an IA Benchmarking Service to provide SIROs with an independent assessment of the maturity of a Department against the requirements of the IA Maturity Model (full details of this service are available on the CESC website). However, the IAAF can also be used by SIROs who wish to conduct an IA Self-Assessment, using entirely their own resources, or an Assisted IA Assessment, with some limited support from CESC staff.
4. The Aim of this document is to provide guidance to SIROs in conducting an Assisted IA Assessment.

APPROACH TO ASSISTED IA ASSESSMENT

5. A very rough and ready assessment of maturity against the IA Maturity Model can be achieved by making a subjective assessment of the level of compliance against the detailed requirements contained within the IAAF. However, the flaw in such an approach is that the results obtained will be coloured by the roles of the people making the assessment have had in the process that is being assessed. Also experience shows that it is difficult to make an assessment of the effectiveness of a particular measure without speaking to those who have been impacted by it, to assess whether the desired outcome has been achieved.
6. A far better method of conducting an IA assessment is to conduct a more formal IA Assessment designed to mirror the practices and procedures used by the independent review teams who deliver the CESC IA Benchmarking Service. The remainder of this document adopts this approach by providing specific guidance on how to conduct such an Assisted IA Assessment.

SETTING UP AN ASSISTED IA ASSESSMENT

SIRO's RESPONSIBILITIES

7. The SIRO needs to take ownership of the Assisted IA Assessment to ensure that sufficient time and resource are devoted to it. Without this level of involvement it is unlikely that the Assessment will be successful. Guidance on what the SIRO is required to do as part of the CESC IA Benchmarking Service is on the CESC website and much of that detail is relevant to the conduct of an Assisted IA Assessment.

APPOINTMENT OF AN IA ASSESSMENT COORDINATOR

8. Another key factor in determining the success of an IA Assessment is the appointment of an IA Assessment Coordinator. The IA Assessment Coordinator's role is to be the principal point of contact between the Department and the Assessment Team and with CESC. Despite the fact that in an Assisted IA Assessment the Assessment Team Members are part of the Department, they will not have the time during the Assessment to discharge this role. Guidance on what the IA Review Coordinator is required to do as part of the CESC IA Benchmarking Service is on the CESC website and much of that detail is relevant to the conduct of an Assisted IA Assessment.

REQUESTING ASSISTANCE FROM CESC

9. The IA Assessment Co-ordinator, should complete an IA Review Request Form (available from the CESC website) and should submit this to the IA Benchmarking Team Leader (IABTL) at CESC. On receipt, the IABTL will contact the IA Assessment Coordinator to discuss what level of assistance would meet the Department's requirements. In the majority of circumstances this would be limited to four days of effort from an experienced IA Reviewer – one days preparatory assistance to the IA Assessment Coordinator, one day attending the Planning Meeting and two days support to the Assessment Team (normally on the first day and during the Report Writing and Feedback stage)

SELECTING IA ASSESSMENT TEAM MEMBERS

10. The IA Assessment Team should consist of three or four people. Each person involved needs to have some experience of IA. This can be from the perspective of information management, security, or data protection, but in all cases it is imperative that the individuals chosen can take a business orientated view of IA. At least one member of the Team should be of a sufficient grade to be able to lead the discussion when the Assessment Team need to interview members of the Departmental Board. Choosing at least one member of the Team who has experience as an OGC Gateway Reviewer would also be beneficial. One member of the Team should be designated the Assessment Team Leader (ATL), and this person does not necessarily need to be the most senior by grade, but should be the best person to perform the role.

11. The selected Assessment Team Members (ATMs) will need to be free to set aside one day for a Planning Meeting, at least one day to read IA documentation and then they will each need to be able to devote 5 consecutive, working days to the

Assessment.

12. Briefing notes for RTLs and the RTMs working as part of the CESG IA Benchmarking Service are on the CESG website and much of that detail is relevant to the conduct of an Assisted IA Assessments.

13 CESG Review Teams undergo training on both the IA Model and the policy on which it is based. Without this training, it is important that those chosen to conduct an Assisted IA Assessment are fully conversant with the IA Model and the IAAF, before the IA Assessment Planning Meeting.

THE IA ASSESSMENT PLANNING MEETING

14. The Planning Meeting is an essential part of the Review process for a number of reasons. It is likely to be the first time that the Assessment Team will have come together to discuss the Assessment and it is possible that it will be the first time that they will have met the SIRO and the IA Assessment Coordinator. It gives an opportunity for the Assessment Team to familiarise themselves with the full range of the Department's business and decide how best to approach the Assessment, as well as confirming all of the stakeholders to be interviewed.

15. A generic Agenda for the Planning Meeting is at Annex A and it is the responsibility of the ATL, in conjunction with the IA Assessment Coordinator to ensure that all of the necessary points are covered. At the conclusion of the Meeting it is essential that at least the following are determined:

- a. **Document Reading List.** A suggested list of the documents which need to be made available to the Assessment Team is at Annex B. This list will need to be adapted to match the level of IA maturity within the Department, together with the terminology which is normally used. It is the responsibility of the IA Assessment Coordinator to assemble the documentation and pass it to the Assessment Team.
- b. **Interview Schedule.** A list of suggested interviewees is at Annex C, together with a template interview schedule. It is the responsibility of the IA Assessment Coordinator to arrange for the interviews required by the Assessment Team. It is recommended that an interview briefing document is sent out to interviewees to ensure a consistent message of what the Assessment is about is communicated. (An example of a suggested briefing note is on the website)

ESTABLISHING EVIDENCE OF IA MATURITY

16. The IA Assessment should be evidence based and discussion led. It is therefore essential that the assessment Team allow sufficient time to read all of the IA documentation provided by the IA Assessment Coordinator. The existence of a document alone is insufficient to meet the IAAF requirement. ATMs are required to

UNCLASSIFIED

exercise judgement in determining the effectiveness of a particular document in delivering the required intent. Other documents may help in this regard, but frequently the effectiveness of the required outcome can only be determined through interview. Consequently whilst reading the documentation provided, ATMs should note which elements of the IAAF are satisfied and which will require interviews to provide corroborating evidence.

CONDUCTING IA ASSESSMENT INTERVIEWS

17. Interviews are an essential part of the IA Assessment process. They serve to establish the views of those who are involved in discharging the Department's IA Strategy and Policy and they provide an insight into how well the intent of the Main Board in discharging its corporate responsibility is joined up with what happens in practice within the Department.

18. Evidence collected during interviews is non-attributable and this must be made clear at the start of each interview so that interviewees feel free to speak their minds. Each interview should last about 40 minutes and therefore scheduling interviews on an hourly basis will leave 20 minutes for the Assessment Team to consider what is said during the interview.

19. Interviews can be intimidating for some people and therefore it is essential that the Assessment Team do all that they can to put interviewees at ease. Experience shows that it is better to divide the available time between interviewers, rather than each member of the Team contributing to each part of the discussion.

20. There are many ways of recording the key points from an interview, but one which has been used very successfully, is for each ATM to record individual key points on separate post-its, which can then be grouped under the six criteria of the Maturity Model. The advantage of this approach is that when the post-its are stuck on a board under the relevant criteria it becomes obvious where there is consensus in opinion, where further corroboration is required, and just as importantly, where no evidence has been found.

THE IA ASSESSMENT REPORT

21. The IA Assessment Report is prepared for the SIRO by the Assessment Team. It is confidential to the SIRO and the Assessment Team should not keep copies of the Report, or any of the material which they were provided to conduct the Assessment. A suggested format for the Report is at Annex D. Recommendations should be limited to a maximum of 12 and should be pitched at a level appropriate to the seniority of the SIRO.

22. A key part of the Report is the assessment of IA maturity. This is made using a R/A/G assessment against each of the six criteria which make up the Model at each of the five levels, until the assessment is Red. The result is a grid which looks like the following:

UNCLASSIFIED

Maturity Model Criteria	Assessment of Maturity Against Level				
	1	2	3	4	5
Leadership and Governance.	GREEN	AMBER	RED		
Training, Education and Awareness	AMBER	RED			
Information Risk Management	AMBER	AMBER	RED		
Through-Life IA Measures	GREEN	GREEN	RED		
Assured Information Sharing	GREEN	GREEN	RED		
Compliance	GREEN	AMBER	RED		

The R/A/G status is defined below:

- **RED** – There are major deficiencies against the performance required at this level.
- **AMBER** – There are significant deficiencies against the performance required at this level.
- **GREEN** – There are only minor deficiencies against the performance required at this level.

FEEDBACK TO CESG

23. The materials to support the use of the HMG IA Maturity Model are regularly updated. If you have any comments on how this Assisted IA Assessment Guide or any of the other information relating to the use of the IA Maturity Model, could be improved, please pass your comments to the IA Maturity Model Benchmarking Team Leader at CESG.

CONCLUSION

24. This guide to Assisted IA Assessment against the HMG IA Maturity Model has been prepared to assist SIROs in setting up and running an Assisted IA Assessment within their Department. It is based on experience gained in delivering the fully independent IA Reviews provided by the CESG Benchmarking Service.

25. An Assisted IA Assessment by its very nature can not replicate the fully independent IA Review provided by CESG, 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 – Generic Agenda for the Planning Meeting

10:00 Assessment Team Meeting – CESG Advisor to Lead:

- Introductions, purpose of day, code of conduct
- Planning for Departmental Meeting - Issues, areas of interest, report

12:00 Assessment & Departmental Introductions – IA Assessment Coordinator to Lead with SIRO

- Code of Conduct and Team working (contacts and communication),
- Purpose of Meeting and Assessment

12:30 Working Lunch

13:00 Presentation on Department – SIRO/IA Assessment Coordinator

14:00 Discussion on Issues for Assessment (ATL to Lead, assisted by CESG Advisor – SIRO in attendance)

14:30 Review Action Planning (ATL to Lead, assisted by CESG Advisor)

- Documentation to be made available
- Stakeholders and Interviews required – IA Assessment Co-ordinator propose list; Interview scheduling
- Hosting requirements/domestics

15.30 Assessment Team discussion

16.00 Close

Annex B – Suggested List of Documents for Assessment

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

- **Leadership & Governance**

- Main Board Policy Statement on IA
- TORs for SIRO, IAO, DSO and ITSO
- 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
- Information Security Policy (may form part of Departmental Security Policy or Instructions), together with any security policy audit reports.
- Details of how IAOs are discharging their responsibilities
- Written Assessment by SIRO to AO of how DHR recommendations are delivering the required change.
- Business Continuity Policy/Strategy
- Business Continuity and Disaster Management Test Report relating to IS
- 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 (Department, arm's length bodies and delivery partners) and 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 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
- Departmental list of all information assets, each with an allocated IAO
- Quarterly IA risk assessment of the Department's delivery chain
- Annual Departmental Information Risk 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
 - Details of the accreditation status of all IS used by the Department
 - 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
 - RMADS for main Departmental IS
 - Sy Ops for main Departmental IS
- **Through-Life IA Measures**
 - Details of plans to determine the IA status of all Departmental IS
 - Details of Departmental vetting process and how it is assured
 - Details of how physical security measures are implemented and 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
 - Departmental Acceptable Use Policy
 - Remote Working Policy including controls on removable media
 - IA Incident management Plan including Incident Reporting Policy
 - Forensic Readiness Plan, and details of how it has been validated
 - Departmental metrics for IA related incidents and problems
 - BC and Disaster Management Plan including details of how it is validated
 - Details of Departmental Access Management policy and practice
 - 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
- **Assured Information Sharing**
 - 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
 - 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 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

2. This may seem an enormous list, but the reading task is split between Team members depending on their experience and expertise. In addition, 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.

DRAFT

Annex C – Suggested List of Interviewees

1. The following list, gives an indication of the responsibilities of the people who will need to be made available for interview. A single person may be responsible for several of the responsibilities listed below:

- **Leadership & Governance**
 - SIRO
 - CIO
 - IAO
 - Data Controller
 - DSO
 - CE, or Head of one of the Department's arm's length bodies
 - Head of the Department's principle Delivery Partner.
- **Training, Education & Awareness**
 - The person responsible for organising IRM Training
 - The person responsible for IRM Cultural Change Plan
- **Information Risk Management**
 - The person responsible for maintaining the Department's IA Risk Register
 - Head of Accreditation
- **Through-Life IA Measures**
 - Head of HR security
 - Head of physical security
 - ITSO
 - IA Incident Manager
 - The person responsible BC & DM, particularly as it applies to IT
 - For Main IS:
 - IS Service Manager (if outsourced those on both side of deal responsible for delivery of assured IS facilities)
 - Chair of Security Working Group
 - Accreditor
- **Assured Information Sharing**
 - The person responsible for information sharing external to the Department
 - The person responsible for Departmental security architecture
 - The person responsible for Departmental network security management & protective monitoring
- **Compliance**
 - Head of Audit Committee
 - Head of Internal Audit Unit
 - Head of any IT audit team.

2. This list is not exhaustive, but it gives an indication of those senior managers who will need to be interviewed. It may be that to get the detail required, particularly on the more technical issues, specialists will need to be interviewed, but ideally the Team will wish to interview managers who can take a broad view of the issues being discussed.

Annex D – Suggested Format for Assisted IA Assessment Report

[Insert security classification (in capitals) or UNCLASSIFIED]

INFORMATION ASSURANCE **ASSISTED ASSESSMENT REPORT**

Department: [Insert name]
Agency or NDPB: [Insert name]
SIRO: [Insert name]
Version number: [Insert Draft 0.1,0.2,0.3 or Final 1.0]
Date of issue to SIRO: [Insert date]
IA Assessment dates: [Insert dates dd/mm/yyyy to dd/mm/yyyy]

IA Assessment Team Leader: [Insert name of team leader]
IA Assessment Team Members: [Insert name of team member]
[Insert name of team member]
[Insert name of team member]

[Insert security classification (in capitals) or UNCLASSIFIED]

[Insert security classification (in capitals) or UNCLASSIFIED]

Background

[Insert two or three short paragraphs giving details of the organisation that is subject to the Assisted IA Assessment and any specific factors which impact on the approach taken by the Department in achieving IA Maturity]

Purpose of the Assisted IA Assessment

The primary aim of the Assisted IA Assessment is to provide a rough and ready assessment of the extent to which effective IA risk management processes and procedures are embedded within a Department. This should assist the Department in developing a programme of work to improve the processes around IA risk management. An Assisted IA Assessment does not assess the effectiveness of particular IA security measures on specific systems, nor does it produce an estimate of how secure a Department's information might be.

The Assisted IA Assessment is based on an assessment of maturity against the HMG IA Maturity Model. As such the Assisted IA Assessment is not a formal audit against a set of standards, but it is an evidence based assessment of the levels at which a Department is operating in each of the six core IA processes contained within the IA Maturity Model.

Conduct of the Assisted IA Assessment

This Assisted IA Assessment was carried out from [Insert: Date 1] to [Insert: date 2] at [Insert: location of review]. The team members are listed on the front cover.

The people interviewed are listed in Annex A.

The Assessment Team would like to extend its thanks to the SIRO and other members of the Department who have contributed during the week by giving their time to interview sessions. Their support and openness has contributed to the Assessment Team's understanding and the outcome of this Assessment.

We would also like to express our appreciation, in particular to [Insert: name of the Point of Contact], for the help provided in setting up the Assessment and for ensuring that the programme of interviews ran smoothly.

[Insert security classification (in capitals) or UNCLASSIFIED]

[Insert security classification (in capitals) or UNCLASSIFIED]

Conclusions

The IA Assessment Team finds that [Insert a brief statement outlining the Assessment Team’s view of the IA status of the Department]

[Insert instances of significant good practice found, especially those that may be transferable to other Departments]

A summary of recommendations can be found in Appendix B.

Status

The overall status of IA maturity of the organisation is assessed to be:

Maturity Model Criteria	Assessment of Maturity Against Level				
	1	2	3	4	5
Leadership and Governance					
Training, Education and Awareness					
Information Risk Management (IRM)					
Through-Life IA Measures					
Assured Information Sharing					
Compliance					

The R/A/G status is defined below:

- **RED** – There are major deficiencies against the performance required at this level.
- **AMBER** – There are significant deficiencies against the performance required at this level.
- **GREEN** – There are only minor deficiencies against the performance required at this level.

[Note whether the recommendations of any earlier IA Assessments or Reviews have been implemented, and if not, comment on the justification for any alternative course of action]

[Insert security classification (in capitals) or UNCLASSIFIED]

[Insert security classification (in capitals) or UNCLASSIFIED]

Findings and Recommendations

1: Leadership, Governance and Training

Recommendation x:

2: Information Risk Management

Recommendation x:

3: Through-Life IA Measures

Recommendation x:

4: Assured Information Sharing

Recommendation x:

5: Compliance

Recommendation x:

[Insert security classification (in capitals) or UNCLASSIFIED]

[Insert security classification (in capitals) or UNCLASSIFIED]

ANNEX B

Summary of Recommendations

Ref. No.	Recommendation
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	

Add or delete rows as required.

[Insert security classification (in capitals) or UNCLASSIFIED]