

UNCLASSIFIED



2010 Cabinet Office Information Risk Report: HMG IA Maturity Model Supported Self-Assessment

(Version 1.1 dated 27th November 2009)

© Crown Copyright 2009 – 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

This document is authorised by:

P J Hooper
IA Maturity Model Benchmarking Team Leader

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 Information Risk Report 1

Using the IRR Tool 3

IRR Tool Assessment Planning Meeting 4

Establishing Evidence of IA Maturity 4

Support Available from CESH 5

Feedback to CESH 5

Conclusion 5

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

Annex B – CO IRR Tool – Example Results Grid B-1

UNCLASSIFIED

References

1. HMG Information Assurance Maturity Model and Assessment Framework Version 3.0 dated 15 October 2009
2. HMG Security Policy Framework (HMG SPF) Version 3.0 dated 20 November 2009
3. Cabinet Office Data Handling Review Report dated June 2008
4. HMG IA Standard No 6 Protecting Personal Data and Managing Information Risk
5. BS ISO/IEC 27001:2005 dated 15 October 2005
6. National Information Assurance Strategy (NIAS) dated June 2007
7. SPF and Information Risk: Annual Information Risk Report to Cabinet Office 2009/10 to be issued early in 2010

INTRODUCTION

1. On 30 September 2008 the Cabinet Office and CESG 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[3], (also available as IS6[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) which gives considerably more detail of the measures required to deliver the specific levels of maturity on which the Model is based.
3. In 2009 Ministerial Departments were required to provide an annual report to Cabinet Office using the IAMM and IAAF and for 2010 the decision has been made to extend this requirement to include Non-Ministerial Departments. The Cabinet Office is required to provide a report to Parliament on the progress being made by Central Government Departments on this issue as a whole and these departmental reports will be used to inform the process of completing this Report to Parliament.
4. The Aim of this document is to give details of how the Information Risk Report (IRR) Tool is to be used as part of the overall IRR to the Cabinet Office and provide guidance on the CESG IA Supported Self-Assessment Service, which is designed to provide limited support from CESG staff to assist the SIRO in making the assessments that the Tool is designed to record. It is anticipated that Departments will draw heavily on this assessment for their annual report and in their Statement on Internal Control. Note that this document does not cover all aspects of the content of the IRR, which is covered in full within the Guidance produced by IS&A[7].

CABINET OFFICE INFORMATION RISK REPORT

5. The 2010 Cabinet Office IRR is required to be completed by each Department and submitted by the SIRO to Information Security and Assurance (IS&A) by 14 June 2010. The results from Departments will then be collated by IS&A to form the basis of evidence on which a report to Parliament will be prepared and submitted. A key part of the IRR consists of populating an IRR Tool with details of what the Department has done to implement effective IA. The use of such an evidence-based process should provide a reliable indicator of year-on-year progress.
6. The IRR Tool is based on a Microsoft Excel Workbook consisting of Worksheets that contain detail extracted from the IAAF in the form of a series of IRM requirements against which the Department is required to provide an assessment of the degree to which the Department complies, together with details of completion. An example from one of the Worksheets is as follows:

UNCLASSIFIED

TRAINING, EDUCATION & AWARENESS

Serial	Requirement	Level 1 Score	Requirement	Level 2 Score	Requirement	Level 3 Score	Evidence/ Comment
IRM Training - Personal Data							
1a	Every member of the Department, its delivery partners and 3rd party suppliers who have access to personal data undergoes an annual session of information risk awareness training	D	0	Regular annual refresher training is undertaken and details of the % of staff who have undergone training is collected.	D	0	
1b		DP	0		DP	0	
1c		3rd	0		3rd	0	
2a	A process is in place to assure the SIRO that every member of staff within the Department, its delivery partners and 3rd party suppliers who have access to personal data receives information risk awareness training on induction and annually thereafter.	D	0	Effective mechanisms are in place to ensure that all those who should have undertaken the compulsory training are trained.	D	0	
2b		DP	0		DP	0	

7. Where the Department has an obligation to ensure that its Delivery Partners and 3rd Party Suppliers (these categories are defined in an Appendix to Reference 7 - or alternately prior to publication available on request from datareview@cabinet-office.x.gsi.gov.uk) meet the specified requirement separate scores are required to be entered. The scoring regime is as follows:

N/A	Not applicable. Note: this item will not be included in the total score calculations. It should not be used in place of a genuine score of zero.
0	Issue not recognised, or not on the agenda for action.
1	A plan to deliver the requirement is under construction but with key issues yet to be resolved e.g. any of the following: <ul style="list-style-type: none"> - delivery not started - not endorsed at appropriate level - resources (fiscal and human) yet to be formally committed - no formal governance structure to deliver the plan - a plan is in progress with uncontrolled risks that threaten delivery.
2	A fully endorsed and resourced project or programme (or similar formal process) is underway to deliver the plan, under a recognised formal governance structure (e.g. OGC guidelines) with achievable timescales, and with a fully managed risk profile.
3	Action complete

8. The worksheets are constructed so that when completed, the % of IRM Requirements falling into each of the assessment categories is calculated. The workbook then summates the results against each of the six categories of the IA Maturity Model and presents these back in three ways:

- a. As an assessment of the Department's compliance against the mandatory DHR requirements listed in IS6[4].

UNCLASSIFIED

b. As an overall assessment of compliance against the IA Maturity Model at each of the first three levels of the Model. An example of how the results are provided is at Annex B.

c. As an assessment that enables each Department to determine and report its progress against the mandatory requirements of Security Policy No:4 (Information Security and Assurance) of the HMG Security Policy Framework[2].

9. This mechanistic approach to providing an overall assessment is necessary, but not sufficient and must be accompanied by a commentary from the SIRO against each category where this would be helpful in describing the Department's assessments.

USING THE IRR TOOL

10. Whilst a significant amount of detailed information is required to complete the entries required by the IRR 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.

11. 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.

12. 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.

13. 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. Devote one day to a workshop with the other Team members during which the IRM Assessment is made and the IRR Tool populated with data.

14. Experience gained from running these assessments in 2009 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

UNCLASSIFIED

assessment prior knowledge of the HMG IA Maturity Model and the IAAF is essential. CESC and CSIA are running training sessions for individuals involved in these assessments and Departments are strongly encouraged to take full advantage of these events. As a minimum, it is essential that staff have had the opportunity to read this Guide and understand the make-up of the IRR Tool, prior to the Assessment Planning Meeting, so that they are aware of the breadth and depth of the task, they are to undertake.

IRR TOOL ASSESSMENT PLANNING MEETING

15. 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.

16. 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 IRR Assessment 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 level of IRM maturity within the Department, together with the terminology which is normally used.

17. 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. CO Guidance [7] includes an extract from the IRR Tool 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

18. The Assessment Team should meet for a workshop during which evidence against the Requirements set out in the IRR Tool should be considered, and a status for the 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 measures with a commentary where considered applicable.

19. The IRR 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 contained in the IRR. The Assessment Team will be 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 Assessment will have to exercise their subjective judgement based on their knowledge of how the Department operates.

SUPPORT AVAILABLE FROM CESG

20. Support to Departments is available from CESG. Members of CESG have been trained in the use of the IA Maturity Model and IAAF, and the IRR 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 IRR 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.

21. To engage the services of a member of CESG to assist in the completion of the IRR Assessment, a member of the Department should complete the IAMM Assessment Services and Application Form available from the CESG website and submit this to the IACS Delivery Office at CESG. On receipt, the IA Maturity Model Benchmarking Team Leader will make contact with the Department with a view to determining the availability of CESG staff to meet the Department's requirements.

FEEDBACK TO CESG

22. 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 IRR Tool, 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

23. This Guide to the Cabinet Office IRR: HMG Supported Self-Assessment has been prepared to assist SIROs in setting up and running an Assessment within their Departments and to provide details of the CESG 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 CESG Benchmarking Service.

24. An IA Supported Self-Assessment designed to complete the IRR Tool 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 - Suggested List of Documents for Assessment

1. The precise list of documents that will need to 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 will 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.

- **Leadership & Governance**

- Main Board Policy Statement on IA
- TORs for SIRO, IAO, DSO and ITSO
- 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
- 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 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
- 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 including details of operations and data located off-shore
 - 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
 - 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 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
 - Departmental Acceptable Use Policy
 - Remote Working Policy including controls on removable media
 - IA Incident management Policy including Incident Reporting Policy
 - Forensic Readiness Plan, and details of how it has been validated
 - Departmental 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
 - 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**
 - 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

Annex B – 2010 CO IRR Tool - Example Results Grid

FULL INFORMATION RISK MATURITY ASSESSMENT AGAINST ALL CRITERIA			
Weighted	Level 1	Level 2	Level 3
Leadership & Governance	100%	96%	82%
Training, Education & Awareness	97%	92%	75%
Information Risk Management (IRM)	99%	97%	89%
Through-Life IA measures	98%	98%	75%
Assured Information Sharing	95%	79%	56%
Compliance	100%	100%	97%

IAMM Colour coding Rule Set			
Green		95-100%	Compliant, or on track to be compliant
Amber		80-94%	
Red		<80%	