

UNCLASSIFIED



HMG Information Assurance Maturity Model and Assessment Framework

(Version 3.0 dated 14 October 2009)

© Crown Copyright 2009 – All Rights Reserved

UNCLASSIFIED

UNCLASSIFIED

Document History

Version	Date	Description
0.6	6 Aug 08	Initial draft made available on CESG website
0.8	28 Sep 08	Re-formatted
1.0	30 Sep 08	Formal Release
2.0	20 Feb 09	Incorporating SPF and Digital Continuity Requirements
2.0.5	10 Oct 09	Incorporating comments from limited external circulation.
3.0	14 Oct 09	Enhancing alignment with ISO/IEC 27001:2005, introduction of more section headings and guidance on how to achieve maturity.

This document is authorised by:

P J Hooper
IA Maturity Model Benchmarking Team Leader

This document is issued by Cabinet Office and 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

IA Maturity Model & Assessment Framework 1

IA Maturity Model 1

IA Assessment Framework 3

Using the Model and Assessment Framework 4

Developing the Model and Assessment Framework 4

Achieving IA Maturity 5

Conclusions 6

Annex A – IA Maturity Model A-1

Annex B – IA Assessment Framework B-1

Leadership and Governance B-1

Training, Education and Awareness B-6

Information Risk Management B-9

Through-Life IA Measures B-14

Assured Information Sharing B-22

Compliance B-25

UNCLASSIFIED

References

1. HMG Security Policy Framework (HMG SPF)
2. Cabinet Office data Handling Review Report dated June 2008
3. HMG IA Standard No: 6 Protecting Personal Data and Managing Information Risk dated October 2008
4. ISO/IEC 27001:2005 dated 15 October 2005
5. National Information Assurance Strategy (NIAS) dated June 2007
6. HMT Risk Management Assessment Framework Version 2.0 dated 29 October 2004
7. See OGC Website – www.ogc.gov.uk
8. Managing Information Risk – A Guide for Accounting Officers, Board Members and SIROs produced by the National Archive dated March 2008
9. Guidance on the FY 08/09 Annual Information Risk Report to Cabinet Office dated February 2009

INTRODUCTION

1. Information is a key asset within Government, but it can also become a key liability. Departmental Accounting Officers (AOs), through their Senior Information Risk Owners (SIROs) and their Information Asset Owners (IAOs), are accountable for the adequate protection of information which is collected, processed and stored within their Departments. To do so they must put in place effective Information Risk Management (IRM) processes and procedures. They will also need to be assured that these arrangements are sufficient to reveal what impact the range of programmes in Transformational Government will have on their Department's information risk.
2. The growing need for Departments to share information in response to the Transformational Government and Shared Services initiatives means that common standards need to be applied across Government. This is to ensure that those accountable and responsible for IRM can have confidence that the information will be handled appropriately when it is passed to others. The HMG Security Policy Framework (HMG SPF)[1] lays down mandatory standards to be applied by Departments. However, in addition to these standards there is a body of best practice measures, which if applied will assist Departments in discharging their obligations to enact effective IRM.
3. To assist SIROs in putting in place an effective change programme to improve IRM an Information Assurance (IA) Maturity Model has been created. This Model incorporates the mandatory information related requirements of the HMG SPF, which includes the requirement to apply the 2008 Data Handling Review[2], (also available as IS6 [3]), and it is aligned with the ISO/IEC 27001:2005 Standard[4] and the broader outcomes sought by the National IA Strategy[5].
4. The Model is underpinned by an IA Assessment Framework (IAAF) which gives considerably more detail of the measures required to deliver the levels of maturity contained within the Model. In addition, the IAAF has been designed for use by independent IA Review Teams as part of an independent IA Benchmarking Service delivered by CESG. However, the IAAF can also be used by Departments that wish to conduct IA self-assessments, either by themselves, or with some limited support from CESG staff.

IA MATURITY MODEL

3. The IA Maturity Model (see Annex A) has been designed to help SIROs establish a comprehensive programme of work (see Paragraph 15) to achieve progress through clearly identifiable milestones towards the achievement of three main IA goals:
 - a. **Embedding IRM Culture within the Organisation:**
 - The need to assure information as a key business asset is embedded within the culture of the Department, its delivery partners and its 3rd party suppliers.
 - Procedures are in place so that the Main Board is able to understand and

UNCLASSIFIED

manage the information risk to which the total organisation¹ is exposed

- The agreement of external stakeholders is reached on the treatment of information risks, particularly when they will impact on the delivery of Shared Services and Transformational Government objectives

b. **Implementing Best Practice IA Measures:**

- Through-life measures are implemented to assure all information within the Department, its delivery partners and its 3rd party suppliers, so that changes can be made to processes and systems to match the tempo of the business without introducing undue vulnerabilities
- Systematic monitoring of networks, systems and boundary points is undertaken so that the Department can effectively detect and respond to vulnerabilities, threats and incidents in a timely manner, thus reducing potential adverse impacts to its business to an acceptable level

c. **Effective Compliance:**

- An effective compliance regime is implemented across the Department, its delivery partners and its 3rd party suppliers, to ensure the Department's compliance with legislation and the proper management of information risks in accordance with HMG SPF and national policy & standards
- Internal and external review provides independent assurance to the SIRO and the AO that the compliance processes are working effectively

4. Achieving maturity towards these goals assisted by the IA Maturity Model will enable Departments to generate greater trust in their information systems and processes, both internally and between Departments. This will be particularly important in the context of Shared Services, and the issues surrounding shared versus individual risks to information, whether it belongs to the Government or the citizen.

5. Each level of the Model is designed to build on the achievement of the preceding levels; as such the measures are cumulative:

- **Level 1 – Initial**. At this level the Main Board is aware of the criticality of IA to the business and of its legal requirements. Consequently it has initiated activity to address areas of immediate weakness and has policy in place to guide the improvement process. It also applies this policy to all new Information Systems (IS). The majority of the DHR mandatory measures are built into Level 1 of the IA Maturity Model, the few that are at Level 2 are those that require more time to implement before a Department can be fully compliant. Hence, putting in place measures to deliver this level of IA maturity will result in delivering all of the near-term DHR requirements.
- **Level 2 – Established**. At this level IA processes are institutionalised within the Department, its delivery partners and its 3rd party suppliers. The Main Board has endorsed the adoption of a strategic approach to improving the IA maturity of the organisation. A programme of targeted IA education and training has been initiated and work to inculcate an appropriate IRM culture

¹ The Department, its delivery partners (some of whom operate at arm's length) and 3rd party suppliers. Refined definitions of these terms will be published by IS&A during autumn 2009.

UNCLASSIFIED

has started. Discovery work has been undertaken and the IA status of the entire Department's IS and related processes have been determined. A definitive list of business critical IS has been endorsed by the SIRO and Chief Information Officer (CIO). Based on this list and the discovery work, a fundamental requirement at this level, is for the SIRO to have personally made and gained approval for a business case to the board of directors for a targeted programme of work to improve the understanding and control of information risk. Within most Departments progress to Level 2 will require extensive work to be undertaken.

- **Level 3 – Business Enabling.** At level 3 IA awareness across the organisation has increased leading to a measured improvement in IRM behaviours at all levels within the organisation, its delivery partners and its 3rd party suppliers. Building on the framework of IA processes rolled out at Level 2, Level 3 will be achieved when all critical areas of the business are subject to a robust IA regime.
- **Level 4 – Quantitatively Managed.** At level 4 there is evidence to show that staff attitudes and behaviours towards assuring information are aligned to the needs of the business. The regime established at level 3 for critical areas of the business is extended to embrace the whole business. As a consequence the SIRO has the IA metrics available to take an informed approach to managing the risk to the information used by the business.
- **Level 5 – Optimised.** Level 5 is achieved when IA is fully integrated as an aspect of normal business and the culture of the business is such that at all levels of management, IA is judged to be a business enabler.

6. The IA Maturity Model and the IAAF are living documents which will be updated in line with changes in the threat, changes in the HMG SPF and as a result of lessons learned from applying them to Departments.

7. The top-level statements contained in each box of the Model are by necessity very brief. To gain a full understanding of what is required to satisfy a particular Level; reference has to be made to the IAAF.

IA ASSESSMENT FRAMEWORK

8. The IAAF (See Annex B) provides specific details of the measures which are expected to be in place within Departments seeking to meet the top level statements of maturity contained within the IA Maturity Model. The Framework has been laid out in a similar manner to the HMT Risk Management Assessment Framework [6], but modified to follow the approach taken in the Work Books produced by the OGC as part of their Gateway Review process [7]. This modification enables the IA Maturity Model and the IAAF to be used as an integral part of an IA Review Process.

9. The contents of both the IA Maturity Model and IAAF have been drawn from a variety of sources. They embody the relevant HMG SPF mandatory policy requirements which includes the requirement to apply the 2008 DHR [2], (also available as IS6 [3], together with material drawn from the Managing Information Risk Guidance document [8] produced by the National Archives. They are also aligned with the requirements of the Information Security Management System (ISMS) embodied in ISO/IEC 27001:2005.

UNCLASSIFIED

However, it must be noted that the detail included within the IAAF is there as a guide of best practice and will need to be interpreted to meet the specific business needs of any particular Department.

10. Recognising that Departments may require more specific guidance on implementing some of the more technical IA controls mentioned in the IAAF, CESC is in the process of developing guidance material, which will be promulgated and linked to the IAAF in due course.

USING THE IA MATURITY MODEL AND ASSESSMENT FRAMEWORK

11. Included within the DHR mandatory requirements and therefore embedded within the main body of the IA Maturity Model is a range of internal reporting and compliance mechanisms, which are aimed at establishing and maintaining clear management responsibility and accountability for IRM within Departments. These arrangements should facilitate the collection of the information required annually by the AO for potential inclusion in the Statement of Internal Control (SIC) and Departmental Report.

12. Departments are encouraged to use the IA Maturity Model and IAAF to establish the programmes of work needed to achieve IA maturity and also to conduct self-assessment IA reviews². CESC will also provide limited support to Departments who wish to conduct their own IA Reviews and details of the “CESG Assisted Assessment Service” are available on the CESC website. However, to achieve an objective assessment of IA maturity an external IA Review will need to be undertaken and details of how a Department can arrange for such a Review as part of the “CESG IA Benchmarking Service” are included on the CESC website.

13. Departments were required to use the IA Maturity Model and IAAF in making their annual Information Risk Report (IRR) to the Cabinet Office in 2009 [9] and the intention is that it will be used again in 2010, but the CO Guidance has not yet been produced. Guidance on the Supported Self Assessment Service, together with the 2009 IRR Tool³, are also on the CESC website. The intention is to have the 2010 IRR Tool available in a final version in early November 2009.

DEVELOPING THE MODEL AND ASSESSMENT FRAMEWORK

14. As part of the process of validation of the IA Review Process, evidence derived from IA Reviews and Assessments conducted in 2009 has been used to refine the Model and IAAF. However, Cabinet Office – Information Security & Assurance (IS&A)⁴ and CESC recognise that further refinement is necessary and would welcome considered feedback, which will help develop the IA Maturity Model and IAAF further.

² To assist Departments CESC have produced a “Guide to Conducting a Self Assessment IA Review” which is available through the CESC website.

³ The 2009 CO IRR Tool includes details of the correlation between entries in the Tool and the mandatory Information Security and Assurance requirements of the SPF, together with the specific requirement of the DHR embodied in IS6.

⁴ Formerly known as CSIA

ACHIEVING IA MATURITY

STRATEGIC APPROACH

15. The contents of the IA Maturity Model and Assessment Framework are based on the following strategic approach:

- **Policy** - A policy is produced to address an issue of concern.
- **Strategy** – A strategy is produced to show how a policy, or a number of policies, are to be enacted in the business over a period of time.
- **Programme** – A programme of work is put in place under formal programme management controls to bring about the change(s) detailed in the Strategy.
- **Compliance** – A compliance regime is established to assure senior management that the strategic approach is achieving the desired outcomes in the business.
- **Audit** – Both internal and external audit are used to assure the effectiveness of the compliance regime.

16. This more strategic approach to achieving IA maturity has been adopted because in large organisations, such as Government Departments, a more piecemeal, system by system, approach:

- a. Does not normally provide senior management with an accurate picture of the information risk which is being taken by the organisation.
- b. Can conceal significant, systemic enterprise-wide information risks.
- c. Does not usually provide sufficient evidence to support strategic investment in IA.
- e. Tends to prevent organisations from making savings through economies of scale.

17. Thus a key step to any organisation wishing to improve its IA maturity using the IA Maturity Model and Assessment Framework is to adopt this or a similar strategic approach.

DEVELOPING AN IA STRATEGY

18. An effective strategy aimed at improving the IA maturity of an organisation can be readily derived from the contents of the IA Maturity Model and the Assessment Framework. The headings used throughout the IAAF provide a template of the issues that should be included.

19. There is no pre-determined level of maturity required of departments. It is a business decision what level to aspire to. However, departments should note that the application of effective IA controls to business critical systems is introduced at level 3,

and this therefore may well be considered a business critical goal. Departments should also note that there are some very important steps to effective IRM embedded in Level 4 of the IA Assessment Framework, particularly with regard to providing effective metrics to the SIRO and the Main Board, without which the ability of senior management to take effective decisions will be hindered.

CONCLUSIONS

20. The IA Maturity Model and IAAF have been developed to assist Departmental SIROs establish and monitor an effective programme of work to change the culture and approach to IRM within Departments so that the benefits of the HMG Transformational Government and Shared Services initiatives can be achieved in an assured and cost-effective way.

21. Use of the IA Maturity Model and IAAF by IA Review Teams will provide an objective assessment of the IA maturity of a Department across the wide range of disciplines and help to identify where additional work may be required to achieve the desired level of maturity.

UNCLASSIFIED

Annex A: IA MATURITY MODEL

	Process	Level 1 – Initial Awareness of the Criticality of IA to the Business and Legal Requirements	Level 2 – Established IA Processes are Institutionalised	Level 3 – Business Enabling IA Processes are Implemented in Critical Areas of the Business	Level 4 – Quantitatively Managed The Number of Corporate Exceptions to Implementing IA Processes is Known & Reported	Level 5 – Optimised Responsive IA processes are integrated as Part of Normal Business
Embedding Information Risk Management (IRM) Culture Within Department	Leadership & Governance	Main Board recognition that information is a vital business asset and that IA is an integral requirement of corporate governance. Board commitment to effective IA is promulgated in a top-level policy statement. Appointment of a SIRO on the Main Board and Information Asset Owners throughout the Department taking responsibility for their assets. Publication of an Information Charter.	Board members understand and accept their responsibility for the effective application of IA measures across the Department. The Board has endorsed a Departmental IA Strategy as part of an overall Information Management Strategy and has put in place an accountable IA governance regime to assure the effective use of information to support the business.	The Main Board is exercising due diligence with regard to the effective discharge of IA within the Department. Main Board members are proactively engaged in leading and championing IA awareness across the Department so that the essential behavioural changes needed to embed the Board's policy become rooted in the culture of the Department.	Main Board monitors progress towards embedding IA policy across the Department and re-directs effort where appropriate to deliver its strategic intent.	The need to assure the Department's Information and that of its external stakeholders as a key business asset is fully embedded within the Departmental culture and is subject to a regime of continuous improvement.
	Training, Education & Awareness	A programme of annual information risk awareness training is instituted for all who have access to personal data within the Department its delivery partners and 3 rd party suppliers. A Departmental cultural change plan is implemented.	All members of the Department undergo annual risk awareness training. A programme of targeted IA education and training is instituted. Staff behaviours are measured and trends analysed. Progress against the cultural change programme is managed and reported to the SIRO.	A programme of pre-appointment training is instituted for key staff and all existing key staff are trained. A sustained improvement in staff awareness of their IA responsibilities is achieved.	Accurate details of the training received by all staff are collated and reported to the SIRO. Staff surveys show that staff attitudes and behaviours towards assuring information are aligned to the needs of the business.	
	Information Risk Management (IRM)	A comprehensive information risk policy is in place. The Department's information risk appetite is clearly articulated. Information risks with appropriate owners and managers are identified within risk registers at the strategic level. All new IS are subject to an effective accreditation process, where appropriate Privacy Impact Assessments are used and effective contract mechanisms are used to apply IA through life. The Department's approach to addressing information risks is agreed with the Department's external stakeholders, where applicable.	The Accreditation status of all existing IS is determined and the information risks are identified within risk registers for all accredited in-service IS. A risk based programme of work is initiated to rectify any Accreditation shortfall where this is required to support the business need. A process is in place to escalate information risks through the Department's management structure for effective decision making within the Department, its delivery partners, and with external stakeholders.	All IS that are critical to the business have been subject to Accreditation and the Department has effective information risk management processes in place to manage the residual risks and the related, systemic IA risks.	For all IS, the residual risks that are to be tolerated are quantified and the Main Board is fully aware of the total level of information risk and systemic IA risk the Department is carrying and ensures that the risks are managed to assure the Integrity, Availability and Confidentiality of key business information.	
Implementing Best Practice IA Measures	Through-Life IA Measures	The requirement for taking a coordinated and systematic approach to through-life IA measures is understood and plans exist to determine the status of existing IS. All new IS are subject to through-life IA measures to deal with the full range of vulnerabilities and threats to information, including those arising from personnel behaviour, business process, natural disaster, malicious intent and obsolescence. The Department has a Forensic Readiness Policy.	The status of the through-life IA measures employed across the Department is determined and gaps are identified. A risk based programme of work is initiated to address the identified weaknesses in the technical, personnel, physical and procedural aspects of assurance, where this is justified by the business need.	Systematic, through-life processes are in place to assure all IS which are critical to the Department's business. Regular technical and operational risk reviews are undertaken and an effective process is in place to verify that remedial work is completed in a timely manner.	Level 3 processes are extended to embrace all of the Department's IS. Details of the IS that are not maintaining effective IA measures are known and are reported to the Main Board. Metrics on all IA related incidents and problems are produced and reported	Incident and problem management processes adapt to new risks and problems. The need to maintain the through-life assurance of IS becomes embedded across the Department so that changes can be made in IS to match the business tempo, without introducing undue vulnerabilities.
	Assured Information Sharing	The requirements for sharing information across the Department's boundaries are identified and arrangements are in place to work with external stakeholders to achieve shared IA objectives. The need to understand and control how IS interact with one another both internally and externally is acknowledged and work to implement IA control mechanisms is implemented.	Network boundaries are defined and policies for sharing information across these boundaries are defined and implemented, including those with delivery partners and 3 rd party suppliers. The Department takes an enterprise-wide approach to the security of new IS and a systematic method is used to implement the control measures needed to mitigate problems when inter-connecting IS.	The business activities that are critically dependant on information sharing are known. A comprehensive protective monitoring regime is implemented to provide situational awareness and enable essential information flows to be maintained. The Department has effective processes in place to respond in a timely manner to internal and external incidents and problems so that the impact on stakeholders and on the business is controlled.	Level 3 measures are extended so that incident management moves from being reactive to proactive. The impact of incidents and problems on information sharing both internally and externally is minimised. Metrics on system and network incidents and problems, and their subsequent resolution are collected and this information is reported to the Main Board and is shared with external stakeholders.	The definition and implementation of network boundaries and the associated protective monitoring regime is continually improved to reduce the departmental and collective, shared exposure to information risk.
Effective Compliance	Compliance	A compliance regime is established to confirm the effectiveness of IRM against mandated minimum standards. The Board's Audit Committee ensures that it receives comprehensive assurance on IRM and challenges assurance, where required. The Department reports annually on IA issues.	The Department has a comprehensive IRM compliance regime. External IA Review undertaken to provide independent assessment of progress towards compliance with the HMG Security Policy Framework (SPF) and national policy & standards.	Critical IA Review and internal audit recommendations are actioned and progress tracked.	IA incident and problem management processes are fully assured by internal audit. Main Board is aware of the significant areas of the Department's non-compliance with the HMG SPF and national policy & standards. Remedial action has been commissioned.	There are no critical or significant IA audit issues. Independent assessment of the Department's approach to IA shows that it is aligned with the National IA Strategy is fully compliant with the HMG SPF and national policy & standards. It is considered to be an exemplar of best practice across HMG.

Annex B: IA ASSESSMENT FRAMEWORK

1. Leadership and Governance

Level 1 – Initial Awareness of the Criticality of IA to the Business and its Legal Requirements	Level 2 – Established IA Processes are Institutionalised	Level 3 – Business Enabling IA Processes are Implemented in Critical Areas of the Business	Level 4 – Quantitatively Managed The Number of Corporate Exceptions to Implementing IA Processes is Known & Reported	Level 5 – Optimised Responsive IA processes are integrated as Part of Normal Business
Main Board recognition that information is a vital business asset and that IA is an integral requirement of corporate governance. Board commitment to effective IA is promulgated in a top-level policy statement. Appointment of a SIRO on the Main Board and Information Asset Owners throughout the Department taking responsibility for their assets. Publication of an Information Charter.	Board members understand and accept their responsibility for the effective application of IA measures across the Department. The Board has endorsed a Departmental IA Strategy as part of an overall Information Management Strategy and has put in place an accountable IA governance regime to assure the effective use of information to support the business.	The Main Board is exercising due diligence with regard to the effective discharge of IA within the Department. Main Board members are proactively engaged in leading and championing IA awareness across the Department so that the essential behavioural changes needed to embed the Board's policy become rooted in the culture of the Department.	Main Board monitors progress towards embedding IA policy across the Department and re-directs effort where appropriate to deliver its strategic intent.	The need to assure the Department's Information and that of its external stakeholders as a key business asset is fully embedded within the Departmental culture and is subject to a regime of continuous improvement.

Goal IA responsibilities are assigned from the Main Board downwards to ensure that the need to assure information as a business asset is balanced with other business drivers at every level of the Department.

Justification Without effective top-level leadership and governance, Departments seldom properly factor IA into their activities. Short-term decisions tend to be taken without consideration of their affect on longer-term IA objectives.

LEVEL 1 – Initial - Awareness of the Criticality of IA to the Business and its Legal Requirements

Areas to Probe	Evidence Expected
<p>1.1 General</p> <ul style="list-style-type: none"> Is IA perceived to be an enabler to the business of the Department, or is it considered to be an impediment? Is IA perceived to be a specialised and technical subject, or is genuinely acknowledged to be part of the mainstream business of the Department? 	<ul style="list-style-type: none"> Board members accept the need to invest in implementing IA measures and do not look to find excuses why they should not comply with HMG policy Board members speak authoritatively about IA and its importance to the business. They may not know much about the subject, but they recognise its criticality
<p>1.2 Board Responsibilities</p> <ul style="list-style-type: none"> Do the AO and the Main Board members recognise their responsibility for IA as part of their corporate governance responsibility and for ensuring the proper management of information risks in their delivery chains, subject to meeting the mandatory rules set out in IS6? Has the Board issued a top-level policy statement committing the Department to the changes needed to implement effective IA? What has the Board done to ensure that its delivery partners (including 3rd party suppliers based offshore and in the EU) and any other public body handling information on the Department's behalf are compliant with HMG SPF (which incorporates DHR) mandatory requirements? Has the Board endorsed the Cultural Change Plan produced by the SIRO? (Connect with TEA 1.3) 	<ul style="list-style-type: none"> Board members recognise that they have responsibility for the implementation of IA measures to comply with statutory requirements embodied in the DPA and other similar legislation, together with other mandated IA policy requirements, within the Department, its delivery partners and within 3rd party suppliers. Top level IA Policy Statement. Information Security Policy setting out how all those involved in delivering the Department's business comply with mandatory requirements. Details of assurance mechanism. Details of Board engagement.
<p>1.3 Transparency</p> <ul style="list-style-type: none"> Has an Information Charter has been published setting out how the Department handles information and how members of the public can address any concerns that they have and is the Charter readily accessible by members of the Department, its delivery partners, 3rd party suppliers, and the public? 	<ul style="list-style-type: none"> An Information Charter applicable to the entire Department's business has been endorsed and published. The existence of the Charter is known within the Department. A copy of the Charter can be readily accessed from the Department's website.
<p>1.4 SIRO Responsibilities</p> <ul style="list-style-type: none"> Has a Board Member been appointed as SIRO and is he/she an effective advocate for information risk on the Board and in internal discussions? Does the SIRO own the Department's Information Risk Policy and Information Risk Assessment? (Connect IRM 1.1 & 1.3) 	<ul style="list-style-type: none"> Evidence of commitment from a trained and competent SIRO to the role, both at Board level and within the Department. SIRO acknowledges his/her responsibility and has the process in place to produce and maintain these documents on a regular basis.

UNCLASSIFIED

<ul style="list-style-type: none"> • Has the SIRO endorsed a statement of the Department's Information Risk Appetite, following consultation with the HMG CIO? (Connect with IRM 1.2) • Does the SIRO maintain an IA Risk Register and is there an effective methodology in place to address the risks (connect with IRM 1.4) • Has information risk has been specifically addressed in the Departmental annual Statement on Internal Control (SIC), which is signed off by the Accounting Officer and has the SIRO provided written advice to the AO on the content of the SIC relating to information risk. • Has the SIRO provided a written assessment to the AO of how DHR recommendations are delivering required change? • Does the SIRO receive annual reports from all IAOs detailing the information security and use assessments (including access control measures) for each information asset? • How does the SIRO assure the contents of the annual reports from the IAOs? • Has the SIRO taken responsibility for producing and staffing for approval to the Main Board an information risk cultural change plan aimed at fostering a culture that values, protects and uses information for the public good? (connect with TEA 1.3) • What has the SIRO done to initiate a programme of work to share and learn best practice from others, including, other Departments, fellow SIROs, IA specialists in NTA and industry? • Is the SIRO engaged in discussions involving new (and possibly unexpected) ICT requirements to ensure that IA requirements are factored in from the start? 	<ul style="list-style-type: none"> • Statement of the Department's Information Risk Appetite. • Clear governance framework, with procedures for the allocation of responsibilities and management of actions. • SIC and the written advice. • Written assessment. • Sample of an approved annual report. • Details of assurance mechanism, together with any reports that have been made. • Evidence that the cultural change plan is receiving the degree of high level involvement and exposure required by the DHR. • Engagement with SIRO network. • Other initiatives. • Details of effective SIRO engagement in forward ICT planning.
<p>1.5 DSO Responsibilities</p> <ul style="list-style-type: none"> ▪ Does the Department have a DSO (who has day-to-day responsibilities for all aspects of Protective Security {including physical, personnel and information security}), an ITSO (responsible for the security of information in electronic form) and if cryptographic material is handled, a ComSO? 	<ul style="list-style-type: none"> • Details of who the designated personnel and their TORs.
<p>1.6 Information Asset Owner (IAO) Responsibilities</p> <ul style="list-style-type: none"> • Are IAOs in place for all information assets on the Departmental list of information assets and are they sufficiently senior to discharge the role envisaged in the DHR? • Have the IAOs that are accountable for protected personal data explicitly defined and documented the access rights granted to this data, within a level of risk which is acceptable to the Department? • Has the Department put in place mechanisms to identify and keep a record of all staff and contractors who have access to, or involved in handling personal data? • Has the Department put in place arrangements to log the activity of data users in respect of electronically-held protected personal data, particularly those working remotely and those with higher levels of IS functionality? • Have IAOs put in place mechanisms to ensure that managers check that the activity log process is working properly? • Do the respective IAOs have oversight of this process and is a process in place to ensure that details of the process are recorded so that they are available for inspection by the ICO? • Have decisions relating to the direction given in Paragraphs 11-14 of IS6 been approved in writing by the relevant IAO? • Where action is taken within a Department on behalf of an IAO or a number of IAOs, to discharge the DHR mandatory measures, has the Department made it clear to IAOs that the obligation remains with them to satisfy themselves that the action taken meets the DHR requirement and where it does not it is their responsibility to ensure remedial action is taken to increase the efficacy of the measure? 	<ul style="list-style-type: none"> • Details of IAO regime, IAO TORs and Information asset list annotated to show IAOS. • Written details of where IAOS have defined the access rights to protected personal data, taking specific account of the need to minimise access relating to; pools of records, numbers of records, the nature of the information and the IS functionality as defined in Paragraph 18 of IS6. • Details of the mechanism and how this is assured. • Details of the process and its efficacy. • Details of the mechanism and its efficacy. • Management reports. • Details of the consideration of the mandatory requirements, together with the written approval by the relevant IAO. • IAO guidance material. • Details of IAOS testing the efficacy of centrally implemented measures. • Details of IAOS taking remedial action to discharge their obligations.
<p>1.7 Governance Structure</p> <ul style="list-style-type: none"> • Is the top level governance of information related matters joined up in a sensible way so that there are effective linkages between different parts of the business (such as CIO, SIRO, DSO, business continuity, operations, ICT delivery etc)? • Is the governance structure between the SIRO, DSO and ITSO clear and does it work effectively? • Is the governance structure below the SIRO fit for purpose and is there an effective delegation process down through the IA governance chain? 	<ul style="list-style-type: none"> • Clear lines of responsibility and accountability within governance framework. • Details of governance structure and how the different parties interact and gain their authority. • Effective governance structure including delegations exists between SIRO and those charged with implementing IA policy.

<p>1.8 Information Security Policy</p> <ul style="list-style-type: none"> • Does the Department have an Information Security Policy as a component of their overarching Security Policy setting out how the Department, its delivery partners and 3rd party suppliers (including those offshore), comply with the minimum requirements set out in HMG SPF and particularly Security Policy No: 4? • Does the Information Security Policy include the requirement to apply the Government Protective Marking System and the necessary controls and technical measures relating to the system as laid out in the Security Policy Framework (SPF MR11)? • Does the Policy include a clear definition of the need for Confidentiality or Non-Disclosure Agreements (NDAs) for the protection of information and where these are to be applied? • Does the Policy make it clear who is responsible for establishing the process by which all employees, contractors and 3rd party users who have had access to information assets and processing facilities surrender any assets in their possession and have their access rights removed upon the termination of their employment, contract, or agreement? 	<ul style="list-style-type: none"> • Information Security Policy document. • Information Security Policy document. • Detail from Information Security Policy, or details of where requirement for such agreements is established. • Clear establishment of responsibilities
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

LEVEL 2 – Established - IA Processes are Institutionalised

Areas to Probe	Evidence Expected
<p>2.1 Board Responsibilities</p> <ul style="list-style-type: none"> • Do the Board members understand and accept their responsibility for IA as part of their corporate governance responsibility? • Has the Board endorsed an up-to-date IA Strategy, as part of an overarching Information Strategy, detailing how the Department is to develop its IA maturity over time? • Is the resultant programme to implement the strategy, particularly as it relates to business critical systems, adequately resourced? 	<ul style="list-style-type: none"> • Board members accept that they have responsibility for the implementation of IA measures to comply with statutory requirements embodied in the DPA and other similar legislation, together with other mandated IA policy requirements (including the detail on IA Policy in the latest edition IS2⁵) within the Department, its delivery partners and within 3rd party suppliers. • An up-to-date Strategy exists together with a process to update it on a regular basis. • Allocation of resources to implement the Strategy.
<p>2.2 Transparency</p> <ul style="list-style-type: none"> • Has the Department a philosophy of transparency? • Does the Department understand the need to, and value of, keeping the public informed to assist in engendering trust in the Department's ability to safeguard their information? 	<ul style="list-style-type: none"> • The Board applies what it has endorsed in its Information Charter and there is documentary evidence to show regular action to disseminate information. • A plan exists to keep the public informed of what the Department is doing to safeguard their information and there is evidence of its successful implementation.
<p>2.3 SIRO Responsibilities</p> <ul style="list-style-type: none"> • Does the SIRO receive effective progress reports from those who manage the programme to implement the IA aspects of the Information Strategy? • Does the SIRO report progress against the endorsed IA Strategy to the other Main Board members? • Has the SIRO put in place a review to assess whether the way the Information Risk Management (IRM) initiatives have bedded down within the Department are delivering the improvement in IRM required by the business? • Does the SIRO know which of the Department's IS are business critical? (Connect with IRM 2.7) • Does the SIRO know the accreditation status of the Department's IS and has he been involved in prioritising, in terms of business risk, the list for remedial action? (Connect with IRM 2.7) • Is the SIRO and the rest of the Department benefiting from sharing and learning best practice from others, including, other Departments, fellow SIROs, IA specialists in NTA and industry etc? 	<ul style="list-style-type: none"> • Evidence of effective two-way engagement between the SIRO and those charged with running the IA Programme. • Evidence that SIRO ensures that Programme Milestones are achieved. • Main Board Minutes or Reports. • Details of the Review and any action taken to improve the efficacy of the IRM regime. • Criteria for establishing business criticality and a definitive list of business critical systems exist. • Prioritised list endorsed by the SIRO. • Engagement with SIRO network. • Details of other engagement.
<p>2.4 IAO Responsibility</p> <ul style="list-style-type: none"> • Do IAOs consider on an annual basis how better use could be made of their information assets and do they maintain logs of requests for further access to their information? 	<ul style="list-style-type: none"> • Sample of IAO approach to better use, together with evidence of maintaining a log.

⁵ Publication coincident with SPF issue of autumn 2009.

<p>2.5 Governance Structure</p> <ul style="list-style-type: none"> Is there effective engagement between the SIRO/IA organisation and the DSO/security organisation? Are the IA Policy requirements reflected in personnel and physical security policies and procedures? <p>Is there an effective IA governance regime and are there effective mechanisms to hold staff accountable for their actions?</p>	<ul style="list-style-type: none"> Evidence of a mutually supportive approach to IA being taken by the Departmental CIO, SIRO and DSO, which is then reflected in the inter-working of the respective areas. Details of the IA governance regime below the SIRO, showing clear lines of responsibility and accountability.
<p>2.6 Information Security Policy</p> <ul style="list-style-type: none"> Is the Information Security Policy reviewed at planned intervals, or when significant changes occur, to ensure its continuing suitability, adequacy and effectiveness? How are members of the Department, its Delivery Partners and its 3rd Party Suppliers made aware of the need to comply with the Information Security Policy? 	<ul style="list-style-type: none"> Details of the review process and changes that were made at the last review. Details of the process and how its effectiveness is validated
<p>2.7 IA Strategy</p> <ul style="list-style-type: none"> Is the IA Strategy endorsed by the Board fit for purpose; does it represent good/best practice? <ul style="list-style-type: none"> Does the IA Strategy include the methodology by which the Department seeks to implement a coherent IRM regime? How aligned is it to the guidance provided in ISO/IEC 27001:2005 which details the requirements for an effective Information Security Management System (ISMS)? Does the IA Strategy take a though-life approach from concept to disposal of information and equipment? <ul style="list-style-type: none"> Does the IA Strategy include all aspects of the business requirement? Does the IA strategy take due account of the need to engage early with the business as it examines new ICT solutions to ensure that IA requirements are factored in from the start? Are specific IA risk issues such as those concerning Flexible Working and the use of removable media included? <ul style="list-style-type: none"> Has the full range of vulnerabilities and threats to information been captured within the Strategy (both current and those considered to be relevant to the business in the future) and has the Department engaged with the expert community in drawing up the list? Is there sufficient linkage of the IA Strategy with other relevant policies? 	<ul style="list-style-type: none"> The IA Strategy establishes the Department's approach to all IA measures, embracing all risks to information from natural disasters to electronic attack. Evidence of engagement with stakeholders and peers in developing IA Strategy. Evidence that the IRM methodology to be implemented within the Department takes due cognisance of the guidance contained in ISO/IEC 27001:2005. Due emphasis is given to secure waste disposal and the effective elimination of stored data prior to disposal of equipment. The policy follows NTA advice and guidance. Evidence of strong business driven linkage. Evidence of the strategy being focussed on the future preparedness of the Department to produce ICT solutions that are IA compliant from the start. Specific IA risk issues concerning Flexible Working, particularly the use of Personal Electronic Devices and removable media follows NTA advice and guidance. Evidence of effective engagement with CPNI, NTA and law enforcement agencies. Resultant range of vulnerabilities is comprehensive and applicable to the business of the Department, both now and in the foreseeable future. Evidence of clear linkage with at least the Department's Information Policy, Risk Policy and Business Continuity Management Policy.
<p>2.8 IA Programme</p> <ul style="list-style-type: none"> Is there evidence of a programme of work to implement the IA Strategy? 	<ul style="list-style-type: none"> Evidence of formal programme documentation and processes Evidence of an effective programme management regime.

LEVEL 3 – Business Enabling - IA Processes are Implemented in Critical Areas of the Business

Areas to Probe	Evidence Expected
<p>3.1 Board Responsibilities</p> <ul style="list-style-type: none"> Are the owners of the business processes which are critical to the business actively engaged in championing the adoption of good IA practice both within the IS and by the staff who use them? When funding becomes tight is IA spending maintained to ensure IA processes are implemented in an effective way in the critical areas of the business? Is there evidence that key IRM decisions relating to business critical systems have been elevated to the Board for a decision, or failing that, that the SIRO has taken the decision, on behalf of the Board? (Connect with IRM 3.2) Is the Management Board aware of the systemic IA risks that impact on the delivery of the Department's outputs? (Connect with IRM 3.2) 	<ul style="list-style-type: none"> Action that has been taken by Business Unit to raise the awareness of IA across the critical areas of their business. Evidence that IA funding is not taken as a soft option and is maintained to address issues relating to the critical areas of the business. Details of the risk analysis that supported the decision made, either by the Board or by the SIRO, on behalf of the Board. Main Board papers showing submission of data and subsequent actions being taken
<p>3.2 IA Strategy</p> <ul style="list-style-type: none"> Is the IA strategy subject to regular review to ensure that it remains aligned to the needs of the business in the context of the current threat and vulnerabilities? 	<ul style="list-style-type: none"> Details of the review process and what changes have been made.

UNCLASSIFIED

<p>3.3 IA Programme</p> <ul style="list-style-type: none"> Is the IA programme managed effectively? Does the SIRO receive regular updates from the IA programme manager? Is the IA programme on course to deliver the Board's intent detailed in the IA strategy in a timescale and at a cost acceptable to the business? 	<ul style="list-style-type: none"> Details of the programme management regime. Details of the reporting regime to the SIRO and of any action taken by the SIRO to ensure the programme meets its deliverables. Details of the benefit realisation plan.
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

LEVEL 4 – Quantitatively Managed - The Number of Corporate Exceptions to Implementing IA Processes is Known & Reported

Areas to Probe	Evidence Expected
<p>4.1 Board Responsibilities</p> <ul style="list-style-type: none"> Does the Main Board know how many business processes and related IS are not implementing good IA practice? Is the Management Board made aware of the key IA risks affecting all systems, together with the systemic IA risks that impact on the delivery of the Department's outputs? (Connect with IRM 4.2) Has the Main Board been presented with an investment appraisal quantifying the amount of effort and resource needed to bring all IS up to the same standard as the Business Critical systems? If a Board-Level decision has been made not to extend good IA measures from the business critical IS to the remainder, was the decision based on an accurate IRM analysis? Does the Main Board receive regular reports of progress against the IA Strategy Milestones? Does the Main Board ensure that sufficient funding is allocated to IA as a % of its overall ICT spend and its importance of information to its business? 	<ul style="list-style-type: none"> Reports made to the Main Board by the SIRO detailing the IA status of all IS and related processes within the Department. Main Board papers showing submission of data and subsequent actions being taken. Investment Appraisal. Details of the IRM analysis presented to the Main Board. Main Board Minutes provide evidence of discussion and resultant actions. Evidence of follow-up of actions Either the Main Board has taken a paper from the CIO analysing and quantifying the importance of Information to the Business of the Department, or the detail is included within the Department's Information Policy. The ICT approvals process for new expenditure within the Department requires the percentage of spend on IA to be broken out as a separate amount. A process exists to capture the IA expenditure of the Department as a % of total ICT expenditure. Evidence that funds are allocated to IA commensurate with its importance to the business.
<p>4.2 IA Programme</p> <ul style="list-style-type: none"> What action has been taken to provide evidence of hard and soft benefits delivered by the IA programme to justify further investment? 	<ul style="list-style-type: none"> Details of the benefits realised and how that information has been used to influence further investment.

LEVEL 5 – Optimised - Responsive IA processes are integrated as Part of Normal Business

Areas to Probe	Evidence Expected
<p>5.1 General</p> <ul style="list-style-type: none"> Is IA still considered to be a discrete discipline, or is it considered to be an integral part of normal business? Is the Department being transparent? 	<ul style="list-style-type: none"> Where appropriate IA is considered as an integral part of the standard processes within the Department at all levels and within its delivery partners and 3rd party suppliers. Quality of reporting to Parliament, PQs and other public responses.
<p>5.2 Board Responsibilities</p> <ul style="list-style-type: none"> Is the Main Board regularly presented with an accurate picture of the IA risk exposure of the Department? (Connect with IRM 5.1) Do all Board Members appreciate the critical role that information plays in the success of the Department's business? 	<ul style="list-style-type: none"> Main Board papers and Annual Departmental Report. Evidence that decisions have been made based on expert guidance. By word and action all Main Board members advocate the need for effective IA measures to be implemented to safeguard the business of the Department.

2. Training, Education and Awareness

Level 1 – Initial Awareness of the Criticality of IA to the Business and its Legal Requirements	Level 2 – Established IA Processes are Institutionalised	Level 3 – Business Enabling IA Processes are Implemented in Critical Areas of the Business	Level 4 – Quantitatively Managed The Number of Corporate Exceptions to Implementing IA Processes is Known & Reported	Level 5 – Optimised Responsive IA processes are integrated as Part of Normal Business
A programme of annual information risk awareness training is instituted for all who have access to personal data within the Department its delivery partners and 3 rd party suppliers. A Departmental cultural change plan is implemented.	All members of the Department undergo annual risk awareness training. A programme of targeted IA education and training is instituted. Staff behaviours are measured and trends analysed. Progress against the cultural change programme is managed and reported to the SIRO.	A programme of pre-appointment training is instituted for key staff and all existing key staff are trained. A sustained improvement in staff awareness of their IA responsibilities is achieved.	Accurate details of the training received by all staff are collated and reported to the SIRO. Staff surveys show that staff attitudes and behaviours towards assuring information are aligned to the needs of the business.	The need to assure the Department's Information and that of its external stakeholders as a key business asset is fully embedded within the Departmental culture and is subject to a regime of continuous improvement.

Goal IA responsibilities are assigned from the Main Board downwards to ensure that appropriately trained staff are held accountable for their decisions and actions. The result is a culture within the Department that values information as a business asset.

Justification Without effective training, education and awareness staff within the Department will not implement policies and procedures in a way that values and protects information as a core business asset.

LEVEL 1 – Initial - Awareness of the Criticality of IA to the Business and its Legal Requirements

Areas to Probe	Evidence Expected
<p>1.1 IRM Training – Personal Data</p> <ul style="list-style-type: none"> Does every member of the Department, its delivery partners and 3rd party suppliers who have access to personal data undergo an annual session of information risk awareness training? Is this training incorporated as part of the induction process? Does the training include some form of assessment so that there is an improved chance that the material is remembered? How does the SIRO assure himself/herself that every member of staff within the Department, its delivery partners and 3rd party suppliers who have access to personal data receive this training on induction and annually thereafter? 	<ul style="list-style-type: none"> Details of the material provided and how it is delivered. Details of how the training is incorporated within the induction process for new joiners to all of the applicable organisations. An effective mechanism exists to ensure that those who have undergone the training remember what they have been taught. Details of the assurance process.
<p>Note: Departments will wish to satisfy themselves that their delivery partners and 3rd party suppliers are discharging the training requirement satisfactorily. Departments should make available the evidence that they are relying on to manage this risk and any assurance process they have put in place to satisfy themselves that the training is adequate.</p>	
<p>1.2 IRM Training for Key Personnel</p> <ul style="list-style-type: none"> Has specific training been established for the AO, SIRO, IAOs and members of the Audit Committee, on appointment and at least annually thereafter? 	<ul style="list-style-type: none"> Details of how the education and training is provided and promoted
<p>1.3 Cultural Change Plan</p> <ul style="list-style-type: none"> Does the Department have an information risk cultural change plan aimed at fostering a culture that values, protects and uses information for the public good? Does the cultural change plan include the following mandatory requirements?: <ul style="list-style-type: none"> Adequate HR arrangements to reward positive approaches to information risk and to penalise negative activity, HR arrangements make it clear that failure to apply Departmental procedure is a serious matter and, in some situations, amounts to gross misconduct. Mechanisms so that staff can bring concerns about information risk to the attention of senior management, or the Audit Committee, anonymously if necessary, recording concerns expressed and action taken in response. Questions inserted in personnel surveys to determine the effectiveness of the cultural change programme. 	<ul style="list-style-type: none"> Details of cultural change plan Details of reward and retribution mechanisms. Details of mechanisms which command the confidence of staff. Details of concerns and resulting action taken. Details of planned survey questions and the responses derived.

UNCLASSIFIED

LEVEL 2 – Established - IA Processes are Institutionalised

Areas to Probe	Evidence Expected
<p>2.1 IRM Training – Personal Data</p> <ul style="list-style-type: none"> Is there evidence that regular, compulsory refresher training is undertaken by all staff who access personal data? How does the SIRO satisfy himself/herself that the training is sufficient in terms of depth, breadth and coverage to meet the needs of the business? Are details of the % by grade within each organisation who have successfully undertaken the training are known? What action is taken to ensure that all those who should have undertaken the training are trained? 	<ul style="list-style-type: none"> Details of the training. Details of any review of training put in place by the SIRO. Details of the % of the staff that should be trained are known. Effective mechanisms exist to chase those who have not yet undertaken the training.
<p>2.1 IRM Training – All Information</p> <ul style="list-style-type: none"> Has the information risk awareness training which was mandatory for those with access to personal data users at Level 1 been extended so that applicable information risk awareness training is given to all staff in the Department, its delivery partners and 3rd party suppliers? Is this training incorporated as part of the induction process? Does the training include some form of assessment so that there is an improved chance that the material is remembered? How does the SIRO assure himself/herself that every member of staff within the Department, its delivery partners and 3rd party suppliers receive this training on induction and annually thereafter? 	<ul style="list-style-type: none"> Details of the material provided and how it is delivered. Details of how the training is incorporated within the induction process for new joiners to all of the applicable organisations. An effective mechanism exists to ensure that those who have undergone the training remember what they have been taught. Details of the assurance process.
<p>2.2 IRM Training for Key Personnel</p> <ul style="list-style-type: none"> Are the AO, SIRO, IAOs and members of the Audit Committee up to date in completing their annual training? Has the effectiveness of this training been assessed? 	<ul style="list-style-type: none"> Training details. Details of the validation process and any action taken to re-align the training to the needs of the business.
<p>2.3 Specialist IRM Training</p> <ul style="list-style-type: none"> Does a programme of targeted education and training exist for staff who manage/maintain the secure configuration of ICT systems or have IA responsibilities and is an effective process in place to select staff for further education and/or training on IA matters and to monitor the effectiveness of the training/education? Are the DSO, ITSO and COMSO trained and competent to perform the roles? How is the success of the education and/or training measured? 	<ul style="list-style-type: none"> Details of the training provided. Details of the numbers of staff who have undergone the education and/or training and details of its effectiveness. The individuals are trained to discharge their duties in a competent manner. Course feedback of the applicability of the education and training
<p>2.4 Cultural Change Plan</p> <ul style="list-style-type: none"> How is progress against the cultural change programme managed and reported to the SIRO? How effective are the measures put in place by the cultural change plane in achieving the following? <ul style="list-style-type: none"> Rewarding positive approaches to information risk and penalising negative activity. Staff concerns about information risk are brought to the attention of senior management, or the Audit Committee, anonymously if necessary. Feedback from staff through personnel surveys about the effectiveness of the cultural change programme. Does the system of Reward and Recognition to acknowledge those who adopt the right approach to IA work? Is disciplinary action taken, and is it seen to be taken, against those who flout IA requirements? 	<ul style="list-style-type: none"> Details of the cultural change management process. Details of progress reports submitted to the SIRO. Details of reward and retribution mechanisms. Details of mechanisms which command the confidence of staff. Details of concerns and resulting action taken. Details of planned survey questions and the responses derived. Evidence that Reward and Recognition system is working and is proving useful in promoting IA awareness. Prompt and effective action is taken against those who break the IA rules.

LEVEL 3 – Business Enabling - IA Processes are Implemented in Critical Areas of the Business

Areas to Probe	Evidence Expected
<p>3.1 IRM Training – All Information</p> <ul style="list-style-type: none"> Is there evidence that regular, compulsory refresher training is undertaken by all staff who have access to the Department's information? How is the effectiveness of the mandatory information risk awareness training which was put in place at Level 2 for every member of the Department, its delivery partners and 3rd party suppliers validated? Are details of the % by grade within each organisation who 	<ul style="list-style-type: none"> Details of the training. Details of the validation process and any action taken to modify the training to achieve the desired result. Details of the % of the staff that should be trained are known.

UNCLASSIFIED

<p>have successfully undertaken the training are known?</p> <ul style="list-style-type: none"> What action is taken to ensure that all those who should have undertaken the training are trained? 	<ul style="list-style-type: none"> Effective mechanisms exist to chase those who have not yet undertaken the training.
<p>3.2 IRM Training for Key Personnel</p> <ul style="list-style-type: none"> Has the effectiveness of the training provided for the AO, SIRO, IAOs and members of the Audit Committee been assessed? 	<ul style="list-style-type: none"> Details of the validation process and any action taken to re-align the training to the needs of the business.
<p>3.3 Specialist IRM Training</p> <ul style="list-style-type: none"> Is there an effective IA training regime in place for all staff who hold key IA related appointments? Is this training undertaken prior to appointment? How is this specialist training validated? 	<ul style="list-style-type: none"> Identification of the key staff that need training. Details of the training provided. Details of the % of identified staff who have undertaken the training. Details of how the training is given pre-appointment. Course feedback of the applicability of the training
<p>3.4 Cultural Change Plan</p> <ul style="list-style-type: none"> Is there evidence of effective data gathering to assess whether the desired changes in approach are being adopted into the culture of the Department, its delivery partners and within 3rd party suppliers? Is the resultant data analysed and is action taken to re-adjust the approach to IRM education and training to promote the desired cultural change? Is there a sustained improvement in staff awareness of the importance of effective IRM to the business of the Department as measured through a staff attitude survey, or similar mechanism? 	<ul style="list-style-type: none"> Details of how the data is gathered. Details of the analysis made and how this is used to change the approach to IRM training. Details of how the efficacy of the Cultural Change plan is measured and what is done with the results.

LEVEL 4 – Quantitatively Managed - The Number of Corporate Exceptions to Implementing IA Processes is Known & Reported

Areas to Probe	Evidence Expected
<p>4.1 Effectiveness of all IRM Training</p> <ul style="list-style-type: none"> Are accurate details of the members of staff who have been educated and trained reported to the SIRO? Is an assessment made of the coverage and effectiveness of education and training against the requirements of the cultural change programme? Is there a plan to take action in response to the education and training assessment? 	<ul style="list-style-type: none"> Details of the education and training reports submitted to the SIRO. Details of the education and training analysis submitted to the SIRO. Details of any action taken with respect to the education and training regime.
<p>4.2 Cultural Change</p> <ul style="list-style-type: none"> Is the positive trend established at Level 3 in the awareness of the importance of effective IRM to the business by Departmental staff being sustained? What action is being taken to keep the message fresh and relevant to the needs of the business? 	<ul style="list-style-type: none"> Trend information derived from the data gathering process adopted at Level 3 shows a year on year improvement. Details of the plan to maintain the relevance of the IA message fresh and applicable.

LEVEL 5 – Optimised - Responsive IA processes are integrated as Part of Normal Business

Areas to Probe	Evidence Expected
<p>5.1 Cultural Change</p> <ul style="list-style-type: none"> Is there evidence to show that IRM is accepted to be part of normal business and that it effective application is ingrained in the culture of the Department? What actions are taken to ensure that effective IA remains embedded within the culture of the Department? 	<ul style="list-style-type: none"> Where appropriate IRM is considered as an integral part of the standard processes within the Department at all levels and within its delivery partners and 3rd party suppliers. Evidence of engagement with other Departments to promote best practice. Details of initiatives used to ensure that staff remain focussed on applying effective IA as a routine activity.

3. Information Risk Management (IRM)

Level 1 – Initial Awareness of the Criticality of IA to the Business and its Legal Requirements	Level 2 – Established IA Processes are Institutionalised	Level 3 – Business Enabling IA Processes are Implemented in Critical Areas of the Business	Level 4 – Quantitatively Managed The Number of Corporate Exceptions to Implementing IA Processes is Known & Reported	Level 5 – Optimised Responsive IA processes are integrated as Part of Normal Business
A comprehensive information risk policy is in place. The Department's information risk appetite is clearly articulated. Information risks with appropriate owners and managers are identified within risk registers at the strategic level. All new IS are subject to an effective accreditation process, where appropriate Privacy Impact Assessments are used and effective contract mechanisms are used to apply IA through life. The Department's approach to addressing information risks is agreed with the Department's external stakeholders, where applicable.	The Accreditation status of all existing IS is determined and the information risks are identified within risk registers for all accredited in-service IS. A risk based programme of work is initiated to rectify any Accreditation shortfall where this is required to support the business need. A process is in place to escalate information risks through the Department's management structure for effective decision making, within the Department, its delivery partners, and with external stakeholders.	All IS that are critical to the business have been subject to Accreditation and the Department has effective information risk management processes in place to manage the residual risks and the related, systemic IA risks.	For all IS, the residual risks that are to be tolerated are quantified and the Main Board is fully aware of the total level of information risk and systemic IA risk the Department is carrying and ensures that the risks are managed to assure the Integrity, Availability and Confidentiality of key business information.	The risk exposure of the Department is within the risk appetite and threshold of the Main Board, its external stakeholders and those with whom it shares information. The threats, vulnerabilities and risks to the Department's information are kept under active review.

Goal Information risk is managed throughout the Department in a structured way so that management boards throughout the Department understand the business impact of IA related risks and manage them effectively in consultation with external stakeholders to assure the business of the Department.

Justification Without effective IRM processes that enable the sensible aggregation of information risks being taken across the Department, decision makers will be prevented from making informed decisions, particularly relating to the treatment of systemic risks which have the potential to cause severe disruption of the Department's business.

LEVEL 1 – Initial - Awareness of the Criticality of IA to the Business and its Legal Requirements

Areas to Probe	Evidence Expected
<p>1.1 Information Risk Policy</p> <ul style="list-style-type: none"> Does the Department have an Information Risk Policy, (or is information risk adequately included in the overall Departmental Risk Policy)? Does The Information Risk Policy adequately cover delivery partners and 3rd party suppliers and does it set out how compliance with the policy and its effectiveness is to be measured? Do the Departmental IA staff have access to CO guidance and if they have access to it, do they understand it and have they applied it in the formulation of the Information Risk Policy? Where a decision has been made not to apply CO guidance, is there evidence to show that a risk assessment has been undertaken? 	<ul style="list-style-type: none"> Departmental Risk Policy or discrete Information Risk Policy Statement. The Information Risk Policy must explicitly include: <ul style="list-style-type: none"> How the DHR measures are to be implemented in the Department's activity and that of their delivery partners. How compliance with the policy is to be monitored. How its effectiveness is to be measured. Details of how the IA staff keep up to date with developing IA Guidance. A valid risk assessment
<p>1.2 Information Risk Appetite</p> <ul style="list-style-type: none"> Does a clear statement of the Department's Risk Appetite exist? How is this made available to those who need to apply it? Is the Department's Information Risk Appetite aligned to that of the rest of HMG? 	<ul style="list-style-type: none"> SIRO endorsed statement of the Department's risk appetite. Details of where the Department's Information Risk Appetite is detailed and how it is promulgated, particularly to the accreditation staff. Assessment of the alignment of the Information Risk Appetite with that of the HMG CIO, or any evidence that he/she has been consulted in formulating the Information Risk Appetite Statement.

UNCLASSIFIED

<p>1.3 Risk Assessments</p> <ul style="list-style-type: none"> • Does the Department have access to the generic Threat Assessment to HMG ICT systems? • Has the Department undertaken the DHR required annual Departmental Information Risk Assessment, to include the effectiveness of the overarching policy and does this recognise the HMG Threat Assessment? • Has the SIRO ensured that the assurance activities listed at Paragraph 15 of IS6 have been completed as part of the preparation of the Annual information risk assessment? • Is there a plan in place to repeat the departmental information risk assessment on a quarterly basis? • Is the Department up-to-date in producing the DHR required quarterly risk assessment of the delivery chain? • Is a process in place to produce an annual assessment of service, technology and threat change? • Does the Department conduct an annual technical risk assessment using IS1 for all its ICT projects and programmes? • Are such technical risk assessments and risk management decisions recorded in an RMADS in accordance with IS2? 	<ul style="list-style-type: none"> • Evidence of access to the Security Service Annual Threat Assessment and Infosec Memorandum No: 2. • Departmental information risk report covering the entire delivery chain and an assessment of the risk policy. • Specific details of the eight aspects of assurance listed at Paragraph 15 of IS6. • Risk assessment plan. • Last two quarterly risk assessments of the delivery chain. • Process of annual re-assessment. • Details of the schedule of assessments. • Evidence of the use of IS1 and IS2
<p>1.4 Risk Registers</p> <ul style="list-style-type: none"> • Have significant information risks affecting the Department, its delivery partners and 3rd party suppliers been recorded within the Departmental Risk Register? • Does the SIRO maintain an IA Risk Register and is there an effective methodology in place to address the risks? • Do the appropriate levels of management responsible for the delivery of in-service IS reflect IA risks within their risk registers and do they have an effective process for managing the IA risks both to the existing configuration and any proposed change in the in-service configuration? 	<ul style="list-style-type: none"> • Up-to date list of major risks analysed by likelihood and impact, with evidence of regular reviews of the risks, mitigation options and contingency plans. • Clear governance framework, with procedures for the allocation of responsibilities and management of actions.
<p>1.5 Information Assets</p> <ul style="list-style-type: none"> • Are all of the Department's information assets (not just personal data) identified within an Information Asset List (inventory of assets)? • Are IAOs allocated to every asset? • Is there an effective process to maintain the accuracy of the Asset List? • Has the Department determined what personal information it and its delivery partner(s) hold in the DHR categories A & B? • Have processes been put in place to ensure that personal information falling into DHR categories A & B is handled as at least PROTECT – PERSONAL DATA? 	<ul style="list-style-type: none"> • Sample Information Asset List. • Details of the updating process. • Details of how the Department has approached categorising the personal information it holds, together with details of how much information is held by whom in each category? Details of the process and what measures have been used to ensure compliance.
<p>1.6 New Programmes & Related Contracts</p> <ul style="list-style-type: none"> • What horizon scanning activities are in place to take advantage of new ICT solutions to business issues? • Is there a documented process for authorising the acquisition of a new information processing facility within the Department? • Are those responsible for IA within the Department aware of both the internal sponsored and the pan-Departmental ICT programmes which will impact on the work of the Department in the next 3-4 years? • Are there credible plans and/or processes in place so that emerging new ICT requirements are recognised early enough enabling a full range of information risk management processes to be applied from the outset? • Have the risk assessments relating to external stakeholders, and especially those with whom the Department will be required to share information, been agreed with them? • Does the Department ensure Privacy Impact Assessments (PIAs) are used to assess the DPA compliance of all new policies, procedures and systems? • How does the Department ensure that security requirements are specified in ICT contracts and all new ICT contracts handling personal data adhere to the Office of Government Commerce (OGC) ICT model terms and conditions? Is a process in place to ensure that should any changes relevant to information risk be required, such changes are approved personally by the SIRO? • Are newly negotiated contracts flexible enough to ensure that cost effective changes can be made to take account of changes in the IA environment. • Do procurement processes (for IA measures) use HMG approved IA sources? 	<ul style="list-style-type: none"> • Details of what activity the Department has put in place to keep abreast of new ICT technology which, if implemented, would bring business benefit. • Details of the process. • Evidence to show that the IA community are fully engaged with the future ICT strategy for the Department. • Details of how new ICT requirements are intercepted sufficiently early in their consideration by the IA community to ensure that effective IA measures are implemented from the start. • Evidence to show that there is mutual agreement of the risk assessment relating to shared information • Evidence of agreed mitigation action. • Evidence of policy statement on PIA for a policy, process or IS. • Departmental directive to include SIRO's role in the change process. • Cases that have been made to the SIRO for changes. • Contract change procedures. • Measures selected from IA Directory of HMG IA Catalogue

<p>1.7 Accreditation</p> <ul style="list-style-type: none"> • Does the Department understand the requirement for Accreditation and does it have access to Accreditation services, which meet national standards. • Are the Accreditors used by the Department trained and proficient in the use of IS2? Do they all meet the standards of the CO ITPC Scheme? • What process is in place to ensure that all new IS processing information requiring protection are subject to Accreditation? • Does the Department use Business Impact Levels to assess and identify the impacts to the business caused through the loss of Confidentiality, Integrity and/or Availability of data or ICT systems should risks be realised? • Does the Department take adequate account of the affect of aggregation on determining Business Impact Levels? • What plan exists to comply with the DHR requirement that all ICT systems handling protectively marked information are accredited and for every such system to be re-accredited when they undergo significant change or at least every 5 years? • HMG SPF requires that the accreditation status of all ICT systems processing protectively marked Government data must be reviewed annually to determine whether changes have occurred which could alter the original accreditation decision. How is the Department satisfying this requirement? 	<ul style="list-style-type: none"> • Details of how accreditation requirement is met. • Details of the accreditation staff • Details of how all new IS are subject to accreditation. • Details of how Business Impact Levels are used. • Details of where aggregation of data has been used. • Plan to establish accreditation status of all ICT systems handling protectively marked information and to comply with the DHR requirement. • Details of how annual reviews are undertaken.
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

LEVEL 2 – Established - IA Processes are Institutionalised

Areas to Probe	Evidence Expected
<p>2.1 Information Risk Policy</p> <ul style="list-style-type: none"> • Is the Information Risk Policy subject to regular review to assess its continuing applicability to the needs of the business? 	<ul style="list-style-type: none"> • Details of the review process and its effective implementation.
<p>2.2 Information Risk Appetite</p> <ul style="list-style-type: none"> • Is the Information Risk Appetite subject to regular review to assess its continuing applicability to the needs of the business? 	<ul style="list-style-type: none"> • Details of the review process and its effective implementation.
<p>2.3 Risk Assessments</p> <ul style="list-style-type: none"> • Has the Department an up to date Threat Assessment specific to their business? • Has the Department engaged with CPNI, CESG and SOCA in the construction of this Assessment? • Does the annual Departmental Information Risk Assessment recognise this specific Threat Assessment? • Is there evidence to show that when there is a significant change in a risk component (threat, vulnerability, impact etc) to an ICT system in operation then an immediate technical risk assessment is undertaken? 	<ul style="list-style-type: none"> • A tailored Threat Assessment specific to the Department's business activity (i.e. not just the Security Service annual Threat Assessment and IM2) • Evidence of effective engagement such as Threat Workshops. • There is clear documentary evidence that there is direct linkage between the Risk Assessment and the Threat Assessment. • Details of Assessments that have been undertaken in response to a change in a risk component.
<p>2.4 Risk Management</p> <ul style="list-style-type: none"> • Do the escalated IA risks have risks owners and managers allocated and are they appropriate to the significance of the risk being considered? • Is the Department's IA risk governance structure merely a reporting mechanism, or does it take effective action? • Does an effective process exist to escalate significant IA risks from Programmes and Projects up through the management chain of the Department, its delivery partners and its 3rd party suppliers? • Are effective bi-lateral and multi-lateral arrangements in place to manage IA risks which relate to external stakeholders? 	<ul style="list-style-type: none"> • Evidence that the risk owners and managers have sufficient seniority and competence to take the required action to treat the risk concerned. • Evidence to show that decisions are taken on a Departmental basis to manage significant IA risks. • Documentary evidence to show the process that should be followed, together with evidence that the process works. • Evidence to show that the views and opinions of external stakeholders are taken into account when managing Departmental level IA risks.
<p>2.5 Information Assets</p> <ul style="list-style-type: none"> • Does the Information Asset List, in accordance with the Departmental Plan to address Digital Continuity, include details of the retention requirements based on the business value of the information? 	<ul style="list-style-type: none"> • Accurate register of information assets and owners, and retention schedules based on business value, with procedures for implementation.
<p>2.6 New Programmes & Related Contracts</p> <ul style="list-style-type: none"> • Is there evidence that the process for authorising the acquisition of a new information processing facility within the Department is used effectively? • How is the Department preparing for any change in business procedures which are consequent on the deployment of new ICT 	<ul style="list-style-type: none"> • Records of how a new facility has been authorised. • Details of the integrated business change process which is being managed to gain maximum benefit from the new ICT.

UNCLASSIFIED

<p>programmes?</p> <ul style="list-style-type: none"> To what extent does the Department rely on 3rd party suppliers to design the information security features of new programmes? How does the Department assess the quality of the information security design of new programmes? How are contract risks as they relate to IA managed? 	<ul style="list-style-type: none"> Where the Department relies on 3rd party suppliers, evidence that they have taken appropriate steps to assess the quality of the supplier's security team. Details of the process employed, together with any evidence that they have sought external verification of the design from bodies such as CESC. Evidence of effective engagement of the IA staff with the programme staff to ensure effective management of IA risks.
<p>2.7 Accreditation</p> <ul style="list-style-type: none"> Does the SIRO know which of the Department's IS are business critical? Does the Department have a centralised record of the Accreditation status of the Department's IS? Has the list of un-accredited IS been prioritised in terms of business risk and is a programme of work in place to Accredite these systems? Is there a process in place to ensure that IS are re-accredited at appropriate intervals or following specific trigger events (such as: significant changes in threats, vulnerabilities, system configuration, management structure, Business Impact levels etc) or at least every 5 years? Are there instances where; legal treaty, technical or contractual constraints prevent the encryption of information? If there are, what action is being taken to overcome these constraints? 	<ul style="list-style-type: none"> Criteria for establishing business criticality and a definitive list of business critical systems exist. Details of the records. Prioritised list endorsed by the SIRO. Details of how accreditation is maintained through-life. Evidence to show that the Department does not just accept the status quo when it has the potential to impact on its business, but takes action to affect change.

LEVEL 3 – Business Enabling - IA Processes are Implemented in Critical Areas of the Business

Areas to Probe	Evidence Expected
<p>3.1 Risk Assessments</p> <ul style="list-style-type: none"> In addition to the generic Departmental Threat Assessment have Threat Assessments been developed for critical parts of the business? Is a systematic process in place to conduct operational and technical risk reviews of business critical IS and their related business policies and processes? 	<ul style="list-style-type: none"> Tailored threat Assessments exist for specific ICT systems that service critical business functions and is evidenced in IS1 calculations. Schedule of reviews and action plans to conduct remedial work.
<p>3.2 Risk Management</p> <ul style="list-style-type: none"> Are the significant IA risks managed at a level appropriate to their impact to the business critical systems? Is the SIRO aware of the residual risks that have been accepted and is he satisfied that these are within the risk appetite of the business? Have processes been put in place to deal with tolerated risks when they arise? Are processes in place for capturing the systemic IA risks facing the Department (e.g. those relating to network vulnerabilities) and for assessing the overall effect on the delivery of the Department's outputs? Is the Management Board made aware of the key IA risks affecting business critical systems, together with the systemic IA risks that impact on the delivery of the Department's outputs? 	<ul style="list-style-type: none"> Evidence to show that the significant IA risks to business critical systems are escalated to the SIRO. Endorsement of the residual risks relating to business critical IS. Details of the process. Evidence to show that the SIRO is aware of the systemic IA risks and has commissioned work to address the inherent risks to the delivery of the Department's outputs. Main Board papers showing submission of data and subsequent actions being taken
<p>3.3 Accreditation</p> <ul style="list-style-type: none"> Are all business critical IS accredited and have all of the significant, through-life (from concept to disposal) IA risks to business critical systems been captured? 	<ul style="list-style-type: none"> Details of the accreditation status of all business critical IS and evidence to show that all significant IA risks, but particularly those relating to in-service systems, are captured..

LEVEL 4 – Quantitatively Managed - The Number of Corporate Exceptions to Implementing IA Processes is Known & Reported

Areas to Probe	Evidence Expected
<p>4.1 Risk Assessments</p> <ul style="list-style-type: none"> Is a systematic process in place to conduct operational and technical risk reviews of all IS and their related business policies and processes? 	<ul style="list-style-type: none"> Schedule of reviews and action plans to conduct remedial work
<p>4.2 Risk Management</p> <ul style="list-style-type: none"> Has the regime set up to manage the IA risk to business critical systems been extended to embrace all systems? Is there an effective process in place to aggregate the individual system IA risks to produce a corporate IA risk picture 	<ul style="list-style-type: none"> Evidence required is the same as that detailed above for business critical systems. Evidence of regular updating in line with changes in strategic direction and the environment. Details of the process and its effective use, including endorsement of the residual risks relating to all IS.

UNCLASSIFIED

<p>of the residual risks that have been accepted?</p> <ul style="list-style-type: none"> • Are key vulnerabilities that are common to more than one system captured with a view to assessing the overall impact to the Department if that vulnerability were to be exploited? • Is there a process in place to assess where an IA weakness in a non-business critical system could undermine the Integrity, Availability or Confidentiality of a business critical system? • Is the Management Board made aware of the key IA risks affecting all systems, together with the systemic IA risks that impact on the delivery of the Department's outputs? • What proactive and reactive measures, including resources can the SIRO deploy to limit the business impact of risks when they materialise? 	<ul style="list-style-type: none"> • Details of the process and its effective use. • Details of the process and its effective use. • Main Board papers showing submission of data and subsequent actions being taken. • Details of the planned responses to key risks.
<p>4.3 Accreditation</p> <ul style="list-style-type: none"> • Are all IS accredited and have all of the significant, through-life (from concept to disposal) IA risks been captured? • Does a systematic process of accreditation and re-accreditation exist? • Are there sufficient qualified and trained accreditors to manage the work-load? 	<ul style="list-style-type: none"> • Details of the accreditation status of all IS and evidence to show that all significant IA risks, but particularly those relating to in-service systems, are captured.. • Details of the process. • Details of the accreditation work-load.

LEVEL 5 – Optimised - Responsive IA processes are integrated as Part of Normal Business

Areas to Probe	Evidence Expected
<p>5.1 Risk Management</p> <ul style="list-style-type: none"> • Is the Main Board regularly presented with an accurate picture of the IA risk exposure of the Department? • Does the Main Board regularly review the IA risk exposure and risk appetite of the Department? • Are the Department's external stakeholders and particularly those with whom it shares information, content with the IA risk exposure of the Department? 	<ul style="list-style-type: none"> • Main Board papers and Annual Departmental Report. • Evidence that decisions have been made based on expert guidance. • Internal and external audit reports and other assessments. • Main Board papers. • Main Board papers.

4. Through-Life IA Measures

Level 1 – Initial Awareness of the Criticality of IA to the Business and its Legal Requirements	Level 2 – Established IA Processes are Institutionalised	Level 3 – Business Enabling IA Processes are Implemented in Critical Areas of the Business	Level 4 – Quantitatively Managed The Number of Corporate Exceptions to Implementing IA Processes is Known & Reported	Level 5 – Optimised Responsive IA processes are integrated as Part of Normal Business
The requirement for taking a coordinated and systematic approach to through-life IA measures is understood and plans exist to determine the status of existing IS. All new IS are subject to through-life IA measures to deal with the full range of vulnerabilities and threats to information, including those arising from personnel behaviour, business process, natural disaster and malicious intent. The Department has a Forensic Readiness Policy.	The status of the through-life IA measures employed across the Department is determined and gaps are identified. A risk based programme of work is initiated to address the identified weaknesses in the technical, personnel, physical and procedural aspects of assurance, where this is justified by the business need.	Systematic, through-life processes are in place to assure all IS which are critical to the Department's business. Regular technical and operational risk reviews are undertaken and an effective process is in place to verify that remedial work is completed in a timely manner.	Level 3 processes are extended to embrace all of the Department's IS. Details of the IS that are not maintaining effective IA measures are known and are reported to the Main Board. Metrics on all IA related incidents and problems are produced and reported	Incident and problem management processes adapt to new risks and problems. The need to maintain the through-life assurance of IS becomes embedded across the Department so that changes can be made in IS to match the business tempo, without introducing undue vulnerabilities.

Goal A full range of IA control measures are implemented in a cost effective way to reduce the vulnerability of IS to compromise throughout their service life (from system concept to equipment disposal) and to deal with incidents in a way that reduces the business impact.

Justification Without effective control measures IS are susceptible to compromise, which could undermine the confidentiality, integrity or availability of the information and thus have a detrimental effect on the business. Even with the best control measures it is likely that incidents will happen and therefore it is important that an incident management capability is provided to deal with the incident and ensure lessons are learned.

LEVEL 1 – Initial - Awareness of the Criticality of IA to the Business and its Legal Requirements

Areas to Probe	Evidence Expected
<p>1.1 General</p> <ul style="list-style-type: none"> Does the Department understand the need to take a coordinated and systematic approach to IA measures for both information and the related IS through their whole life and do plans exist to determine their ongoing status? At the ICT level, what evidence is there to suggest that the Department is implementing through-life IA measures in a co-ordinated way, rather than on a system-by-system basis? Does the Department have plans to determine the status of the IA control measures in use on all existing IS? Does the Department make best use of the knowledge and experience of its commercial partners drawing on their internal best practice? Are strong and effective arrangements in place to safeguard unencrypted personal information collected, held, processed or transferred within the Department? Where applicable, does the Department comply with HMG IA Standard No.4 – Communications Security and Cryptography (parts 1-3) for the protection of protectively marked material? Is particular attention paid to the circumstances when encryption is required, the requirement to only use CESG approved solutions and the control mechanisms for cryptographic items? Where applicable, are the cryptographic key management arrangements satisfactory and do they meet the needs of the business? Where applicable, is the requirement for specified levels of personnel security clearance for individuals handling cryptographic items understood by the Department and is it complied with? 	<ul style="list-style-type: none"> Evidence to show that IRM is not just considered from the technical standpoint. Plans to show that a coordinated view is being taken to establish and maintain effective through-life IA control measures. Analysis of the current through life measures Taking a coordinated approach. Implementing cross-cutting measures that impact on more than one system. Details of the plans. Details of engaging with commercial delivery partners to implement best practice. Details of the process by which unencrypted personal information is subject to strong safeguards. Details of measures employed by the ComSO. Details of any decision making relating to the use of cryptographic protection. Details of the key management arrangements. Vetting details

<p>1.2 Physical & Environmental Security Measures</p> <ul style="list-style-type: none"> • Are physical protection measures and access controls to sites, buildings and equipment rooms adequate to protect the information contained? In particular, are adequate physical security measures in place to safeguard PROTECT level information held in both paper and electronic form? • Does the Department follow the specific Government procedures to manage the risk posed by eavesdropping and electro-magnetic emanations? 	<ul style="list-style-type: none"> • Details of physical protection measures employed. • Details of the number of trained individuals available, the procedures used and when last they were employed.
<p>1.3 Personnel Security Measures</p> <ul style="list-style-type: none"> • Does the Department apply a security checking and/or vetting process to its staff before they are given access to sensitive information? • Is the vetting process rigorous enough to meet the business need? • Are ICT users with higher levels of privilege and/or potentially wide access (e.g. system administrators, architects, programmers etc.) or those responsible for ICT security subject to vetting appropriate to the protective marking of the aggregated information being processed? • Are members of the Department, Delivery Partners and employees of 3rd party suppliers required to sign confidentiality, or non-disclosure agreements, stating their responsibilities for information security, as part of their initial terms and conditions of contract? • Is there a process in place to ensure that all employees, contractors and 3rd party users of the Department's information surrender all of the Department's information assets in their possession upon the termination of their employment, contract, or agreement? • Are the access rights of all employees, contractors and 3rd party users, to the Department's information and information processing facilities removed upon the termination of their employment, contract, or agreement? 	<ul style="list-style-type: none"> • Details of the security checking and vetting process, to include lead times and backlog. • Details of how staff are employed before their vetting comes through. • Details of the process used to ensure all such uses are of the appropriate vetting status. <ul style="list-style-type: none"> ▪ Details of the process and any results of assessments as to whether it is sufficient to meet the needs of the business. ▪ Details of the process and any results of assessments as to whether it is sufficient to meet the needs of the business. ▪ Details of the process and any results of assessments as to whether it is sufficient to meet the needs of the business.
<p>1.4 Acceptable Use Policy</p> <ul style="list-style-type: none"> • Is there an effective Acceptable Use Policy? 	<ul style="list-style-type: none"> • Policy exists with effective sanctions and a method exists to assess compliance with policy. Evidence that users are informed of the policy.
<p>1.5 Remote Working</p> <ul style="list-style-type: none"> • Does the Department have a remote working (e.g. home or mobile) policy that complies with the requirements of HMG SPF? • Is there a policy covering the control of removable media, to include laptops, removable disks, CDs, USB memory sticks, PDAs and media card formats? • Is the Department's Remote Working Policy aligned to the mandatory requirements of the DHR? In particular, does the policy require line management to record the reason why a particular solution identified in Paragraph 11 of IS6 has been adopted to meet the business need and does it specifically prohibit the storage of protectively marked information on unprotected privately owned computers? 	<ul style="list-style-type: none"> • Details of the policy and how staff are made aware of it. • Details of the policy and how staff are made aware of it. • Evidence that the DHR mandatory requirements are reflected in the policy
<p>1.6 IA Incident Management</p> <ul style="list-style-type: none"> • Does the Department have clear policies and processes for reporting, managing and resolving IA incidents and do these policies clearly define the responsibilities of individuals charged with managing such incidents? • Is the policy fit for purpose? • How are staff made aware of the policy? • Are all security incidents reported routinely to: a) The appropriate Departmental security authorities, b) The HMG incident management bodies: GovCERT for network incidents and CINRAS for communications security (involving cryptographic items) and c) The Information Commissioner's Office and IS&A within the Cabinet Office for significant actual or possible losses of personal data? • Does the Department have a Forensic Readiness Policy (FRP) which is designed to maximise the ability of the Department to preserve, analyse and use evidence for legal and management purposes derived from an IS involved in an IRM incident? Is it fit for purpose? 	<ul style="list-style-type: none"> • Policy document • Details of exercising the policy and how it is promulgated in a way that staff know about it and what to do. • Details of incidents reported in the last 6 months to GovCERTUK, CINRAS, the ICO and the CO. • FRP and details of any testing of the efficacy of the FRP.
<p>1.7 IT Service Management</p> <ul style="list-style-type: none"> • Are those responsible for ICT service management aware of the need to exercise effective management of the security aspects of their role? • Is there an inventory of properly labelled ICT system assets for new IS and is the ownership understood? 	<ul style="list-style-type: none"> • Clear understanding and commitment by those responsible for ICT service management is expressed in management documents. • ICT system asset registers are maintained and used effectively.

UNCLASSIFIED

<ul style="list-style-type: none"> • Is IA embedded within IT service management procedures for all new IS so that they are operated and administered in accordance with Security Operating Procedures (Sy Ops), including effective configuration management? • Are 3rd party suppliers held adequately accountable for the IA of new IS? • Is the Department aware of the current off-shoring policy (specifically that relating to personal data contained in IS6) and the current guidance (contained in GPG No 6), particularly the requirement to gain Cabinet Office clearance before entering into any new off-shoring arrangements involving personal data? 	<ul style="list-style-type: none"> • Evidence of clearly documented processes and procedures. Sy Ops and security policy are produced for each IS. The configuration and change control process aligns with the security policy requirements of the RMADS. • Legally binding contract and service level agreements covering IA responsibilities are in place underpinned by an effective audit regime. • Appropriate internal directives ensuring that the security risks of new IS procurements are managed in accordance with current policy.
<p>1.8 Business Continuity (BC) & Disaster Management (DM)</p> <ul style="list-style-type: none"> • Are the appropriate BC & DM measures in place for all new IS? • Are back-up processes institutionalised for all new IS? • Is there a systematic methodology for testing BC & DM measures for all new IS? • Are effective arrangements in place to safeguard unencrypted personal information contained on back up media? 	<ul style="list-style-type: none"> • Evidence of BC & DM measures. • Details of corporate policy and its implementation for new IS. • Recent BC & DM test report. • Details of the process by which back-up media is safeguarded.
<p>1.9 Digital Obsolescence</p> <ul style="list-style-type: none"> • Has the Department recognised in their corporate IA risk register the risks to continuity of access to their business information assets arising from digital obsolescence? 	<ul style="list-style-type: none"> • Risk detailed in the SIRO's IA risk register.
<p>1.10 Access Management</p> <ul style="list-style-type: none"> • Do all new ICT systems have suitable identification and authentication controls to manage the risk of unauthorised access, enable auditing and the correct management of user accounts? • Is there an identification and authentication methodology established for new systems and is it effective? • Has the Department a plan to link access control mechanisms to HR processes so that accounts are created and cancelled to match staff turnover? • Is a process in place to ensure that all remote computers that access personal data are password protected? • Are arrangements in place to log the activity of users in respect of protected personal data which is held electronically, particularly those working remotely and those with higher levels of functionality? • Is a process in place whereby managers check the access logs to ensure that the access policy is being applied correctly and take remedial action where applicable? • How are the specific DHR minimum measures for preventing unauthorised access to personal information contained on existing IS applied? • Where measures assessed as equivalent to these minimum measures have been applied, has the AO agreed the approach and has CO been notified in accordance with the DHR? 	<ul style="list-style-type: none"> • Details of the identification and authentication controls used. • Identification and authentication methodology follows guidance from NTA. • Details of the plan and how it is to be implemented. • Details of the process. • Details of what is logged and how this can be used to identify inappropriate access • Details of the process whereby managers take action to check access logs and what remedial action has been taken. • Details of how compliance with the minimum measures has been achieved and is assured. • Record of AO agreeing approach and details of how CO has been notified.
<p>1.11 Vulnerability Detection</p> <ul style="list-style-type: none"> • Is there a process for detecting IA vulnerabilities for new systems? • Have all in-service systems processing 100,000 or more individual personal data records been subject to independent penetration testing? • Has any action been taken to rectify any serious vulnerabilities detected as a result of the penetration tests? 	<ul style="list-style-type: none"> • Details of the process and its reach. • Penetration test report. • Details of any resulting action plan.
<p>1.12 Patching</p> <ul style="list-style-type: none"> • Does the Department have a patching policy covering all ICT systems, including operating systems and applications, to reduce the risk of known vulnerabilities? • Is a patching process specified for new IS with a distinction being made between routine, critical and emergency patches? • If a 3rd party supplier is to be involved in the supply of new IS, is the specification of the audit arrangements sufficient to establish that patching will be applied in compliance with policy? • Is the patching regime for new IS agreed with the Accreditor? • Is an effective process in place to ensure that the patching status of all remote computers processing personal data is kept updated in a timely manner? 	<ul style="list-style-type: none"> • Details of the Policy. • Details of the process. • Details of audit of 3rd party supplier patching compliance. • Details exist of the Accreditors agreement to the patching regime agreed for new IS. • Evidence of the process and its effective application.
<p>1.13 Lock-Down</p> <ul style="list-style-type: none"> • Does the Department have a lockdown policy to restrict unnecessary services and ensure that no user has more privileges (access and functionality) than required? • Is the process for locking down new IS to a secure 	<ul style="list-style-type: none"> • Details of the lockdown policy and how it is implemented. • Evidence of the process and its effective application to

UNCLASSIFIED

<p>configuration agreed with an Accreditor?</p> <ul style="list-style-type: none"> Is an effective process in place to ensure that all remote computers processing personal data are configured to minimise their functionality to the intended business use? 	<p>restrict user privileges to those required by the business.</p> <ul style="list-style-type: none"> Evidence of the process and its effective application.
<p>1.13 Anti-Malware Services</p> <ul style="list-style-type: none"> Does the Department have a policy to manage the risk posed by all forms of malicious software including viruses, spyware and phishing etc.? Is an effective process in place to ensure that all remote computers processing personal data have up to date anti-virus software? 	<ul style="list-style-type: none"> Details of the malware policy and how it is implemented Evidence of the process and its effective application.
<p>1.14 Controlled Disposal</p> <ul style="list-style-type: none"> Does the Department have effective processes in place for the controlled disposal (incineration, pulping or shredding) of protected information in paper form so that reconstruction is unlikely? Does the Department have effective processes in place for the controlled disposal (secure destruction, overwriting, erasure, or degaussing) of electronic media that have been used for protected information in accordance with HMG IA Standard 5 – Secure Sanitisation of Protectively Marked or Sensitive Information? 	<ul style="list-style-type: none"> Details of the process and how its effectiveness is determined. Details of the process and how its effectiveness is determined.

LEVEL 2 – Established IA Processes are Institutionalised

Areas to Probe	Evidence Expected
<p>2.1 General</p> <ul style="list-style-type: none"> Does an accurate picture exist of the status of the IA control measures in use across the Department? Does a gap analysis exist of the deficiency in IA control measures in use across the Department? Does a risk based programme of work exist to address the issues raised in the gap analysis? Has the Department established effective methodologies to make all users of ICT systems familiar with the security operating procedures governing their use at induction and annually thereafter? 	<ul style="list-style-type: none"> Details of the IA control measures in use. Gap analysis report. Details of the plans that exist to address the identified weaknesses in IA control measures needed to support the business need. Details of the process and its efficacy.
<p>2.2 Physical and Environmental Security Measures</p> <ul style="list-style-type: none"> Does the Department, its Delivery Partners and its 3rd party suppliers have processes in place to ensure that all locations where information and system assets (including cryptographic items) are kept have appropriate levels of physical security as set out in the HMG SPF? 	<ul style="list-style-type: none"> Details of the processes used and any assurance activity undertaken, together with details of any remedial action taken
<p>2.3 Personnel Security Measures</p> <ul style="list-style-type: none"> Do the personnel security measures in use by the Department, its delivery partners and its 3rd party suppliers, particularly in terms of security checking and vetting, meet HMG SPF Tier 3 requirements? 	<ul style="list-style-type: none"> Details of any security checking and vetting assurance activity undertaken, together with details of any remedial action taken
<p>2.4 IT Service Management</p> <ul style="list-style-type: none"> Do those who are responsible for ICT service management recognise the need for an institutionalised approach to the management of IA? Do those responsible for ICT service management allocate sufficient resource and funding to tackle IA issues? Has the Department catalogued and assessed the ownership, business criticality and IA requirements of all ICT system assets? Is IA good practice institutionalised into the ICT service management function so that systems are likely to be operated and administered according to corporate security operating procedures? Are 3rd party suppliers applying effective IA measures and are they being held accountable for non-compliance? 	<ul style="list-style-type: none"> Policy, guidance and direction have been issued that go beyond the need to achieve mandatory SPF compliance and which aim to embed a systematic approach to IA. The resolution of IA issues is given appropriate priority in the programme to address IT service management requirements. ICT system asset registers are accurate and are used to determine the priority of work to rectify IA issues Evidence of the application of clearly documented processes and procedures. Details of the measures 3rd party suppliers are employing are known and are subject to audit. Where extant contractual arrangements preclude legally binding contracts and service level agreements covering IA responsibilities, evidence exists of the Department employing alternative ways of achieving desired outcome.

UNCLASSIFIED

<p>2.5 IA Incident Management</p> <ul style="list-style-type: none"> • Is there a nominated IA Incident Manager and is the individual trained and competent to perform the role? • Is there an effective IA Incident Management Plan, including an escalation process and has it been tested? • Does the IA incident management Plan take account of the Forensic Readiness Policy? • Is root-cause analysis performed and is an analysis of any trends established? • Lessons are learned and shared across HMG IA community. <p>• Is adequate training in IA incident management given?</p> <p>• Are all users made aware of the IA incident management and reporting procedures?</p>	<ul style="list-style-type: none"> • TORs are established and the individual is trained to discharge their duty in a competent manner. • A workable process exists to reduce the business impact of any incident, to learn lessons and maintain forensic information, where this is appropriate. Date of when the effectiveness of the plan has been evaluated. • Evidence of successful application of these techniques. • Evidence of Lessons Learned Reports and engagement with external HMG stakeholders. • Details of the training given and records of who has undergone training. • Details of how information about the procedures is disseminated and how efficacy of dissemination.
<p>2.6 Business Continuity (BC) & Disaster Management (DM)</p> <ul style="list-style-type: none"> • Does the Department have appropriate Business Continuity and Disaster Recovery Plans for all locations where information and system assets (including cryptographic items) are kept? • Is the need for effective back-up processes understood and do plans exist to implement appropriate BC & DM measures for all IS? • Is a systematic methodology in place for testing BC & DM measures for all IS? 	<ul style="list-style-type: none"> • Departmental BC & DM policy complies with HMG SPF. • Evidence planning for the implementation of effective BC & DM measures. • Details of corporate policy and its implementation. <p>• Recent BC & DM test report and schedule of tests.</p>
<p>2.7 Digital Obsolescence</p> <ul style="list-style-type: none"> • Do Departmental strategies and policies for IT, IA and Information Management reflect the need to identify and mitigate digital obsolescence risks? • Has the Department engaged its 3rd party ICT providers in digital obsolescence risk management? <p>• Is there a documented plan for undertaking a risk assessment process to identify the specific digital obsolescence risks to the department, with timescales, resources and a board-level SRO?</p>	<ul style="list-style-type: none"> • Strategy and Policy documentation reflect need to manage digital obsolescence risks. • Departments have met 3rd party suppliers and have agreed that they need to be involved in plans to deal with the Department's digital obsolescence risks. • Details of the Risk Assessment Plan, which is consistent with the Digital Continuity approach and Guidance from The National Archives (TNA).
<p>2.8 Access Management</p> <ul style="list-style-type: none"> • Has a corporate identification and authentication methodology been established and is it effective? • Is an audit regime in place for access control? • Are access lists kept up-to-date and are they aligned to personnel security and HR processes? • How are they assured? 	<ul style="list-style-type: none"> • Identification and authentication methodology follows guidance from NTA. • Audit logs and related management process. • Documented processes exist, together with evidence of accounts being created and cancelled to match staff turn over. • Details of assurance of the process
<p>2.9 Vulnerability Detection</p> <ul style="list-style-type: none"> • Is the process for detecting IA vulnerabilities institutionalised? • Are specific objectives set for reducing vulnerabilities based upon threats, ease of exploitation and potential impact? • Are penetration tests regularly undertaken by an approved authority and recommendations acted upon? • What access to up-to-date sources of publicly available vulnerabilities is available? • What vulnerability analysis tools are available and are the staff trained to use them? 	<ul style="list-style-type: none"> • Details of the process and its reach. • Details of objectives and plan for reducing vulnerability. • Penetration reports and subsequent action plans. • Details of accesses available and use made of the data. • Details of the tools and the training given to the personnel who use them
<p>2.10 Patching</p> <ul style="list-style-type: none"> • Has a comprehensive patching regime been introduced? <p>• If a 3rd party supplier is involved, are the audit arrangements sufficient to establish that patching is applied in compliance with policy?</p>	<ul style="list-style-type: none"> • A comprehensive patching regime is in existence and where it is applied there is evidence that patches are applied in a time scale applicable to the seriousness of the vulnerability. • Details of audit of 3rd party supplier patching
<p>2.11 Lock-Down</p> <ul style="list-style-type: none"> • Is the process for locking down IS to a secure configuration agreed with an Accreditor institutionalised? 	<ul style="list-style-type: none"> • Evidence of the process and its effective application to restrict user privileges to those required by the business.
<p>2.12 Anti-Malware Services</p> <ul style="list-style-type: none"> • Are Anti Virus Service (AVS) processes institutionalised? 	<ul style="list-style-type: none"> • Details of the process and methodology for assessing compliance?

LEVEL 3 – Business Enabling IA Processes are Implemented in Critical Areas of the Business

Areas to Probe	Evidence Expected
<p>3.1 IT Service Management</p> <ul style="list-style-type: none"> Have those responsible for IT service management been set corporate objectives, priorities and qualitative performance targets for the improvement of the IA aspects of service management? Have the process or service owners for IT service management been made responsible for delivering specific levels of improvement in IA? Is IA embedded within IT service management procedures for all business critical IS? <p>Are the IA elements of 3rd party ICT services relating to business critical IS actively monitored and managed?</p>	<ul style="list-style-type: none"> Details of the objectives, priorities and qualitative performance targets. Details of the targets that have been set and the method by which reporting against them. Evidence of clearly documented processes and procedures. Comprehensive and consistent Sy Ops are applied across the Department to business critical IS. The IA performance of 3rd party ICT suppliers is qualitatively assessed and they are held to account for any deficiencies.
<p>3.2 Business Continuity (BC) & Disaster Management (DM)</p> <ul style="list-style-type: none"> Are the appropriate BC & DM measures in place for all business critical IS? Are back-up processes institutionalised for all business critical IS? Is there a systematic methodology for testing BC & DM measures for all business critical IS? 	<ul style="list-style-type: none"> Evidence of BC & DM measures. Details of corporate policy and its implementation for all business critical IS. Recent BC & DM test report.
<p>3.3 Digital Obsolescence</p> <ul style="list-style-type: none"> Has a risk assessment been undertaken to identify the Department's specific digital obsolescence risks to the continuity of their information assets, and has a risk mitigation plan, with timescales and resources, been signed off by board-level SRO? Is the Department undertaking any initial, priority digital obsolescence risk mitigation action, as identified in their Risk Mitigation Plan, to mitigate any immediate risks to continuity of access to key business information assets? Is work in hand to address any necessary changes in agreements and contracts with 3rd party suppliers to implement the required digital obsolescence mitigation activity? 	<ul style="list-style-type: none"> Detail of the Risk Assessment, with technical profile of information assets (to include formats, file type, age of files etc) Detail of the Risk Mitigation plan, which is consistent with the Digital Continuity approach and Guidance from The National Archives (TNA) Details of initial, prioritised risk mitigation interventions based on information asset value and desired business outcomes Departments have put in place, or are in the process of drafting, agreements or contract changes with IT providers in accordance with their risk mitigation plan.
<p>3.4 Access Management</p> <ul style="list-style-type: none"> Is there an identification and authentication methodology established for all business critical systems and is it effective? Is an audit regime in place for access control for all business critical IS? 	<ul style="list-style-type: none"> Identification and authentication methodology follows guidance from NTA. Audit logs and related management process.
<p>3.5 Vulnerability Detection</p> <ul style="list-style-type: none"> Is the process for detecting IA vulnerabilities for business critical systems institutionalised? Are specific objectives set for reducing vulnerabilities based upon threats, ease of exploitation and potential impact? Are penetration tests regularly undertaken by an approved authority and recommendations acted upon? 	<ul style="list-style-type: none"> Details of the process and its reach. Details of objectives and plan for reducing vulnerability. Penetration reports and subsequent action plans.
<p>3.6 Patching</p> <ul style="list-style-type: none"> Is the patching process for all business critical IS institutionalised with a distinction being made between routine, critical and emergency patches? If a 3rd party supplier is involved, are the audit arrangements sufficient to establish that patching is applied in compliance with policy? Is the patching regime for all business critical IS agreed with the Accreditor? 	<ul style="list-style-type: none"> A comprehensive patching regime is in existence and evidence exists that for new IS patches are applied in a time scale applicable to the seriousness of the vulnerability. Details of audit of 3rd party supplier patching compliance. Details exist of the Accreditor's agreement to the patching regime agreed for all business critical IS.
<p>3.7 Lock-down</p> <ul style="list-style-type: none"> Is the process for locking down all business critical IS to a configuration agreed with an Accreditor institutionalised? 	<ul style="list-style-type: none"> Evidence of the process and its effective application to restrict user privileges to those required by the business.
<p>3.8 Anti-Malware Services</p> <ul style="list-style-type: none"> Are all business critical IS subject to an anti-malware regime agreed with the Accreditor? Are AVS and back-up processes institutionalised for all business critical IS? 	<ul style="list-style-type: none"> Evidence of the process and its effective application. Details of the process and methodology for assessing compliance.
<p>3.9 IA Incident Management</p> <ul style="list-style-type: none"> Are metrics available for all IA related incidents and problems relating to business critical IS? 	<ul style="list-style-type: none"> Comprehensive data is available and is reported to senior managers in a way that enables effective action to be taken.

UNCLASSIFIED

LEVEL 4 – Quantitatively Managed - The Number of Corporate Exceptions to Implementing IA Processes is Known & Reported

Areas to Probe	Evidence Expected
<p>4.1 General</p> <ul style="list-style-type: none"> Do accurate details exist of the status of IA control measures which impact on all IS in use across the Department? Is the SIRO and hence the Main Board aware of those IS that are not maintaining effective IA control measures and has an analysis been performed to determine the business impact if an IA attack exploited the vulnerabilities? 	<ul style="list-style-type: none"> Management reports. Management reports.
<p>4.2 IT Service Management</p> <ul style="list-style-type: none"> Have metrics been developed to assess the IA aspects of IT service management across the Department to ensure that the service provided meets the business need with an acceptable level of information risk? Is the IT service management Department able to predict the service demand from the business and posture secure IT services to meet the business need in a timely manner? Is IA embedded within IT service management procedures for all IS? <p>Are the IA elements of 3rd party ICT services relating to all IS actively monitored and managed?</p>	<ul style="list-style-type: none"> A process is in place for the metrics to be reviewed by senior management and there is evidence of effective action being taken to address concerns. The likely service demand is quantified and processes are in place to provide secure ICT services to meet the needs of the business. Evidence of clearly documented processes and procedures. Comprehensive and consistent Sy Ops are applied across the Department to all IS. The IA performance of 3rd party ICT suppliers is qualitatively assessed and they are held to account for any deficiencies.
<p>4.3 Business Continuity (BC) & Disaster Management (DM)</p> <ul style="list-style-type: none"> Are the appropriate BC & DM measures in place for all IS? Are back-up processes institutionalised for all IS? Is there a systematic methodology for testing BC & DM measures for all IS? 	<ul style="list-style-type: none"> Evidence of BC & DM measures. Details of corporate policy and its implementation for all IS. Recent BC & DM test report.
<p>4.4 Digital Obsolescence</p> <ul style="list-style-type: none"> Is the Department undertaking digital obsolescence risk mitigation action, as identified in their Risk Mitigation Plan, to ensure continuity of access to all relevant business information assets? Are all information assets subject to regular digital obsolescence risk reviews and mitigation schedules, with exceptions and legacy systems/assets identified and agreed? <p>Has digital obsolescence and incidents affecting the continuity of access to business information assets been incorporated into incident reporting procedures?</p> <ul style="list-style-type: none"> Are the Department's 3rd party suppliers fulfilling contractual obligations around digital obsolescence and is there a mechanism to monitor compliance? 	<ul style="list-style-type: none"> Details of risk mitigation interventions at the policy, procedural and technical levels and evidence of business outcomes and benefits being tracked and realised Evidence that information asset owners are aware of digital obsolescence risks to their information assets Exceptions to risk mitigation actions and plans to address these gaps are documented in SIRO/board-level reporting Detail of incident reporting procedures and incident reports, if any SLA agreements and relevant KPIs, with contract management or service review processes
<p>4.5 Access Management</p> <ul style="list-style-type: none"> Is there an identification and authentication methodology established for all IS and is it effective? Is an audit regime in place for access control for all IS? 	<ul style="list-style-type: none"> Identification and authentication methodology follows guidance from NTA. Audit logs and related management process.
<p>4.6 Vulnerability Detection</p> <ul style="list-style-type: none"> Is the process for detecting IA vulnerabilities for all IS institutionalised? Are specific objectives set for reducing vulnerabilities based upon threats, ease of exploitation and potential impact? Are penetration tests regularly undertaken by an approved authority and recommendations acted upon? 	<ul style="list-style-type: none"> Details of the process and its reach. Details of objectives and plan for reducing vulnerability. Penetration reports and subsequent action plans.
<p>4.7 Patching</p> <ul style="list-style-type: none"> Is the patching process for all IS institutionalised with a distinction being made between routine, critical and emergency patches? If a 3rd party supplier is involved, are the audit arrangements sufficient to establish that patching is applied in compliance with policy? Is the patching regime for new all IS agreed with the Accreditor? 	<ul style="list-style-type: none"> A comprehensive patching regime is in existence and evidence exists that for new IS patches are applied in a time scale applicable to the seriousness of the vulnerability. Details of audit of 3rd party supplier patching compliance. Details exist of the Accreditor's agreement to the patching regime agreed for all IS.
<p>4.8 Lock-down</p> <ul style="list-style-type: none"> Is the process for locking down all IS to a configuration agreed with an Accreditor institutionalised? 	<ul style="list-style-type: none"> Evidence of the process and its effective application to restrict user privileges to those required by the business.
<p>4.9 Anti-Malware Services</p> <ul style="list-style-type: none"> Are all IS subject to a malware regime agreed with the Accreditor? Are AVS and back-up processes institutionalised for all IS? 	<ul style="list-style-type: none"> Evidence of the process and its effective application. Details of the process and methodology for assessing compliance.

UNCLASSIFIED

<ul style="list-style-type: none"> Are details of malware incidents for all IS collated and reported to senior management? 	<ul style="list-style-type: none"> Details of recent reports submitted to senior management.
4.10 IA Incident Management <ul style="list-style-type: none"> Are metrics available for all IA related incidents and problems within the Department? 	<ul style="list-style-type: none"> Comprehensive data is available and is reported to senior managers in a way that enables effective action to be taken.

LEVEL 5 – Optimised - Responsive IA processes are integrated as Part of Normal Business

Areas to Probe	Evidence Expected
5.1 IT Service Management <ul style="list-style-type: none"> Is IA embedded within the culture of the IT service management organisation? Is there evidence of action being taken by the IT service management organisation to promote IA as an enabler of the business? 	<ul style="list-style-type: none"> Evidence that IA is viewed as a key discipline within IT professionals and the processes exist to monitor performance in such a way that management action can be taken to achieve continuous performance improvement as part of business as usual processes. Evidence of a unified approach.
5.2 Digital Obsolescence <ul style="list-style-type: none"> Is there a systematic process embedded for reviewing digital obsolescence risks and mitigation actions on a regular basis, as part of digital information lifecycle management processes? Are procedures in place to test accessibility of data over 5 years old to ensure continuity of access to information assets? Are policies and procedures in place to ensure that any new IS is assessed for impact on digital obsolescence and continuity of access to information assets, prior to implementation? Has digital obsolescence risk management been embedded as a key task within the Department's IA, IT and IM teams and business as usual processes? Is the Department sharing best practice and lessons learned about digital obsolescence risk management across government? 	<ul style="list-style-type: none"> Details of policies and procedures, evidence that these processes are implemented Details of procedures for testing and reports created post testing. Details of policies and procedures for implementing new IS, including change control Evidence of relevant staff training and objectives to demonstrate capability All IA, IT and IM policies and procedures include digital obsolescence risk management Evidence that retention schedules are being properly implemented Evidence of shared experiences amongst relevant communities, feedback to the National Archives.
5.3 Access Management <ul style="list-style-type: none"> Is investment in access management optimised across personnel, physical, procedural and technical aspects and against functional delivery? 	<ul style="list-style-type: none"> Evidence that continual improvement in access management has a strategic business focus, with a strong and balanced understanding of the value of security to the business.
5.4 Vulnerability Detection <ul style="list-style-type: none"> Does the Department foster and develop the expertise to detect vulnerabilities in the business context and is effective action taken to act on reports made? 	<ul style="list-style-type: none"> Details of process to assess vulnerabilities in the business context. Details of timely remedial action taken to act on vulnerability reports.
5.5 Patching <ul style="list-style-type: none"> Is the management of patching automated and integrated and as a result are alerts produced when an IS breaks the terms of its patching regime? 	<ul style="list-style-type: none"> Details of the automated process and the exception reporting mechanism.
5.6 Lock-down <ul style="list-style-type: none"> Is there a process to continually refine lock-down configurations and processes to minimise IA vulnerabilities? 	<ul style="list-style-type: none"> Evidence of the process and its effective application.
5.7 Anti-Malware Services <ul style="list-style-type: none"> Are objectives set for eliminating the root causes of malware incidents and is there an effective funded programme of continuous improvement? 	<ul style="list-style-type: none"> Realistic objectives are in place with an effective implementation programme.
5.8 IA Incident Management <ul style="list-style-type: none"> Is the Department capable of identifying warning signs for potential incidents and taking action to avoid or prevent the incident from occurring? Is there effective engagement with external stakeholders so that the Department learns from the experience of others? 	<ul style="list-style-type: none"> Details of the process and successful interventions. Details of the engagement process and action taken to avoid potential incidents.

5. Assured Information Sharing

Level 1 – Initial Awareness of the Criticality of IA to the Business and its Legal Requirements	Level 2 – Established IA Processes are Institutionalised	Level 3 – Business Enabling IA Processes are Implemented in Critical Areas of the Business	Level 4 – Quantitatively Managed The Number of Corporate Exceptions to Implementing IA Processes is Known & Reported	Level 5 – Optimised Responsive IA processes are integrated as Part of Normal Business
The requirements for sharing information across the Department's boundaries are identified and arrangements are in place to work with external stakeholders to achieve shared IA objectives. The need to understand and control how IS interact with one another both internally and externally is acknowledged and work to implement IA control mechanisms is implemented.	Network boundaries are defined and policies for sharing information across these boundaries are defined and implemented, including those with delivery partners and 3 rd party suppliers. The Department takes an enterprise-wide approach to the security of new IS and a systematic method is used to implement the control measures needed to mitigate problems when inter-connecting IS.	The business activities that are critically dependant on information sharing are known. A comprehensive protective monitoring regime is implemented to provide situational awareness and enable essential information flows to be maintained. The Department has effective processes in place to respond in a timely manner to internal and external incidents and problems so that the impact on stakeholders and on the business is controlled.	Level 3 measures are extended so that incident management moves from being reactive to proactive. The impact of incidents and problems on information sharing both internally and externally is minimised. Metrics on system and network incidents and problems, and their subsequent resolution are collected and this information is reported to the Main Board and is shared with external stakeholders.	The definition and implementation of network boundaries and the associated protective monitoring regime is continually improved to reduce the departmental and collective, shared exposure to information risk.

Goal Information is readily shared within the Department and with external stakeholders in an assured and cost effective way that maximises the benefits delivered by HMG's Transformational Government and Shared Services Initiatives, whilst reducing the business impact should a compromise occur.

Justification The business demand for sharing data from one system to another invariably introduces vulnerabilities, particularly if the design of distributed systems is not properly managed so that the vulnerabilities in one IS can be used to exploit connected systems. In such an inter-connected environment the risk of compromise is high and therefore effective measures are needed to manage and control the spread of detrimental effects when they arise, whilst simultaneously minimising the impact on the business.

LEVEL 1 – Initial - Awareness of the Criticality of IA to the Business and its Legal Requirements

Areas to Probe	Evidence Expected
<p>1.1 Information Sharing</p> <ul style="list-style-type: none"> Are the risks associated with sharing information both within the Department and with external stakeholders understood and managed appropriately? Is the business need to share information with external organisations understood and is this need embodied in policy statements? Does a mechanism exist to take into account the IA needs of OGDs and Stakeholders when handling their information? Is the responsibility to work with external organisations to achieve shared IA objectives clearly articulated and is this achieved in practice? Is there someone clearly accountable for implementing the policy? 	<ul style="list-style-type: none"> Process exists to assess and manage the risks associated with internal and external information sharing Information Sharing Policy statement. Where inter-Departmental working is involved there is evidence that the Department understands the need to gain the confidence and trust of other stakeholders and proactively aims to manage, and where required, meet their expectations. Details of how policy is to be implemented and by whom.
<p>1.2 Information Transfer</p> <ul style="list-style-type: none"> Where personal information has to be accessed remotely are effective mechanisms in place to protect the information in transit using approved devices in accordance with the DHR mandatory requirements? How are the measures listed at Paragraph 12 of IS6 for the protection of personal data on removable media being applied? How are staff (within the Department, its delivery partners and its 3rd party suppliers) made aware of the DHR mandatory requirements? What assurance mechanism is in place to ensure that the DHR mandatory requirements are being applied in all areas? 	<ul style="list-style-type: none"> Details of how such remote access links are protected and how assurance is provided of the effectiveness of the protection. Details of the effective application of policy. Details of how the policy and arrangements are promulgated to all areas. Details of the assurance mechanism in place together with any reports that have been made.

UNCLASSIFIED

<p>1.3 Delivery of Services to the Citizen</p> <ul style="list-style-type: none"> Does the Department understand the need to secure the delivery of citizen facing services? Are these requirements embodied in standards that are clearly explained? Are the same protective measures used in transacting business with individual citizens? If not, is there a valid reason for not doing so? Is the approach adopted proportionate? 	<ul style="list-style-type: none"> Details of the policies and standards which the Department has chosen to apply for the delivery of secure services to the citizen. Details of the protective measures used and the analysis of why they have been chosen.
<p>1.4 Enterprise-Wide, Architectural Approach to IA</p> <ul style="list-style-type: none"> Does the SIRO understand the operational and financial benefit of adopting an enterprise wide, architectural approach to IA rather than implementing piecemeal controls on a system by system basis? Does a plan exist to take an enterprise-wide, architectural approach to IA within the Department? 	<ul style="list-style-type: none"> Policy papers examining the need for an enterprise-wide, architectural approach exist. Details of the plan.
<p>1.5 Network Security Management</p> <ul style="list-style-type: none"> Does the Department comply with all codes-of-connection, bilateral agreements and/or community or shared service security policies to which it is a signatory. Are the specific technical policies covering; patching, malware, boundary security devices, content checking/blocking and lockdown applicable to such agreements implemented effectively? Is the need to police these arrangements understood and is there a plan to police the arrangements? 	<ul style="list-style-type: none"> Details of how compliance is achieved. Evidence that the mandatory technical controls relating to such agreements are applied correctly. Evidence of plans to police Codes of Connection.
<p>1.6 Protective Monitoring</p> <ul style="list-style-type: none"> What protective monitoring capabilities does the Department employ? Are they effective and are the events generated audited and incidents responded to? Does the SIRO understand the benefits of investing in protective monitoring? Does a plan exist to investigate the introduction of a comprehensive, corporate protective monitoring regime? 	<ul style="list-style-type: none"> Details of current capability. Details of how the capabilities are used. Policy papers examining the need for enhancing protective monitoring. Details of the plan.

LEVEL 2 – Established - IA Processes are Institutionalised

Areas to Probe	Evidence Expected
<p>2.1 Information Sharing</p> <ul style="list-style-type: none"> Does the Department understand the need to, and value of, keeping the stakeholders with whom they share information informed of how they apply IRM? Are all network boundaries with the Department's IS throughout the delivery chain clearly identified and defined? Are the policies for sharing information across these boundaries clearly defined? Are there boundary control devices at all connection points with untrusted networks? Are these boundary controls fit for purpose i.e. are they sourced from trusted suppliers, are they installed correctly, are they patched and penetration tested regularly, are the logs audited and are incidents responded to in an effective manner? Is content checking in place to block inappropriate websites, control the downloading and uploading of data and to check e-mail and other electronic exchanges across boundaries? 	<ul style="list-style-type: none"> Information sharing agreements with other Departments and organisations contain evidence to show an open and collaborative approach to dealing with IRM issues. Details of network boundaries, the policies concerning information sharing across the boundaries. Details of the effective employment of boundary control devices in implementing the policy.
<p>2.2 Enterprise-Wide, Architectural Approach to IA</p> <ul style="list-style-type: none"> Has an enterprise-wide security architecture been specified that accurately reflects what the Department needs to discharge its business and is this used as a goal against which future programmes are specified? Is the security architecture endorsed by the business? Is the chosen architecture aligned to the pan-Government architecture being created by the CTO Council? Are new initiatives checked for compliance with the architecture before implementation? Is architectural compliance specified when procuring new IS? 	<ul style="list-style-type: none"> Details of enterprise security architecture and the methodology used to create the architecture. Endorsement of an enterprise-wide, architectural approach by the Main Board. Details of effective liaison with CTO Council. Details of how the enterprise security architecture is used in practice.
<p>2.3 Network Security Management</p> <ul style="list-style-type: none"> Does the Department have a network management board, or similar body, with clear lines of authority that takes decisions on network issues? Are network management policies endorsed by the SIRO? Are all codes-of-connection, bilateral agreements and/or 	<ul style="list-style-type: none"> TORs and minutes of network management board. Details of how the SIRO interacts with the Board. Details of the policing methodology and any measures of its

UNCLASSIFIED

<p>community or shared service security policies policed to assure compliance? Are processes for controlling access and configuration institutionalised?</p>	<p>effectiveness.</p> <ul style="list-style-type: none"> Evidence that Network Security Management is an accepted discipline in the working practices of the Department.
<p>2.4 Protective Monitoring</p> <ul style="list-style-type: none"> Are objectives set for the use of existing protective monitoring resources? <p>Are processes in place to make effective use of protective monitoring resources at network boundaries and are these processes institutionalised?</p> <ul style="list-style-type: none"> Are staff trained effectively to interpret the output from protective monitoring resources? How advanced is the plan to implement a comprehensive, corporate protective monitoring regime? Has use been made of the CESG IDS Service? 	<ul style="list-style-type: none"> Evidence of systematic employment of protective monitoring devices to achieve effect. Evidence that the use of protective monitoring devices is built into the working practices of the Department. Details of the skills levels and turnover of the staff involved in interpreting the data. Details of the plan to implement an holistic protective monitoring scheme. Details of any reports provided by CESG, together with details of any resulting action taken.

LEVEL 3 – Business Enabling - IA Processes are Implemented in Critical Areas of the Business

Areas to Probe	Evidence Expected
<p>3.1 Information Sharing</p> <ul style="list-style-type: none"> Are the information flows that support critical business activities known? Have these information flows been analysed to determine where there are key dependencies on specific elements of the infrastructure? Has a risk analysis been undertaken to minimise the risk posed by potential single points of failure? Is there sufficient linkage between the need to maintain information flow to support the business and the IA situational awareness activity? 	<ul style="list-style-type: none"> Documentary evidence that the critical information flows are known. Details linking logical information flows to the infrastructure supporting them Risk analysis with evidence that the risk is acceptable to the business. Clear linkage that the IA response is driven by the needs of the business.
<p>3.2 Enterprise-wide, Architectural Approach to IA</p> <ul style="list-style-type: none"> Does a central authority exist to control the granting of waivers to non compliant IS? Is the level of compliance with the security architecture known and managed? Is there a process for sharing the Departmental security architecture approach with external stakeholders? 	<ul style="list-style-type: none"> Details of the control exercised to maintain compliance with the enterprise security architecture. Details of liaison with external stakeholders.
<p>3.3 Network Security Management</p> <ul style="list-style-type: none"> Are network security management policies implemented in a structured manner to provide defence in depth? Is the planning of change based on a sound understanding of network vulnerabilities and the potential business impacts? Are attempts to intrude, whether successful or not, detected and managed? 	<ul style="list-style-type: none"> Details of how policies are designed to cater for the range of likely threats. Details of how the network security management organisation interacts with those delivering new and existing IS capability. Evidence of detection of live threats and results of penetration testing of capability.
<p>3.4 Protective Monitoring (e.g. IPS, IDS etc.)</p> <ul style="list-style-type: none"> Does a comprehensive, corporate protective monitoring capability exist? Does it provide situational awareness of the network, including all boundary points? Are anomaly detection techniques used? Is there effective engagement with CESG regarding the collection and supply of IDS threat signatures? Are processes in place to enable the sharing of protective monitoring data with external stakeholders in such a way that effective and timely action can be taken? 	<ul style="list-style-type: none"> Details of the corporate protective monitoring capability and how it provides effective situational awareness. Details of how anomaly detection is used. Details of the engagement and the use being made of the information supplied. Details of the interaction with OGDs with similar capabilities, together with external sources of expertise.

LEVEL 4 – Quantitatively Managed. The Number of Corporate Exceptions to Implementing IA Processes is Known & Reported

Areas to Probe	Evidence Expected
<ul style="list-style-type: none"> Does the protective monitoring regime provide a 24/7 incident management capability? Are the processes and procedures in place to take advantage of real-time indicators and warnings, so that proactive defensive action can be taken? Is a process in place to collate all data on system and network incidents and problems? Is this data used to provide real-time incident and problem management? Is there effective post incident and problem analysis process? Are the lessons identified in this analysis used effectively to tune the response to future situations? 	<ul style="list-style-type: none"> Details of how the 24/7 capability is provided. Details of how the 24/7 capability takes feeds from external agencies and how decisions are taken to activate defensive procedures in a timely manner. Details of the collation process and evidence of the effective use of the process. Evidence of the effective use of the data to act proactively when problems arise and react in a timely manner to incidents. Evidence that lessons are “learned” and appropriate action taken.

UNCLASSIFIED

<ul style="list-style-type: none">• Is there effective reporting to the SIRO and the Main Board?• Is the investment in network security management and protective monitoring perceived by the Main Board to provide value-for-money?• Is the Department engaged in an effective interchange of data with external stakeholders?	<ul style="list-style-type: none">• Evidence of SIRO engagement.• Reports presented to the Main Board to demonstrate how protective monitoring enables the business.• Evidence of a willingness to be open and share data and experience with external stakeholders.
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

LEVEL 5 – Optimised Responsive IA processes are integrated as Part of Normal Business

Areas to Probe	Evidence Expected
<ul style="list-style-type: none">• Is there a continuous improvement plan to update the network security management and protective monitoring processes and equipment to match the changing threat environment?• Are measures in place to measure the effectiveness of the investment in network security management and protective monitoring as a means to facilitating the trust needed for effective information sharing?	<ul style="list-style-type: none">• Plan to maintain the effectiveness of capability.• Metrics to establish value for money.

6. Compliance

Level 1 – Initial Awareness of the Criticality of IA to the Business and its Legal Requirements	Level 2 – Established IA Processes are Institutionalised	Level 3 – Business Enabling IA Processes are Implemented in Critical Areas of the Business	Level 4 – Quantitatively Managed The Number of Corporate Exceptions to Implementing IA Processes is Known & Reported	Level 5 – Optimised Responsive IA processes are integrated as Part of Normal Business
A compliance regime is established to confirm the effectiveness of IRM against mandated minimum standards. The Board's Audit Committee ensures that it receives comprehensive assurance on IRM and challenges assurance, where required. The Department reports annually on IA issues.	The Department has a comprehensive IRM compliance regime. External IA Review undertaken to provide independent assessment of progress towards compliance with the HMG Security Policy Framework (SPF) and national policy & standards.	Critical IA Review and internal audit recommendations are actioned and progress tracked.	IA incident and problem management processes are fully assured by internal audit. Main Board is aware of the significant areas of the Department's non-compliance with the HMG SPF and national policy & standards. Remedial action has been commissioned.	There are no critical or significant IA audit issues. Independent assessment of the Department's approach to IA shows that it is aligned with the National IA Strategy is fully compliant with the HMG SPF and national policy & standards. It is considered to be an exemplar of best practice across HMG.

Goal Effective compliance mechanisms provide positive assurance that Departmental policy is being implemented in an effective way to achieve the desired outcomes.

Justification Without effective audit and compliance mechanisms those IA control measures which cause inconvenience are likely to be ignored resulting in an increase in the risk to the Department's information.

LEVEL 1 – Initial - Awareness of the Criticality of IA to the Business and its Legal Requirements

Areas to Probe	Evidence Expected
1.1 Legislative Compliance <ul style="list-style-type: none"> How does the SIRO satisfy himself/herself that the Department is compliant with relevant legislation? Has this compliance been independently tested? 	<ul style="list-style-type: none"> Details of any assessment that has been undertaken. Evidence of Legal Advisor involvement with the Assessment Report.
1.2 Compliance Regime <ul style="list-style-type: none"> What form of compliance regime exists within the Department to ensure that IRM measures comply with endorsed Departmental policy? Is the Department fully compliant with the SPF mandatory measures, including those DHR measures detailed in IS6? If it is not, does the SIRO know which SPF mandatory measures have not been met and is he content to accept the risk? How does the SIRO ensure the effectiveness of the compliance regime? 	<ul style="list-style-type: none"> Details of the IRM compliance regime. Reports to the SIRO on SPF compliance. Details of risk assessments supporting decision. Details of any assessments undertaken on the sufficiency of the compliance regime.
1.3 Internal Assurance <ul style="list-style-type: none"> Does the Department have the ability to regularly audit information assets and ICT systems and are regular compliance checks carried out by the Accreditor, ITSO or similarly qualified person and are the results of these checks documented in the RMADS audit of the ICT system against configuration records. 	<ul style="list-style-type: none"> Details of compliance checks Sample RMADS
1.4 External Assurance <ul style="list-style-type: none"> Has an external audit been undertaken of the efficacy of the Department's IA control measures (e.g. ISO/IEC 27001:2005 Assessment, or alternative)? Are the control measures compliant with national policy? How is the effective application of the Remote Access Policy assured within the Department, its delivery partners and 3rd party suppliers? 	<ul style="list-style-type: none"> Audit report or ISO/IEC 27001:2005 assessment report. Details of any checks, audits or controls put in place to police the policy throughout all bodies to which the policy applies.
1.5 Audit Committee <ul style="list-style-type: none"> Does the Audit Committee consider IRM as an integral part of the Department's overall risk management regime? Has the Department's Information Risk Assessment been shared with, and discussed by the Audit Committee and the Main Board as required by the DHR? How does the Audit Committee gain positive assurance of the statements on Information Risk which are included in the SIC and the Department's Annual Report? Has the Chair of the Audit Committee provided a written judgement of information risk to inform the annual review of information risk prepared by the SIRO? 	<ul style="list-style-type: none"> Audit Committee minutes. Board Minutes and briefing notes. Details of audits used to provide assurance of SIC and Annual Report information. Example of a written report.

<p>1.6 Management Reports</p> <ul style="list-style-type: none"> • Is the detail concerning information risk contained in the management commentary to the Resource Accounts compliant with the DHR requirement? • Is the Department's annual report to the Cabinet Office comprehensive and does it give an accurate picture of the progress which is being made? 	<ul style="list-style-type: none"> • Annual Departmental Report includes summary material on information risk, covering the overall judgement in the SIC, the numbers of information risk incidents reported to the ICO, together with the numbers of people potentially affected, together with the actions taken to contain the breach and prevent recurrence. • Annual report required by the DHR
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

LEVEL 2 – Established - IA Processes are Institutionalised

Areas to Probe	Evidence Expected
<p>2.1 Compliance Regime</p> <ul style="list-style-type: none"> • How comprehensive is the compliance regime? • How is its effectiveness validated? • What action has been taken to address weaknesses found as a result of validation? 	<ul style="list-style-type: none"> • Details of the IRM compliance regime. • Assessment reports. • Details of remedial actions taken.
<p>2.2 Internal Assurance</p> <ul style="list-style-type: none"> • How are the physical and personnel security processes assured by audit and are any weaknesses identified rectified by prompt action? • Has an assessment been made of the Department's compliance with the mandatory measures contained in Tier 3 of the SPF, particularly those relating to IA? • Has an assessment been made of the compliance of the Department's delivery partner's and 3rd party suppliers with the mandatory measures contained in Tier 3 of the SPF, particularly those relating to IA? • Where there are non compliances, what remedial action is being taken in terms of contract amendment or service level agreement to bring these bodies into compliance? 	<ul style="list-style-type: none"> • Details of security audits and any follow-up action. • Assessment Report. • Assessment Report. • Details of what action has been taken.
<p>2.3 External Assurance</p> <ul style="list-style-type: none"> • When was the last independent IA Benchmarking Review conducted? • Have the recommendations from that Review been acted upon? 	<ul style="list-style-type: none"> • IA Benchmark Review Report and follow-up action plan

LEVEL 3 – Business Enabling - IA Processes are Implemented in Critical Areas of the Business

Areas to Probe	Evidence Expected
<p>3.1 Compliance Regime</p> <ul style="list-style-type: none"> • Are plans in place to action all of the recommendations made in all reviews and audits of the Department's IA posture relating to Business Critical IS and related processes? • Is progress against any improvement plans relating to Business Critical IS and related processes tracked and managed by the SIRO? 	<ul style="list-style-type: none"> • Plans and details of progress checking mechanisms. • Evidence of SIRO's engagement.
<p>3.2 External Assurance</p> <ul style="list-style-type: none"> • Has the IA risk management process, particularly as it applies to Business critical IS and processes, been subject to independent assurance? 	<ul style="list-style-type: none"> • Audit report or an independent compliance assessment report.

UNCLASSIFIED

LEVEL 4 – Quantitatively Managed - The Number of Corporate Exceptions to Implementing IA Processes is Known & Reported

Areas to Probe	Evidence Expected
<p>4.1 Compliance Regime</p> <ul style="list-style-type: none"> • Does a process exist to bring together all of the IA related control processes so that a single authoritative view can be presented to the SIRO and thence to the Main Board? • Is the Main Board aware of where it is non-compliant with the HMG SPF, national policy and standards and hence the business risk that it is accepting? • Does a plan exist to address the areas of non-compliance? 	<ul style="list-style-type: none"> • Details of process and example report. • Board papers. <p>Details of the plan and activity.</p>
<p>4.2 External Assurance</p> <ul style="list-style-type: none"> • Has the collation process, which brings together all of the IA related control processes into a single authoritative view, been subjected to independent audit so that the Main Board can be assured that they are being presented with an accurate picture? • Have the IA incident and problem management processes been subject to independent audit and have any deficiencies been rectified? 	<ul style="list-style-type: none"> • Audit report. • Audit report.

LEVEL 5 – Optimised - Responsive IA processes are integrated as Part of Normal Business

Areas to Probe	Evidence Expected
<p>5.1 Compliance Regime</p> <ul style="list-style-type: none"> • Does the Department seek to share its knowledge, experience and expertise with departments who are struggling to achieve an equivalent standard? 	<ul style="list-style-type: none"> • Details of knowledge sharing.
<p>5.2 External Assurance</p> <ul style="list-style-type: none"> • Has an independent evaluation of the entire Departmental IA control measures been undertaken? • Is there evidence to confirm that there are no remaining areas of weakness to be addressed? 	<ul style="list-style-type: none"> • Evaluation report. • Independent audit report