

UNCLASSIFIED



Guide to IA Self-Assessment Using the HMG IA Maturity Model and Assessment Framework

(Version 0.6 dated 13 October 2008)

© Crown Copyright 2008 – All Rights Reserved

UNCLASSIFIED

UNCLASSIFIED

Document History

Version	Date	Description
0.2	30 Sep 08	Initial draft
0.5	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 Self-Assessment 1

Setting Up an IA Self-Assessment 2

The IA Review Planning Meeting 2

Establishing Evidence of IA Maturity 3

The IA Review Report 3

Feedback to CESH 4

Conclusion 4

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

Annex B – Suggested Format for IA Review Report B-1

References

1. HMG Information Assurance Maturity Model and Assessment Framework dated 30 September 2008
2. HMG Security Policy Framework (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 (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, either using entirely their own resources, or with some limited support from CESC staff.
4. The Aim of this document is to provide guidance to SIROs in conducting an IA Self-Assessment.

APPROACH TO IA SELF-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 are likely to 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 self-assessment is to conduct a more formal IA Review designed to mirror the practices and procedures used by the independent review teams who deliver the CESC IA Benchmarking Service. Assistance in setting up such a review is available from CESC and further information about the CESC Assisted IA Assessment is available on the CESC website. However, it is appreciated that time and resources might not be available to conduct such a review and the remainder of this document providing specific guidance on how to conduct an IA Self-Assessment.

SETTING UP AN IA SELF-ASSESSMENT

7. An IA Self-Assessment can by its very nature be initiated by anyone with IA responsibilities within the Department. However, given that key to the successful implementation of IA is the effective engagement of members of the Departmental Management Board, it is recommended that the Senior Information Risk Owner (SIRO) is involved in commissioning the IA Self-Assessment Review and receiving the Report at the conclusion of the process.

SELECTING IA REVIEW TEAM MEMBERS

8. The IA Review Team should ideally 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. One member of the Team should be designated the Review Team Leader (RTL), and this person does not necessarily need to be the most senior by grade, but should be the best person to perform the role.

9. The selected Review Team Members (RTMs) will need to be free to:

- a. Meet with the other Team members at a Review Planning Meeting
- b. Set aside sufficient time to read the IA documentation (See Annex A for a list of recommended documents)
- c. Devote one day to a workshop with the other Team members during which the IA Assessment is made and the Report written.

10. 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 IA Self Assessment Review are fully conversant with the IA Model and the IAAF, before the IA Review Planning Meeting.

THE IA REVIEW PLANNING MEETING

11. The Planning Meeting is an essential part of the Review process as it is likely to be the first time that the Review Team will have come together to discuss the Review and clarify any issues they might have.

12. 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 Review Team members and when the IA Assessment Workshop is to be held.

13. A suggested list of the documents which need to be made available to the Review Team is at Annex A. 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.

ESTABLISHING EVIDENCE OF IA MATURITY

14. The Review Team should meet for a workshop during which evidence against the Maturity Model and the IAAF should be considered, and a status for the organisation agreed. It may be necessary during the course of the workshop for a team member to break out to contact other members of the organisation for additional information or to gain clarification of evidence gained from the documentation. By the end of the workshop, a report showing the organisation's status against the various business criteria and levels should be produced, with justification for each assessment and the Review Team may make recommendations where appropriate.

15. The IA Review should be evidence based. It is therefore essential that the Review Team allow sufficient time to read all of the IA documentation. The existence of a document alone is insufficient to meet the IAAF requirement. Review Teams are required to exercise judgement in determining the effectiveness of a particular document in delivering the required intent. Other documents may help in this regard, but it is likely that those conducting the Review will have to exercise their subjective judgement based on their knowledge of how the Department operates.

THE IA REVIEW REPORT

16. The IA Review Report is prepared for the SIRO by the Review Team. It is confidential to the SIRO and the Review Team should not keep copies of the Report, or any of the material with which they were provided to conduct the Review. A suggested format for the Report is at Annex B. It is essential that any recommendations made should be pitched at a level appropriate to the seniority of the SIRO.

17. 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:

Maturity Model Criteria	Assessment of Maturity Against Level					Justification of Assessment & Recommendation
	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			

UNCLASSIFIED

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

18. The materials to support the use of the HMG IA Maturity Model are regularly updated. If you have any comments on how this IA Self 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

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

20. An IA Self-Assessment by its very nature cannot 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 – Suggested List of Documents for Review

1. The precise list of documents that will need to read by the 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

UNCLASSIFIED

- 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.

Annex B – Suggested Format for IA Review Report

RESTRICTED (when completed)

INFORMATION ASSURANCE
SELF-ASSESSMENT REVIEW REPORT

Department: (Insert Name)
SIRO: (Insert Name)
Version number: (Insert Version Number)
Date of issue to SIRO: (Insert Date)
IA Review Workshop Date: (Insert Date)

IA Review Team Leader: (Insert Name)
IA Review Team Members: (Insert Name)
(Insert Name)

RESTRICTED (when completed)

RESTRICTED (when completed)

Background

Insert a short paragraph giving the background to the commissioning of the IA Self-Assessment

Summary

Summarise the main findings of the Review Team to include points of best practice, areas of weakness and key recommendations.

Purpose of the IA Review

The primary aim of the IA Self-Assessment Review 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 IA Self-Assessment Review 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 IA Self-Assessment is based on an assessment of maturity against the HMG IA Maturity Model. As such the IA Review 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 IA Review

This IA Self assessment Review was carried out on (Insert Date) at (Insert Location). The IA Review Team members are listed on the front cover. The Review Team's assessment is based on an extensive document review supplemented by their subjective judgement based on their experience of working within the Department.

RESTRICTED (when completed)

RESTRICTED (when completed)

Status

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

Maturity Model Criteria	Assessment of Maturity Against Level					Justification of Assessment & Recommendation
	1	2	3	4	5	
Leadership and Governance.						
Training, Education and Awareness						
Information Risk Management						
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.

Recommendations

RESTRICTED (when completed)