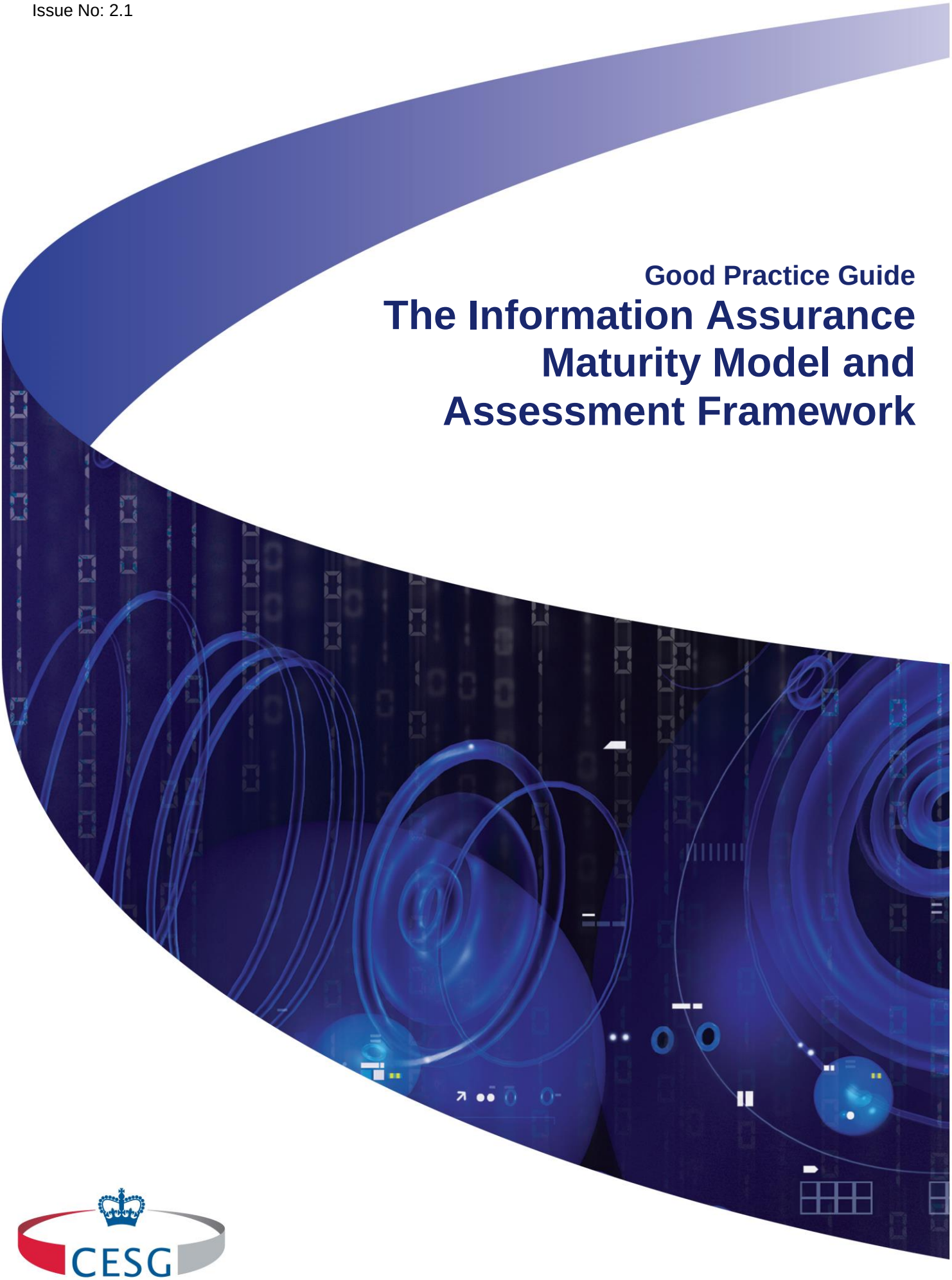
October 2015
Issue No: 2.1

Good Practice Guide

The Information Assurance Maturity Model and Assessment Framework



CESG

NATIONAL TECHNICAL AUTHORITY
FOR INFORMATION ASSURANCE

Good Practice Guide No. 40

The Information Assurance Maturity Model and Assessment Framework

Issue No: 2.1
October 2015

Document History

Version	Date	Comment
HMG IAMM v1	30 Sep 2008	
HMG IAMM v2	20 Feb 2009	
HMG IAMM v3	14 Oct 2009	
HMG IAMM v4	27 May 2010	
GPG 40 1.0	May 2011	First issue
GPG 40 2.0	November 2012	Second issue
GPG 40 2.1	October 2015	Third issue

Executive Summary

Accounting Officers (AOs), supported by their Senior Information Risk Owners (SIROs) and their Information Asset Owners (IAOs), are accountable for the adequate protection of information collected, processed and stored within their organisations.

Information is a key asset within Government, but it can become a critical liability. Increasingly Departments and other public bodies need to share information in response to the Government's digital and shared services agendas. AOs need governance that provides effective Information Risk Management (IRM) processes and procedures that address information risk and provide assurance that information that is passed to others is protected appropriately. The IRM regime must be sufficiently robust to assure the Department on the information risks arising from the impact of the developing Government ICT Strategy (reference [a]) programmes.

If information risk is to be managed effectively and efficiently in a shared service (and reusable applications, equipment and resources) environment then consistent standards are needed across Government. The HMG Security Policy Framework (SPF) (reference [b]) defines 20 Mandatory Requirements for Departments, Agencies and third party suppliers. In addition, there is a body, within HMG, of best practice measures which assist organisations to discharge their obligations to enact effective IRM.

An Information Assurance (IA) Maturity Model (IAMM) was created to assist SIROs to develop an effective change programme to improve IRM. The IAMM incorporates the mandatory information related requirements of the HMG SPF, which also covers requirements to apply appropriate data handling through HMG IA Standard No. 6 (IS6), Protecting Personal Data and Managing Information Risk (reference [c]). The IAMM is aligned with the ISO/IEC 27001:2005 Standard (reference [d]) and the broader outcomes sought by the National Security Strategy (reference [e]), the Government ICT Strategy (reference [a]), the Cyber Security Strategy (reference [f]), and the Civil Service Reform Plan (reference [g]).

To assist effective assurance, it is necessary to be able to assess compliance with the model in a consistent, fair and objective manner. Accordingly the IAMM is underpinned by an IA Assessment Framework (IAAF), which details the measures required to achieve the maturity levels defined in the IAMM. The IAAF is designed for use by IA Review Teams, e.g. as part of an independent IA Review Service delivered by CESG. However, it can equally be used by organisations wishing to conduct IA assessments themselves, or with limited support from CESG staff.

The IAAF helps organisations assess compliance with different levels in the model, but more significantly, if used honestly and objectively, it is a valuable tool at the SIRO's disposal to develop a focussed, affordable and effective IA improvement programme. As use of the IAMM and IAAF matures, the IA improvement programme should become an integral element of the Department's corporate improvement programme and other strategic mechanisms. With increasing HMG experience of the IAMM, and the growing maturity of organisations, this version includes the results of a review of IAMM level 4 aspects, coupled with the introduction of a cyber overlay. Therefore, the CESG IAMM (CIAMM®) may also be known as the CESG Cyber Security Maturity Model (CCSMM®).

Purpose & Intended Readership

This CESG Good Practice Guide provides information about how to use the IAMM and IAAF as part of an enterprise approach to improving IA. It should be read in conjunction with the CESG Good Practice Guide No. 28 (GPG 28), Improving IA at the Enterprise Level (reference [h]).

This is the second version of this GPG, but it continues the development of 5 previous versions, in total, of the IAMM and IAAF into the CESG Policy Portfolio, which was first exposed to the HMG community at IA08 (i.e. 17-18 June 2008). Specifically, this guide replaces version 1.0 of this GPG.

The changes in this document were to update some terms and references, to replace Level 4 aspects of the IAAF with the output from a series of workshops held with the IAMM Community of Interest, and to include a cyber overlay. There were some minor changes in Levels 1 to 3 to better align GPG40 and the IAMM Tool. More details can be found at the end of Chapter 2.

Contents:

Chapter 1 - Introduction and Overview

Key Principle

- The Information Assurance Maturity Model (IAMM) and the IA Assessment Framework (IAAF) provide a common set of criteria, based on recognised standards, for Departments and other organisations to assess their Information Assurance (IA) maturity and develop and maintain meaningful dialogue with other Departments, Delivery Partners and/or 3rd party suppliers

Why do we need an IAMM, IAAF?

1. Information is a critical business asset that is fundamental to the continued delivery and operation of any Government service. Departments need to develop an acceptable level of assurance regarding the Confidentiality, Integrity and Availability of their data. If this is not done, then Departments' data will be vulnerable and this will in turn lead to risks to service delivery. Personal data collected, stored and processed by Departments is subject to specific legal and regulatory requirements.

2. The Government's ICT Strategy (reference [a]) for citizen facing transactional services, of 'digital by default' (e.g. also see 'Action 2' of The Civil Service Reform Plan (reference [g]), and the subsequent indication of the Government Digital Strategy (GDS) in reference [i]), inevitably leads to a considerable increase in direct IT based dealings with the citizen via the untrusted platform of the Internet. There also will be greater reliance on shared services between Departments, and other Government bodies, to achieve efficiencies and economies of scale. This will make the IA Assurance environment inherently more complex and it introduces new and significant risks of untrusted endpoints.

3. In this more complicated environment, organisations need to build mutual trust in each other's Information Risk Management (IRM) and IA capabilities. The IAMM and IAAF provide a common set of criteria, based on recognised standards, for Departments and other organisations to assess their IA maturity, and to develop and maintain a meaningful dialogue with other Departments, Delivery Partners and/or 3rd party suppliers. This model can also be known as the CESG IA Maturity Model (CIAMM®).

What does the IAMM consist of?

4. The IAMM identifies three main IA goals that are subdivided into six sections. For each section, the model defines 5 levels of maturity and it gives high-level criteria that need to be satisfied to justify attainment of that level of maturity. This approach enables assessments to be conducted in a consistent and repeatable manner.

5. It is for the Main Boards of organisations to decide what level of maturity they need to sustain for an IRM environment that is consistent with their business context and risk appetite. IAMM Level 3 is generally considered to be the minimum baseline standard that organisations need to achieve. Level 3 is predicated on delivering effective IRM measures for business critical systems

and their related processes. Activity undertaken in achieving this level also provides assurance on SPF and other aspects of HMG Mandatory Requirements. However, it should also be noted that there are some very important steps to effective IRM that is embedded in Level 4 of the IAMM, although there are elements to help counter the cyber threat at all levels of the IAMM. The IAMM alsoprovides effective metrics to the SIRO and the Main Board, without which the ability of senior management to take effective decisions will be hindered. Therefore, it may be prudent for organisations to specify the level of maturity to be achieved for each of the six sections individually, rather than specify an across the board level to be attained.

6. The IAAF provides a more detailed expansion of the IAMM requirements to a level of detail that enables a consistent interpretation of the Model. A cyber overlay is also included, which does not intend to decrease the importance of any IA aspect, but it does give an indication of where effort can be focused when there is a cyber component (e.g. internet based customer aspects). Hence, the IAAF/IAMM can also be known as the CESG Cyber Security Maturity Model (CCSMM®).

7. CESG has developed a range of services (e.g. see the CESG pages at www.cesg.gov.uk) to assist an organisation's assessment against the Model. Departments can choose to self assess, or commission a supported self-assessment or an Independent Review from CESG. At the appropriate levels, it is possible for Departments and Agencies to setup a shared service, where they can pool resources to achieve a certain amount of independent assessment.

8. There is a CESG supplied IAMM tool (CIAMM®/CCSMM® tool) available for both self and supported self assessments. Whilst this tool can make the assessment process easier, care must be taken to avoid it becoming a "tick box" exercise, which would undermine the value of the assessment and minimise any lasting business benefit of the process.

9. Those Department's who have commissioned CESG to conduct an Independent Review see the key value of this being the report, which includes recommendations on how to address deficiencies and also how to achieve higher levels of IA maturity.

Benefits

To Central Government

10. The IAMM and IAAF together provide a single framework, based on common standards, that is an essential management tool to help address the complex information risk environment. It therefore assists the Government's ICT Strategy (reference [a]) and with it the potentially increasing reliance on shared services and on cloud computing. This framework provides the common language that will enable meaningful, trusted relationships regarding information sharing. This will be an essential enabler for the realisation of the financial and operational benefits of the strategy.

To Departments

11. Departments will seek to improve the delivery of their businesses. They will wish to do so within the boundaries of corporate policy, and within their risk appetites. A clear and informed understanding of the Departmental risk profile and its impact on their business is crucial. In addition, accountable officers require assurance that the measures that they stipulate, to manage the organisation's information risk, are in place and are effective.

12. By applying this framework, which is based on common standards, Departments will be able to assess current levels of IRM and IA capability, set clear targets for improvement to sustain and improve business operations, and develop an IA improvement programme to meet those targets, coupled with the confidence that they are compliant with the Mandatory Requirements of the SPF.

13. The use of a common framework enables effective understanding and communication about information risk between Departments, and all of the organisations within their delivery chains. This is needed to deliver sufficient levels of trust required in a shared service environment. Without it, Departments may not gain the improvements, or deliver the financial savings, that underpin the case for the digital agenda.

To Wider Government Bodies and to Industry Supplying Government

14. Wider Government bodies i.e. Agencies, Non-Departmental Public Bodies (NDPBs) and Local Authorities play a crucial role in the delivery of Departmental services to the citizen. With the increasing impact of digital engagement and shared services, the value of the IAMM, as a vehicle for enabling unambiguous discussion and agreement on IA issues, is increasingly important. The same is true for the role of the 3rd party suppliers and their downstream supply chains. To assist gathering data from 3rd party suppliers, there is an extraction of similar questions (e.g. to those contained within the IAAF) for the Supplier Information Assurance Assessment Framework and Guidance (reference [j]), which contains a requirements specification for a Supplier IA Tool (SIAT), to automate the use of the SIAT assessment framework question set. A version of the SIAT question set had been implemented in HADRIAN (i.e. a system previously used by various Departments, e.g. the Home Office), and this is likely to continue in relation to its replacement.

To Individuals

15. Individuals in specific roles, in particular Accounting Officers (AOs), Senior Information Risk Owners (SIROs), Information Asset Owners (IAOs), Departmental Security Officers (DSOs) and Information Technology Security Officers (ITSOs) can draw on the IAMM and IAAF to gain assurance and evidence that they have taken reasonable steps to execute their responsibilities. They have a common framework and language to communicate their intent and to report progress in terms of business outcomes.

Chapter 2 - The IAMM and IAAF in Detail

Key Principle

- The IAMM and IAAF embody the relevant HMG SPF Mandatory Requirements, together with material drawn from the Managing Information Risk Guidance document (reference [k]) 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 (reference [d])

Introduction

16. This Chapter provides additional detail on the IAMM and IAAF.

IA Maturity Model

17. The IAMM (see Annex A) defines three main IA goals and identifies clear milestones towards their achievement. This structure is designed to help SIROs identify the level of IA maturity required to achieve specific business orientated requirements:

    a. Embedding IRM culture within the organisation:

    - The need to assure information, as a key business asset, is embedded within the culture of the organisation, its Delivery Partners and its 3rd party suppliers
    - Procedures are in place so that the Main Board is able to understand and manage the information risk to which the total organisation[1] is exposed
    - The agreement of external stakeholders is reached on the treatment of information risks, particularly when they will impact on the delivery of the Government's major plans, including those related to shared services (e.g. as indicated in Action 3 of the Civil Service Reform Plan, (reference [g]))

    b. Implementing best practice IA measures:

    - Through-life measures are implemented to assure all information within the organisation, 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 appropriate (e.g. boundary) points is undertaken so that the organisation 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:

[1] The Department, its Delivery Partners (some of whom operate at arm's length) and 3rd party suppliers. Specific definitions of these terms were originally published by Cabinet Office during Autumn 2009, although with the evolution of later documentation, suppliers could be considered a named type of delivery partner, dependent on the context, e.g. in an area of the Government ICT Strategy (reference [a]). If the context of a term is considered to have importance in terms of a legal definition, then that should receive appropriate consideration by the relevant legal advisors.

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

18. Achieving maturity towards these goals, assisted by the IAMM, will enable organisations to generate greater trust in their information systems and processes, both internally and between organisations. 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. SIROs are encouraged to review the effectiveness and sufficiency of their organisation's IA measures on at least an annual basis and, where appropriate, commission work to address shortfalls and hence improve the organisation's IA maturity.

19. 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 and Communication Technology (ICT) systems. Many of the SPF Mandatory Requirements (e.g. related to importance of protecting personal data) are built into Level 1 of the IA Maturity Model. However, this is probably only a stepping stone to achieving a probable business justified target of IAMM Level 3 (i.e. critical systems are appropriately protected)
- **Level 2 – Established**. At this level IA processes are institutionalised within the organisation, 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 has started. Discovery work has been undertaken and the IA status of the entire organisation's ICT systems and related processes have been determined. A definitive list of business critical ICT systems 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 Main Board for a targeted programme of work to improve the understanding and control of information risk. Within most organisations, 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.** Apart from the Main Board having established its broader IA Road Map for all its information, systems and processes (e.g. beyond those previously considered as the critical systems), there is evidence to show that staff attitudes and behaviours towards assuring information are aligned to the needs of the business. Hence, the regime established at Level 3 (i.e. for critical areas of the business) is extended to embrace other areas of business activity that the Main Board determines need to be raised to the same standard of IA protection to meet the business need. 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

20. The IAMM and the IAAF are living documents which will be updated in line with changes in the threat, changes in the SPF (reference [b]) and as a result of lessons learned from applying them to organisations. The IAMM Community of Interest (IAMM COI) workshops, which led to the changes in the Level 4 aspects of this document, have been part of this process.

21. 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

22. The IAAF (See Annex B) provides specific details of the measures that are expected to be in place within organisations seeking to meet the top-level statements of maturity contained within the IAMM. The Framework has been laid out in a similar manner to the HMT Risk Management Assessment Framework (e.g. see section 6 of reference [l]), but adapted to follow the approach taken in the work books (e.g. “areas to probe” and “evidence expected” elements) produced originally by the OGC (which is now part of the Cabinet Office Efficiency and Reform Group (ERG)), as part of their Gateway Review process (reference [m]). This modification enables the IAMM and the IAAF to be used as an integral part of an IA Independent Review Process.

23. The contents of both the IAMM and IAAF have been drawn from a variety of sources. They embody the relevant SPF Mandatory Requirements which includes the requirement to apply IS6 (reference [c]), together with material drawn from the Managing Information Risk Guidance document, (reference [k]), 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 (reference [d]). 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 organisation.

24. Recognising that organisations may require more specific guidance on implementing some of the more technical IA controls mentioned in the IAAF (i.e. see Appendix B, policy column), CESG guidance material has been produced, and is available to those with access to the CESG documentation portfolio.

25. As indicated above, the ISO/IEC27001:2005 methodology for Information Security (reference [d]) mapping resulted in an extra column in the IAAF to reference the appropriate part of the International Standard that correlates with the IAAF requirement. Also, at Annex C, the Standard is mapped onto the IAAF. These may assist organisations that employ ISO/IEC27001:2005. However, in many instances, there is no direct read across between the two documents, because the IAAF includes specific requirements that are not contained within the ISO Standard. Therefore, the existence of a particular ISO 27001 document, or control measure, does not in itself provide evidence of IA maturity against the IAMM, unless it has been drawn up to be IAMM compliant.

Changes from the Previous Version

26. Apart from minor changes to remove typographical errors, and to make elements slightly easier to digest, there were some changes required to ensure mutual GPG40 and IAMM Tool consistency (and GPG40 also contains an improved mapping to the IAMM Tool). Comments from various sources were also incorporated, where these were received (e.g. via the IAMM COI, or feedback). Some changes are outlined below, and the IAAF provides more detail of some specific changes (i.e. especially at level 4 (see below)).

27. In the “Leadership and Governance” section, in the category “Board Responsibilities Governance and IA Strategy and Programme”, question 2.1.1 was modified to include the content of questions 2.1.2 and 2.1.3 from the previous version (i.e. they no longer exist in this version, and they did not explicitly exist in the previous version of the IAMM Tool (e.g. version 3.5)). Similarly, question 3.1.1 was modified to include the content of questions 3.1.2 and 3.1.3 from the previous version (and again they no longer exist in this version, and they did not explicitly exist previously in the IAMM Tool).

28. Also, in the “Leadership and Governance” section, in the category “SIRO’s Responsibilities”, question 3.3.1 was modified to include the content of question 3.3.2 (and again question 3.3.2 no longer exists in this version (Note: question 3.3.2 did not explicitly exist previously in the IAMM Tool)).

29. The Level 4 aspects of the IAMM question set were nearly completely replaced in Version 2 of this document, but they were built on the existing Version 1 content. The Level 4 evidence aspects were reconstructed to fit into this new question set, and appended to, as appropriate. This should not affect most organisations, as most would not yet have utilised Level 4 yet to a comprehensive extent. Those organisations that are affected can view the IAAF Level 4 outcomes which have changed (e.g. they are labelled as such in this document).

Chapter 3 – Using the IAMM and IAAF

Key Principle

- A strategic approach to IA improvement is required by any organisation that uses the IAMM and IAAF to measure their IA maturity. Adopting this type of approach is efficient and it delivers other benefits. Effective compliance and audit arrangements are included within the IAAF that are designed to provide the assurance needed to underpin the IRM detail required for corporate management documents, such as the annual Governance Statement

Introduction

30. This Chapter provides details of how the IAMM and IAAF can be used as part of a strategic approach to IA improvement.

Using the IA Maturity Model and Assessment Framework

31. Embedded within the main body of the IAMM is a range of internal reporting and compliance mechanisms, which are aimed at establishing and maintaining clear management responsibility and accountability for IRM within the organisation. These arrangements should facilitate the collection of the management information on information risk that is required to be included in the organisation's Annual Management Report and the annual Governance Statement (GS).

32. Organisations are encouraged to use the IAMM and IAAF to establish the programmes of work needed to achieve IA maturity and also to conduct self-assessment IA reviews. To achieve an objective assessment of IA maturity an external Independent IA Review will need to be undertaken and details of how a Department can arrange for such a Review as part of the CESG Service portfolio are included on the CESG website. CESG also provides a Supported Self-Assessment service, using a software tool (which can be downloaded from www.cesg.gov.uk) to complete the assessment.

33. The outcomes are cross referenced to the software tool (i.e. the CESG IA Maturity Model (CIAMM®)), to enable users of the IAMM tool to relate the contents of GPG40 to the appropriate versions of the tool. Version 3.5 was the last generally available version of the Excel based IAMM tool, although there was a Version 4.0, on Excel, for specialist use. Version 5.0 of the IAMM tool is Java 1.5 based (Note: The old version of Java was used as a base installation to ensure wide applicability, although it should work with later Java releases).

34. The cyber overlay consists of three aspects (shown below) that relate to the importance of the IAAF category to an endeavour that has a significant cyber component. Although each category receives a rating in the overlay, a lower cyber significance does not mean that it is not important. Good information assurance practices, across all the categories, are still needed, irrespective of any specific system's cyber perspective.

35. The cyber overlay divides the IAAF categories into 3 types, and hence each category in the IAAF is labelled appropriately (and that label cascades down to the respective outcomes). In decreasing order of cyber significance, these are:

    a. Business Critical

    b. Supporting

    c. Peripheral

36. The CESG IAMM (CIAMM®) and CESG CSMM (CCSMM®) tool includes the cyber overlay information, and related to each outcome it allows a measure of achievement to be recorded against the respective recipient categories (e.g. "Organisation", "Delivery Partners" and "Third Parties"), based on the evidence presented. This achievement measure is guided by the below elements:

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

Strategic Approach

37. The contents of the IAMM and IAAF 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, is 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

38. 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 that 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.

    d. Tends to prevent organisations from making savings through economies of scale.

39. Thus, a key step to any organisation wishing to improve its IA maturity, using the IAMM and IAAF, is to adopt this or a similar strategic approach.

Developing an IA Strategy

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

Annex A – CESG IA Maturity Model (CESG Cyber Security 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 board has established its broader IA Road Map for all its information, systems and processes.	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. Main Board commitment to effective IA is promulgated in a top-level policy statement. Publication of an Information Charter. Appointment of a SIRO on the Main Board and IAOs throughout the organisation taking responsibility for protecting, managing and using their assets.	Main Board members understand and accept their responsibility for the effective application of IA measures across the organisation. The Main Board has endorsed an Organisational 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 organisation. Main Board members are proactively engaged in leading and championing IA awareness across the organisation so that the essential behavioural changes needed to embed the Main Board's policy become rooted in the culture of the organisation.	Main Board monitors progress towards embedding IA policy across the organisation and re-directs effort where appropriate to deliver its strategic intent.	The need to assure the organisation's Information and that of its external stakeholders as a key business asset is fully embedded within the organisational culture and is subject to a regime of continuous improvement.
	Training, Education & Awareness	A balanced and targeted programme of annual information risk awareness training is instituted for all staff within the organisation, its Delivery Partners and 3rd party suppliers who have access to the organisation's information. A cultural change plan is implemented.	All members of the organisation undergo annual risk awareness training. A programme of targeted education and training is instituted for IA professionals and for middle and senior managers. Staff behaviours are measured and trends analysed. Progress against the organisation's cultural change goals is managed and reported to the SIRO.	As understanding across the organisation is raised, training becomes more targeted. Key staff are trained and take effective information risk management decisions. 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. The training is matched to the business need and action is taken to ensure specialist, corporate IA knowledge is retained. Evidence shows 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 organisation'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 ICT Systems 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 organisation's approach to addressing information risks is agreed with the organisation's external stakeholders, where applicable.	The Accreditation status of all existing ICT Systems is determined and the information risks are identified within Risk Registers for all accredited in-service ICT Systems. 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 organisation's management structure for effective decision making, within the organisation, its Delivery Partners, and with external stakeholders.	All ICT Systems that are critical to the business have been subject to Accreditation and the organisation has effective information risk management processes in place to manage the residual risks and the related systemic IA risks.	For all ICT Systems, 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 organisation 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 organisation 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 organisation's information are kept under active review.
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 and malicious intent. The organisation has a Forensic Readiness Policy.	The status of the through-life IA measures employed across the organisation 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 organisation'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.	Where there is a business justification, Level 3 processes are extended to embrace all of the organisation'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 organisation so that changes can be made in IS to match the business tempo, without introducing undue vulnerabilities.
	Assured Information Sharing	The requirement to define and manage how information is shared across the organisation's boundaries is identified. Arrangements are in place to work with external stakeholders to achieve shared IA objectives. The need to understand and control how ICT systems 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 and managing information across these boundaries are defined and implemented, including those with Delivery Partners and 3rd party suppliers. The organisation takes an enterprise-wide approach to the security of new ICT systems and a systematic method is used to implement the control measures needed to mitigate problems when inter-connecting ICT systems.	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 organisation 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 organisational 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 Main Board's Audit Committee ensures that it receives comprehensive assurance on IRM and challenges assurance, where required. The organisation reports annually on IA issues.	The organisation has a comprehensive IRM compliance regime. External IA Review is undertaken to provide an independent assessment of progress towards compliance with the SPF and national policy & standards.	Critical IA Review and internal audit recommendations are actioned and progress is tracked.	IA practices are fully assured by internal audit. The Main Board is aware of the significant areas of the organisation's non-compliance with the SPF and national policy and standards. Remedial action has been undertaken.	There are no critical or significant IA audit issues. Independent assessment of the organisation's approach to IA shows that it is aligned with the relevant Strategies (e.g. the National and Cyber Security Strategy) and it is fully compliant with the SPF and national policy and 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 board has established its broader IA Road Map for all its information, systems and processes.	**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. Main Board commitment to effective IA is promulgated in a top-level policy statement. Publication of an Information Charter. Appointment of a SIRO on the Main Board and IAOs throughout the organisation taking responsibility for protecting, managing and using their assets.	Main Board members understand and accept their responsibility for the effective application of IA measures across the organisation. The Main Board has endorsed an Organisational 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 organisation. Main Board members are proactively engaged in leading and championing IA awareness across the organisation so that the essential behavioural changes needed to embed the Main Board's policy become rooted in the culture of the organisation.	Main Board monitors progress towards embedding IA policy across the organisation and re-directs effort where appropriate to deliver its strategic intent.	The need to assure the organisation's Information and that of its external stakeholders as a key business asset is fully embedded within the organisational 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 organisation.

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

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

1.1 Board Responsibilities, Governance Structure and IA Strategy and Programme [Cyber Category Type: Supporting]

1.1.1 Required Outcome: The Main Board recognises the need to put in place effective IA measures throughout the organisation and its delivery chains, to ensure the Availability, Integrity and Confidentiality of the organisation's information
[Links to 2.1.1; IAMM Tool Question Reference: 01.01.01 (v3.5/v4.0), QUES16775599380 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is IA perceived to be an enabler to the business of the organisation, or is it considered to be an impediment? • Does the Main Board understand that IA is not just about protecting the Confidentiality of information, but is also about ensuring its Availability and Integrity, as well as the effective management and use of information to support business objectives?	• Main 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 • Main Board members speak authoritatively about IA in terms of CIA and its importance to delivering business objectives. They may not know much about the subject, but they recognise its criticality	IS1&2 & IS6, GPGs 19 & 28.	5.1.d A.6.1.1
• Is IA perceived to be a specialised and technical subject, or is genuinely acknowledged to be part of the mainstream business of the organisation? • Has the Main Board issued a top-level policy statement committing the organisation to the changes needed to implement effective IA? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: H]	• Top level IA Policy Statement.		A.5.1.1
• 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 Requirements set out in SPF (reference [b]) and particularly IS6 (reference [c])? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Main Board members recognise that they have responsibility for the implementation of IA measures to comply with statutory requirements embodied in the Data Protection Act (DPA) and other similar legislation, together with other mandated IA policy requirements, within the organisation, its Delivery Partners and within 3rd party suppliers.		
• What has the Main Board done to optimise the relationship with Delivery Partners, particularly those that they can only seek to influence, so that they take seriously the need to improve their information handling arrangements?	• Details of bilateral or multi-lateral meetings and other activities undertaken to help bring non-compliant partners into an acceptable level of compliance with the organisation's policy.		A.6.2.1 A.6.2.3
• Has the Main Board minuted its approval of the Compliance Reporting Requirements needed to ensure that its Delivery Partners and 3rd party suppliers (including those based offshore and in the EU) and any other public body handling information on the organisation's behalf are compliant with HMG SPF (and incorporating the data handling embodied in IS6) Mandatory Requirements? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: H]	• Main Board Minutes • Details of compliance reporting requirements.		A.6.2 A.10.2.1 A.10.2.2 A.15.1.1 A.15.1.4 A.8.2.1 A.6.1.2
• Has the Main Board endorsed the plans produced by the SIRO to introduce cultural change processes in the organisation? (Connect with TEA 1.3.1)	• Details of Main Board engagement.		
• 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)?	• Clear lines of responsibility and accountability within governance framework.		A.6.1.2
• 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? • Has the Main Board minuted its approval of the organisation's IA governance structure and the TORs of the principle IRM decision making bodies? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M]	• 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. • Main Board minutes.		A.6.1.3 5.1.d

1.1.2 Required Outcome: Effective engagement by the organisation has resulted in the Main Boards of the organisation's Delivery Partners and 3rd party suppliers recognising the part that they play in ensuring the Availability, Integrity and Confidentiality of the organisation's information
[Links to 2.2.1; IAMM Tool Question Reference: 01.01.04 (v3.5), 01.01.08 (v4.0), QUES16775599387 (v5.0); Recipient Type: Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Have the Main Boards of the organisation's Delivery Partners and 3rd party suppliers issued top-level policy statements committing the organisations to the changes needed to implement effective IA in respect of the services they provides to the organisation. [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H] • Have mechanisms been put in place by Delivery Partners and 3rd party suppliers to give assurance to the organisation of the effective measures that exist to safeguard the organisation's information. [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M]	• Details of the policy statements and any evidence of subsequent action to meet the organisation's needs. • Details of the assurance mechanisms.	IS1&2, IS5 & IS6, GPGs 10, 19, 28 & 35, Technical Threat Briefing No.1 (TTB1).	A.6.2 A.10.2

1.2 Gaining the Public's Trust [Cyber Category Type: Peripheral]

1.2.1 Required Outcome: The Board has committed the organisation to take appropriate care of personal information provided by employees and by the public
[Links to 2.2.1; IAMM Tool Question Reference: 01.02.01 (v3.5/v4.0), QUES16775599388 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Has an Information Charter has been published setting out how the organisation 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 organisation, its Delivery Partners, 3rd party suppliers, and the public? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M] • Has the appropriate body with delegated responsibility for IA matters minuted that it has reviewed the organisation's published Information Charter within the last 12 months confirming that it meets the organisation's needs and has confirmed that it is accessible both internally and externally, particularly by the public. [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M]	• An Information Charter applicable to the entire organisation's business has been endorsed and published. • The existence of the Charter is known within the organisation. • A copy of the Charter can be readily accessed from the organisation's website. • Minutes of a meeting, together with the evidence on which the decision was taken.	IS6, GPGs 19 & 28.	A.15.1.1 A.10.8.2 A.6.2.2 A.8.2.2 4.2.3

1.3 SIRO's Responsibilities [Cyber Category Type: Supporting]

1.3.1 Required Outcome: In accordance with the SPF (reference [b]), the Main Board has appointed one of its members as the Senior Information Risk Owner and that person has taken full and effective responsibility for managing information risks within the organisation and within its delivery chains
[Links to 2.3.1; IAMM Tool Question Reference: 01.03.01 (v3.5/v4.0), QUES167755993813 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Has a Main Board Member been appointed as SIRO and has the Main Board minuted its endorsement of the SIRO's TOR. Is he/she an effective advocate for information risk on the Main Board and in internal discussions? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Evidence of commitment from a trained and competent SIRO to the role, both at Main Board level and within the Organisation.	IS1&2 & IS6, GPGs 19 & 28.	A.6.1.3 A.8.1.1
• Does the SIRO own the Organisation's Information Risk Policy and annual Information Risk Assessment? (Connect IRM 1.1 & 1.3) [IAMM Tool Evidence Reference: 2 & 3 (v3.5/v4.0); Importance: H]	• SIRO acknowledges his/her responsibility and has the process in place to produce and maintain these documents on a regular basis.		4.2.1 c) 2)
• Has the SIRO, on behalf of the Main Board, endorsed a statement of the Organisation's Information Risk Appetite, following consultation with the HMG CIO, where applicable, or with respective parent organisation? (Connect with IRM 1.2) [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: M]	• Statement of the Organisation's Information Risk Appetite.		5.1 f) 4.3
• Does the SIRO review an IA Risk Register on a regular basis and is there an effective methodology in place to address the risks (connect with IRM 1.4) [IAMM Tool Evidence Reference: 5 (v3.5/v4.0); Importance: M]			
• Does the SIRO ensure that as a minimum any material discussions and judgements relating to the organisation's Information Risk Policy and its application (as detailed in IS6, reference [c]) are recorded in writing and stored in accordance with the organisation's records policy? [IAMM Tool Evidence Reference: 6 (v3.5/v4.0); Importance: M]	• Clear governance framework, with procedures for the allocation of responsibilities and management of actions. Resultant decisions and actions are minuted. • Details of formally recorded information.		A.6.1.2 A.6.1.3 4.2.1 c) 4.2.1 d)
• Has the SIRO produced an annual Report to the AO on the effectiveness of information risk management that includes an assessment of not only how secure the information is, for embodiment in the annual Governance Statement (GS), but also, how effective the organisation is in maximising the inherent value of the information? [IAMM Tool Evidence Reference: 7 (v3.5/v4.0); Importance: M]	• Copy of the last annual report.		7.3
• Has information risk been specifically addressed in the organisation's annual Governance Statement (GS), which is signed off by the Accounting Officer? [IAMM Tool Evidence Reference: 8 (v3.5/v4.0); Importance: M]	• Annual GS and the written advice.		4.2.1 c) 4.2.1 d)
• Has the SIRO taken responsibility for producing and staffing, for approval to the Main Board, a plan to introduce processes aimed at fostering a culture that values, protects and uses information for the public good? (connect with TEA 1.3.1) [IAMM Tool Evidence Reference: 9 (v3.5/v4.0); Importance: M]	• Evidence that the cultural change plan is receiving the degree of high level involvement and exposure required to meet the data handling requirements in IS6 (reference [c]).		A.8.2.1
• Has the SIRO taken responsibility for establishing the processes and monitoring regime that will ensure their plan for cultural change will bring about the required change? [IAMM Tool Evidence Reference: 10 (v3.5/v4.0); Importance: M]	• Details of how the plan is to be put into effect.		A.8
• What has the SIRO done to ensure that effective processes are in place within the organisation to govern the activities relating to the approval and management of data sharing with other Government bodies.	• Details of the processes and governance which is in place.		A.6.2
• What has the SIRO done to initiate a programme of work to share and learn best practice from others, including, other Organisations, fellow SIROs, IA specialists in NTA and industry? [IAMM Tool Evidence Reference: 11 & 12 (v3.5/v4.0); Importance: L]	• Engagement with SIRO network within the last 12 months. • Other initiatives.		A.6.1.6 A.6.1.7
• Is the SIRO engaged in discussions involving new (and possibly unexpected) ICT requirements to ensure that IA requirements are factored in from the start?	• Details of effective SIRO engagement in forward ICT planning.		A.12.1.1

1.3.2 Required Outcome: Effective engagement by the organisation has resulted in the Main Boards of the organisation's Delivery Partners and 3rd party suppliers appointing a senior manager to take effective responsibility for IRM. This individual engages with both the organisation and others across Government to learn and share best practice
[Links to 2.3.2; IAMM Tool Question Reference: 01.03.04 (v3.5), 01.03.05 (v4.0), QUES167755993817 (v5.0); Recipient Type: Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Do the senior named individuals who perform the equivalent role of the SIRO in the Delivery Partner and 3rd party supplier organisations own their respective Information Risk Policy and Information Risk Assessment? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Evidence that the SIROs in DPs and 3rd Party Suppliers are not just appointments in name only, but are discharging the role.	IS1&2 & IS6, GPGs 6, 19 & 28.	A.6.1.3 A.8.1.1 4.2.1 c) 2)
• Is there evidence of successful engagement by these individuals with their peers in government and with IA specialists in the NTA and industry?	• Details of meetings amongst SIROs within the organisations delivery chain.		
• Is there any evidence of attempts to share and learn best practice with others? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H]	• Details of effective sharing of best practice.		

1.4 IAOs Responsibilities [Cyber Category Type: Supporting]

1.4.1 Required Outcome: In accordance with the SPF (reference [b]), the organisation has a senior named individual (Information Asset Owner - IAO) identified for each of the information assets identified within the organisation's list of information assets and that person has taken full and effective responsibility for managing the protection and exploitation of the information for which he/she is responsible to ensure that the benefit to the organisation is maximised
[Links to 2.4.1; IAMM Tool Question Reference: 01.04.01 (v3.5/v4.0), QUES167755993819 (v5.0); Recipient Type: Organisation, and Delivery Partners]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Has an IAO governance structure been created within the organisation? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Details of the governance structure.	IS1&2 & IS6, GPGs 13, 19 & 28.	A.6.1.2 A.6.1.3 A.8.1.1
• Have formal TORs been drawn up that hold IAOs responsible for access to all of the organisation's information assets identified within the organisation's list of information assets. [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M]	• Sample TORs.		
• Do the IAO TORs make it clear that in addition to protecting the information, IAO's are also responsible for maximising the benefit to the organisation from using the information? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: M]	• Sample TORs.		
• Are IAOs in place for all information assets on the Organisational list of information assets and are they sufficiently senior to discharge the role envisaged?	• Details of the IAOs in place and Information asset list annotated to show IAOs.		A.7.1.2
• Has the Organisation 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?	• Details of the mechanism and how this is assured.		A.11.2.1 A.15.2.1
• Has the Organisation 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?	• Details of the process and its efficacy.		A.10.10.1 A.10.10.2
• Where action is taken within an organisation on behalf of an IAO or a number of IAOs, to discharge the appropriate SPF mandatory measures, has the organisation made it clear to IAOs that the obligation remains with them to satisfy themselves that the action taken meets the appropriate (e.g. IS6, reference [c]) requirements and where it does not it is their responsibility to ensure remedial action is taken to increase the efficacy of the measure?	• IAO guidance material. • Details of IAOs testing the efficacy of centrally implemented measures. • Details of IAOs taking remedial action to discharge their obligations.		A.6.1.3 A.15.2.1

1.4.2 Required Outcome: IAOs who are responsible for protected personal data have assured themselves that they know how the information is used, by whom and why
[No links; IAMM Tool Question Reference: 01.04.03 (v3.5/v4.0), QUES167755993821 (v5.0); Recipient Type: organisation, and Delivery Partners]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• 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 Organisation? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M]	• 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.	IS1&2 & IS6, GPGs 13, 19 & 28.	A.11.1 A.11.2.1 A.11.2.2
• Have the IAOs conducted critical reviews of the mechanisms that exist to identify and keep a record of all staff and contractors who have access to, or are involved in handling such data? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H]	• Details of any reviews undertaken and any resultant action.		A.11.2.4
• Have the IAOs ensured that management processes are in place to check the efficacy of the activity logging of data users who have access to protected personal information, particularly those working remotely and those with higher levels of IS functionality or with broader levels of access? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: M]	• Details of any reviews or other assurance activity undertaken by IAOs.		A.15.2.1 A.7.1.3 A.11.2.1

1.5 DSO, ITSO & ComSO Responsibilities [Cyber Category Type: Peripheral]

1.5.1 Required Outcome: The organisation satisfies the SPF (reference [b]) requirement to have appropriately trained staff filling the roles of: DSO (who has day-to-day responsibilities for all aspects of Protective Security {including physical, personnel and information security}), ITSO (responsible for the security of information in electronic form), and ComSO (where the organisation handles HMG cryptographic material)
[No Links; IAMM Tool Question Reference: 01.05.01 (v3.5/v4.0), QUES16775588322 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does the organisation 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?	• Details of the designated personnel.	SPF IS1&2 & IS6, GPGs 19 & 28.	A.6.1.3 A.15.1.6
• Do TORs exist for each of these three roles? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Copies of the TORs.		A.8.1.1
• Do the TORs specify the training requirement for those filling the appointments? • Are the individuals filling the roles trained to enable them to fulfil their duties? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M]	• Training requirement included in the TORs. • Details of the training undertaken by the current incumbents in the posts.		

1.6 Information Security Policy [Cyber Category Type: Peripheral]

1.6.1 Required Outcome: The organisation satisfies the SPF requirement to have an information security policy setting out how they, and their Delivery Partners (including offshore and near shore (EU/EEA based) Managed Service Providers), comply with the minimum Mandatory SPF Requirements, particularly, but not exclusively, Security Policy No: 2
[Links to 2.5.1; IAMM Tool Question Reference: 01.06.01 (v3.5/v4.0), QUES167755993823 (v5.0); Recipient Type: Organisation][Modified in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does the Organisation have an Information Security Policy as a component of their overarching Security Policy setting out how the organisation, 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: 2? [IAMM Tool Evidence Reference: Part 1 (v3.5/v4.0); Importance: H]	• Information Security Policy document.	SPF IS1&2 & IS6, GPGs 6, 19 & 28.	A.5.1.1
• 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 SPF MR7?	• Information Security Policy document.		A.7.2.1 A.7.2.2
• 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?	• Detail from Information Security Policy, or details of where requirement for such agreements is established.		A.6.1.5
• 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? [IAMM Tool Evidence Reference: 2, 3, 4 and 5 (v3.5/v4.0); Importance: M]	• Clear establishment of responsibilities.		A.8.3.1
• Does the Information Security Policy make clear reference to the organisation's Knowledge and Information Management (KIM) Policy and detail how the two policies and the related procedures are coordinated? [IAMM Tool Evidence Reference: Part 1 (v3.5/v4.0); Importance: H]	• Details of linkage between the Information Security Policy and the KIM Policy and related procedures.		4.2.3 d) 3)

LEVEL 2 – Established - IA Processes are institutionalised

2.1 Board Responsibilities, Governance Structure and IA Strategy and Programme [Cyber Category Type: Supporting]

2.1.1 Required Outcome: The Main Board has directed and resourced the work needed to address weakness in the organisation's approach, including governance, to IA in a strategic way that assures the effective use of information to support the business
[Links from 1.1.1 and to 3.1.1; IAMM Tool Question Reference: 01.01.02 (v3.5/v4.0), QUES16775599381 (v5.0); Recipient Type: Organisation]
[Modified in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Do the Main Board members understand and accept their responsibility for IA as part of their corporate governance responsibility?	• Main 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 of IS1&2) within the organisation, its Delivery Partners and within 3rd party suppliers.	IS1&2, IS4, IS5 & IS6, GPGs 10, 19, 28 & 35, Technical Threat Briefing No.1 (TTB1).	A.6.1.1 A.6.1.3
• Is the Main Board satisfied with the process put in place to ensure that Delivery Partners and 3rd party suppliers comply with the organisation's policy?	• Main Board minutes.		A.6.2
• Has the Main Board minuted that it is satisfied that the breadth and depth of the reporting mechanisms being put in place within its delivery chains (including 3rd party suppliers based offshore and in the EU) and any other public body handling information on its behalf, adequately reflect those organisations' abilities to manage information risk to a level that is acceptable to the Main Board? [IAMM Tool Evidence Reference: 6 (v3.5/v4.0); Importance: L]	• Main Board minutes.		A.6.2
• Is there effective engagement between the SIRO/IA organisation and the	• Evidence of a mutually supportive approach to IA being taken by the		A.6.1.1

DSO/security organisation? • Is there an effective IA governance regime and are there effective mechanisms to hold staff accountable for their actions? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: M] • Has the Main Board set a target level of IA maturity (e.g. target per IAMM section) that they require the organisation to achieve? • Has the Main Board endorsed an up-to-date IA Strategy, as part of an overarching Information Strategy, detailing how the organisation is to develop its IA maturity over time? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H] • Is the IA Strategy endorsed by the Board fit for purpose; does it represent good/best practice? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H] • Does the IA Strategy include the methodology by which the organisation 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 assets and equipment? • Does the IA Strategy include all aspects of the business requirement, particularly the opportunities for sharing and re-using information to support key business objectives? • Does the IA strategy take 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? • Does the IA Strategy include the need to put in place horizon scanning activities to take advantage of new ICT solutions to business issues? • Does the IA Strategy take due account of both the internal sponsored and the HMG ICT programmes which will impact on the work of the organisation in the next 3-4 years? • Are specific IA risk issues such as those concerning Flexible Working and the use of portable devices and removable media included? • 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 organisation engaged with the expert community in drawing up the list? • Is there sufficient linkage of the IA Strategy with other relevant policies? • Is there evidence of a programme of work to implement the IA Strategy? • Is the resultant programme to implement the strategy, particularly as it relates to business critical systems, adequately resourced? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: H] • Are annual IA performance targets established that detail how the organisation is to improve and achieve policy compliance in line with its endorsed statement of Information Risk appetite. [IAMM Tool Evidence Reference: 5 (v3.5/v4.0); Importance: M]	Organisational 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. • Details of the IA targets set. • An up-to-date Strategy exists, preferably as an integral part of the organisation's information strategy, together with a process to update it on a regular basis. • The IA Strategy establishes the organisation'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 organisation 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, including the requirement to use and re-use information. • Evidence of the strategy being focussed on the future preparedness of the Organisation to produce ICT solutions that are IA compliant from the start. • Evidence that the need to keep abreast of new ICT technology which, if implemented, would bring business benefit, is understood. • Evidence to show that the IA community are fully engaged with the future ICT strategy for the organisation. • Specific IA risk issues concerning Flexible Working, particularly the use of portable 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 Organisation, both now and in the foreseeable future. • Evidence of clear linkage with at least the Organisation's Information Policy, Risk Policy, Business Continuity Management Policy and KIM policy. • Evidence of formal programme documentation and processes • Evidence of an effective programme management regime. • Allocation of resources to implement the IA Strategy. • Details of the IA performance targets and how progress is measured?		A.6.1.2 A.6.1.3 4.2.1 4.2.1 b) 5) 4.2.3 f) A.6.1.1 A.6.1.8 A.6.1.6 A.6.1.7 4.2.1 A.12.1.1 A.9.2.6 A.12.1.1 4.2.3 d) A.6.1.7 A.11.7.1 A.11.7.2 A.6.1.6 4.2.1 d) 3) 4.2.3 d) 3) 4.2.2 4.2.3 5.2.1

2.2 Gaining the Public's Trust [Cyber Category Type: Peripheral]

2.2.1 Required Outcome: The Board has taken action to disseminate information both internally and externally that demonstrates what the organisation is doing to safeguard personal information in its care
[Links from 1.2.1 and to 3.2.1; IAMM Tool Question Reference: 01.02.02 (v3.5/v4.0), QUES16775599389 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Has the organisation a philosophy of transparency? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M] • Does the organisation understand the need to, and value of, keeping the public informed to assist in engendering trust in the organisation's ability to safeguard their information? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M]	• The Main 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 organisation is doing to safeguard their information and there is evidence of its successful implementation.	IS1&2 & IS6, GPGs 19 & 28.	A.15.1.4 A.8.2.2

2.3 SIRO's Responsibilities [Cyber Category Type: Supporting]

2.3.1 Required Outcome: The SIRO is fully aware of the current state of the IA control measures being applied to the organisation's business and leads the organisation's response, taking into account best practice and other HMG initiatives, ensuring that what is done is proportionate to the business need
[Links from 1.3.1 and to 3.3.1; IAMM Tool Question Reference: 01.03.02 (v3.5/v4.0), QUES167755993814 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Has the SIRO made the case and gained the approval of the Main Board for a targeted programme of work to improve the understanding and control of information risk. [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Details of the case and the approval.	IS1&2 & IS6, GPGs 19 & 28.	5.1 5.2.1
• Does the SIRO receive effective progress reports from those who manage the programme to implement the IA aspects of the Information Strategy?	• Evidence of effective two-way engagement between the SIRO and those charged with running the IA Programme.		4.2.2
• Does the SIRO report progress against the endorsed IA Strategy to the other Main Board members?	• Evidence that the SIRO ensures that Programme Milestones are achieved. • Main Board Minutes or Reports.		4.2.3 4.2.3 f)
• Has the SIRO put in place a review to assess whether the way the Information Risk Management (IRM) initiatives have bedded down within the organisation are delivering the improvement in IRM required by the business? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: L]	• Details of the Review and any action taken to improve the efficacy of the IRM regime.		4.2.3 d)
• Does the SIRO know which of the organisation's ICT Systems and information assets are business critical? (Connect with IRM 2.7) [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H]	• Criteria for establishing business criticality and a definitive list of business critical systems and information assets exist.		A.7.1 A.14.1
• Does the SIRO know the accreditation status of the Organisation's ICT Systems and has he been involved in prioritising, in terms of business risk, the list for remedial action? (Connect with IRM 2.7)	• Prioritised list endorsed by the SIRO.		A.15.2.2 A.12.1.1 A.6.1.3
• Is the SIRO and the rest of the organisation benefiting from sharing and learning best practice from others, including, other Organisations, fellow SIROs, IA specialists in NTA and industry etc? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: L]	• Engagement with the SIRO network. • Details of other engagement.		A.6.1.6 A.6.1.7 A.8.2.2

2.3.2 Required Outcome: Delivery partners and 3rd party suppliers are deriving business benefit from wider engagement on IRM matters
[Links from 1.3.2, no to links; IAMM Tool Question Reference: 01.03.05 (v3.5), 01.03.06 (v4.0), QUES167755993818 (v5.0);
Recipient Type: Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is there effective engagement between those engaged in IRM related activity within the organisations' delivery chain? • Has the organisation provided any feedback to Delivery Partners and 3rd party suppliers on the progress they are making to meet the organisation's IRM requirements? • Are there any examples of good practice being shared between organisations within the delivery chain? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: L] • Are the organisations within the delivery chain benefiting from wider IA related engagement? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: L]	• Details of any efforts being made to sponsor engagement. • Details of any feedback given. • Details of any lessons-learned activity existing within the delivery chain. • Feedback from DPs and 3rd parties regarding the success or otherwise of closer engagement.	IS1&2 & IS6, GPGs 6, 19 & 28.	A.6.2 A.10.2

2.4 IAOs Responsibilities [Cyber Category Type: Supporting]

2.4.1 Required Outcome: IAO's consider how the information assets for which they are responsible could be used more effectively to maximise the business benefit
[Links from 1.4.1, no to links; IAMM Tool Question Reference: 01.04.02 (v3.5/v4.0), QUES167755993820 (v5.0); Recipient Type: Organisation, and Delivery Partners]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Do IAOs consider on a regular, but at least 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? • Do information asset lists detail key business information as well as systems, so that a business-wide view of the utility of those assets can be formed? • Do IAOs maintain a dialogue with knowledge and information managers to ensure effective management and use of information assets? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: L]	• Sample of IAO approach to better use, together with evidence of maintaining a log. • IA lists contain details of information as well as systems. • Evidence in IAO objectives / work plans of alignment with KIM objectives.	IS1&2 & IS6, GPGs 19 & 28.	A.7.1.1

2.5 Information Security Policy [Cyber Category Type: Peripheral]

2.5.1 Required Outcome: The Information Security Policy is a working document that is regularly updated and is applied throughout the organisation and its delivery chains
[Links from 1.6.1, no to links; IAMM Tool Question Reference: 01.06.02 (v3.5/v4.0), QUES167755993824 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is the Information Security Policy reviewed at planned intervals, or when significant changes occur, to ensure its continuing suitability, adequacy and effectiveness? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: L]	• Details of the review process and changes that were made at the last review.	SPF IS1&2 & IS6, GPGs 6, 19 & 28.	A.5.1.2
• How are members of the Organisation, its Delivery Partners and its 3rd Party Suppliers made aware of the need to comply with the Information Security Policy? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: L]	• Details of the process and how its effectiveness is validated		A.6.2.3 A.8.2.1
• Are the appropriate parts of the Information Security Policy reflected in personnel and physical security policies and procedures? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: H]	• Relevant extracts from the personnel and physical security policies and procedures.		A.8 A.9

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

3.1 Board Responsibilities, Governance Structure and IA Strategy and Programme [Cyber Category Type: Supporting]

3.1.1 Required Outcome: The required improvements in IA are being delivered, the IA Strategy is regularly reviewed, and Main Board members are taking an active role in leading and championing the need for behavioural change in the staff of the organisation
[Links from 2.1.1 and to 4.1.1, 4.1.2 and 4.1.3; IAMM Tool Question Reference: 01.01.03 (v3.5/v4.0), QUES16775599382 (v5.0); Recipient Type: Organisation]
[Modified in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Are the Main Board members who are owners of the business processes, which are critical to the business actively engaged in championing the adoption of good IA practice both within the ICT Systems and by the staff who use them?	• Action that has been taken by Business Units to raise the awareness of IA across the critical areas of their business.	IS1&2 & IS6, GPGs 19 & 28.	A.6.1.1 A.6.1.3
• Is the target level of IA maturity (e.g. target for each IAMM section) set by the Main Board kept under review to ensure that it meets the needs of the business?	• Details of the review mechanism		4.2.3
• When funding becomes tight is IA spending maintained at a sufficient level to ensure IA processes are implemented in an effective way in the critical areas of the business in line with the business requirement?	• 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.		5.1 e) A.6.1.1
• Has the appropriate body with delegated responsibility for IA matters minuted receipt of periodic status reports against the annual IA Programme Plan? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M]	• Minutes of meeting.		4.2.2
• Are Programme Milestones being met in a way that gives confidence that the organisation is on course to deliver the IA Performance Improvement Targets within the approved annual IA Programme Budget? [IAMM Tool Evidence Reference: 2 & 3 (v3.5/v4.0); Importance: H]	• Progress reports against the programme plan.		4.2.3
• Has the appropriate body with delegated responsibility for IA matters minuted receipt of half yearly Delivery Chain Compliance Reports? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: M]	• Minutes of meeting. • Sample delivery chain compliance reports.		4.3.1
• If these Delivery Chain Compliance Reports show that activity is not in keeping with the organisation's stated Information Risk appetite, has the matter been escalated to the SIRO for action? [IAMM Tool Evidence Reference: 5 (v3.5/v4.0); Importance: M]	• Details of how the SIRO is kept informed of what is being done to ensure that the delivery chain bodies do what is needed to achieve satisfactory IRM.		A.6.1.1
• Is there evidence that key IRM decisions relating to business critical systems or information assets have been elevated to the Main Board for a decision, or failing	• Details of the risk analysis that supported the decision made, either by the Main Board or by the SIRO, on behalf of the Main Board.		A.6.1.1

that, that the SIRO has taken the decision, on behalf of the Main Board? (Connect with IRM 3.4) [IAMM Tool Evidence Reference: 6 (v3.5/v4.0); Importance: M]			
• Is the Management Board aware of the systemic IA risks that impact on the delivery of the Organisation's outputs? (Connect with IRM 3.4)	• Main Board papers showing submission of data and subsequent actions being taken.		4.2.1 d)
• Does the Main Board receive reports from the SIRO on the progress being made by the organisation, its Delivery Partners and its 3rd party suppliers to mitigate the gaps in IA measures that exist within the organisation's delivery chain?	• Details of the gap analysis and what is being done to address the shortfalls.		4.2.4
• Is the IA strategy element of the organisation's Information Strategy (or other similar Corporate Strategy), subject to regular review to ensure that it remains aligned to the needs of the business in the context of the current threat, vulnerabilities and opportunities?	• Details of the review process and what changes have been made.		4.2.3
• Does a process exist to check that IA requirements included in other corporate strategies remain coherent and aligned with the main strategy, so that they meet the needs of the business?	• Details of the process.		A.5.1.2
• Is the IA programme managed effectively? • Does the SIRO receive regular updates from the IA programme manager?	• 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 meet its deliverables.		4.2.2
• Is the IA programme on course to deliver the Main Board's intent detailed in the IA strategy in a timescale and at a cost acceptable to the business?	• Details of the benefit realisation plan.		

3.2 Gaining the Public's Trust [Cyber Category Type: Peripheral]

3.2.1 Required Outcome: There is improvement in the level of trust that both employees and the public have in the organisation's ability to safeguard their information
[Links from 2.2.1 and to 4.2.1; IAMM Tool Question Reference: 01.02.03 (v3.5/v4.0), QUES167755993810 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Has the appropriate body with delegated responsibility for IA matters received progress reports against the communications and an action plan which demonstrate that trust is being built both internally and externally in the organisation's ability to safeguard personal information? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M]	• Progress reports and any other detail that shows that this issue is being taken seriously.	IS1&2 & IS6, GPGs 19 & 28.	4.2.2

3.3 SIRO's Responsibilities [Cyber Category Type: Supporting]

3.3.1 Required Outcome: The SIRO has taken effective control of the IA programme, including effective engagement with the delivery chain, and has taken action to align it to the business needs of the organisation
[Links from 2.3.1 and to 4.3.1; IAMM Tool Question Reference: 01.03.03 (v3.5/v4.0), QUES167755993815 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Has the IA Review been completed and the Report issued? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: L]	• IA Review Report.	IS1&2 & IS6, GPGs 6, 19 & 28.	4.2.3 d)
• Has a gap analysis been undertaken following the Review to determine how the organisation's IA Strategy and IA Programme should be re-aligned to meet the developing needs of the business? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H]	• Details of the Gap Analysis and any work to close identified gaps.		4.2.4
• Does the SIRO regularly produce progress reports for the Main Board detailing how the programme to implement the IA Strategy is delivering the Main Board's intent? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: M]	• Progress reports presented to the Main Board.		5.1
• Does the SIRO hold bilateral or multilateral meetings/workshops to identify gaps in the approach being taken by the organisations that comprise the delivery chain?	• Details of any meetings held and the resultant output.		A.6.2 A.10.2

LEVEL 4 – Quantitatively Managed – The board has established its broader IA Road Map for all its information, systems and processes

4.1 Board Responsibilities, Governance Structure and IA Strategy and Programme [Cyber Category Type: Supporting]

4.1.1 Required Outcome: The main board sets the strategic direction on managing all information (and security) risks that would have an adverse effect on the business [Links from 3.1.1 and to 5.1.1; IAMM Tool Question Reference: 01.01.04 (v4.0), QUES16775599383 (v5.0); Recipient Type: Organisation][Modified in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Has an assessment been made of the overall alignment/coherence of the progress being made by Delivery Partners and 3rd party suppliers with that of the main body of the organisation? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: H]	• Details of the assessment and any action taken to improve alignment/coherence.	IS1&2 & IS6, GPGs 19 & 28.	4.2.3 d)
• Does the Main Board know how many business processes and related ICT Systems are not implementing good IA practice, and do they have a broader road map to correct this, where appropriate? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: H]	• Reports made to the Main Board by the SIRO detailing the IA status of all IS and related processes within the organisation (and evidence of its contribution to the maintenance of the broader IA improvement road map).		4.2.3 4.2.4 A.6.1.8
• Is the Management Board made aware of the key IA risks (including future risks) affecting all ICT Systems, together with the systemic IA risks that impact on the delivery of the Organisation's outputs? (Connect with IRM 4.4) [IAMM Tool Evidence Reference: 3 (v4.0); Importance: M][Modified in GPG40 Version 2.0]	• Main Board papers showing submission of data and subsequent actions being taken (e.g. documented, and active, process to ensure the Main Board is briefed on future risks).		A.15.2.1 4.2.1 h)
• 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? [IAMM Tool Evidence Reference: 4 (v4.0); Importance: H]	• Investment Appraisal.		5.1 e)
• If a Main 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? [IAMM Tool Evidence Reference: 5 (v4.0); Importance: H]	• Details of the IRM analysis presented to the Main Board.		5.1 f)
• Does the Main Board receive regular reports of progress against the IA Strategy Milestones? [IAMM Tool Evidence Reference: 6 (v4.0); Importance: H]	• Main Board Minutes provide evidence of discussion and resultant actions. Evidence of follow-up of actions		5.2.1 a)

• Does the Main Board ensure that sufficient funding is allocated to IA as a % of its overall budget and the importance of information to its business? [IAMM Tool Evidence Reference: 7 (v4.0); Importance: H]	• Either the Main Board has taken a paper from the CIO analysing and quantifying the importance of Information to the business of the organisation, or the detail is included within the organisation's Information Policy. • A process exists to capture the IA expenditure of the organisation as a % of the overall budget. • Evidence that funds are allocated to IA commensurate with its importance to the business.		5.2

4.1.2 Required Outcome: The IA Strategy is fully aligned to the overall business strategy and its application is monitored to ensure proportionality
[Links from 3.1.1; IAMM Tool Question Reference: 01.01.06 (v4.0), QUES16775599385 (v5.0); Recipient Type: Organisation][Modified in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• How is the IA Strategy aligned to other major business strategies? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: H] • Does the IA Strategy form part of an overall Information Management Strategy so that it is aligned to related strategies such as the KIM Strategy? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: M]	• Details of how IA is integrated into the organisation's approach to business so that it is becoming part of business as usual. • IA forming a key building block within other strategies.	IS1&2 & IS6, GPGs 19 & 28.	4.2.3 d) 3)

4.1.3 Required Outcome: The implementation of the strategy is actively managed to ensure that sustainable improvements in IA are made that deliver real business benefits
[Links from 3.1.1; IAMM Tool Question Reference: 01.01.07 (v4.0), QUES16775599386 (v5.0); Recipient Type: Organisation][Modified in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• What has been done to ensure that the IA measures put in place in response to the IA programme are sustainable over time? (i.e. have the changes made been embedded to the extent that they are considered to be business as usual?) [IAMM Tool Evidence Reference: 1 (v4.0); Importance: H] • What action has been taken to provide evidence of hard and soft benefits delivered by the IA programme to justify further investment? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: M]	• Details of specific actions taken (e.g. lessons learned reviews to demonstrate the evolution of measures and the impact on sustainability) to ensure that improvements are not ephemeral. • Details of the benefits realised (e.g. monitoring was sufficiently detailed to detect fraud, inaccuracy, or misuse) and how that information has been used to influence further investment.	IS1&2 & IS6, GPGs 19 & 28.	5.1

4.2 Gaining the Public's Trust [Cyber Category Type: Peripheral]

4.2.1 Required Outcome: The organisation has implemented robust measures to safeguard its information so that both its employees, and the public, trust it with their information
[Links from 3.2.1 to 5.2.1; IAMM Tool Question Reference: 01.02.04 (v4.0), QUES167755993811 (v5.0); Recipient Type: Organisation][Modified in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• In the context of the effective application of IRM, is the organisation held up by those across Government as an exemplar of good IRM practice?" [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M] • Do other bodies, with which the organisation does business, have trust in the IRM regime enacted within the organisation? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: M] • Is there any public (or employee) opinion polling information to confirm that the official views held (e.g. across Government) are shared by the public (or the organisation's employees)? [IAMM Tool Evidence Reference: 3 (v4.0); Importance: M][Modified in GPG40 Version 2.0]	• External assessments and feedback from the CIO council. • No evidence of other bodies requiring additional measures to be put in place to reinforce what is being done in the organisation. • Opinion polls (public and employee), response to on-line feedback pages, level of take-up of on-line services.	IS1&2 & IS6, GPGs 19 & 28.	

4.3 SIRO's Responsibilities [Cyber Category Type: Supporting]			
4.3.1 Required Outcome: The SIRO has oversight of an enduring process that evaluates the effectiveness of its IA governance structure to ascertain whether it meets the business need, is aligned with other business areas and is flexible enough to accommodate business change, without being disproportionate on effort and costs [Links from 3.3.1; IAMM Tool Question Reference: 01.03.04 (v4.0), QUES167755993816 (v5.0); Recipient Type: Organisation][Modified in GPG 40 Version 2.0]			
Areas to Probe	**Evidence Expected**	**Policy Reference**	**ISO27001 Reference**
• Has the SIRO initiated a review of the IA element of the Information Strategy (or other corporate business strategy, e.g. in response to the transparency agenda) to ensure that the appropriate focus is given to Availability and Integrity vis-à-vis Confidentiality, so that IA assists in, and aligns with, the exploitation of information to derive greater business benefit from the organisation's information assets? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: H][Modified in GPG40 Version 2.0]	• Details of the review, and evidence of on-going maintenance alignment of the earlier level cross-referencing between initiatives' official documentation (e.g. strategic inter-relationships established between initiatives, which is minuted), and appropriate cross-fertilisation (e.g. building on IAO's and KIM managers dialogue, and other relationships).	IS1&2 & IS6, GPGs 19 & 28.	4.1 4.2.3 4.2.4
• What proactive and reactive measures, including resources can the SIRO deploy to limit the business impact of information risks when they materialise? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: M]	• Details of the planned responses to key risks.		4.2.3

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

5.1 Board Responsibilities, Governance Structure and IA Strategy and Programme [Cyber Category Type: Supporting]

5.1.1 Required Outcome: Effective IRM disciplines are woven into the fabric of the organisation in such a way that they are an integral part of normal business
[Links from 4.1.1; IAMM Tool Question Reference: 01.01.05 (v4.0), QUES16775599384 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is the Main Board regularly presented with an accurate picture of the IA risk exposure of the organisation? (Connect with IRM 5.2) [IAMM Tool Evidence Reference: 1 (v4.0); Importance: H]	• Where appropriate, IA is considered as an integral part of the standard processes within the organisation at all levels and within its Delivery Partners and 3rd party suppliers.	IS1&2 & IS6, GPGs 19 & 28.	A.6.1.1
• Do all Main Board Members appreciate the critical role that information plays in the success of the organisation's business? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: H][Modified in GPG40 Version 2.0]	• Main Board papers and Annual Report of the organisation (e.g. with evidence that decisions have been made based on expert guidance).		A.6.1.1
• Is IA still considered to be a discrete discipline, or is it considered to be an integral part of normal business? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: M]	• By word and action all Main Board members advocate the need for effective IA measures to be implemented to safeguard the business of the organisation.		A.6.1.1

5.2 Gaining the Public's Trust [Cyber Category Type: Peripheral]

5.2.1 Required Outcome: The organisation is trusted to strike an effective balance between the need to maintain the confidentiality of sensitive information and the need to put information into the public arena
[Links from 4.2.1; IAMM Tool Question Reference: 01.02.05 (v4.0), QUES167755993812 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is the organisation open and honest about what it is doing to safeguard personal information in its charge? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M][Modified in GPG40 Version 2.0]	• Quality of reporting to Parliament, PQs and other public responses, followed-up with opinion polls, response to on-line feedback pages, and measurements like the level of take-up of on-line services.	IS1&2 & IS6, GPGs 19 & 28.	

2. Training, Education and Awareness

Level 1 – Initial	Level 2 – Established	Level 3 – Business Enabling	Level 4 – Quantitatively Managed	Level 5 – Optimised
Awareness of the Criticality of IA to the Business and its Legal Requirements	IA Processes are Institutionalised	IA Processes are Implemented in Critical Areas of the Business	The board has established its broader IA Road Map for all its information, systems and processes	Responsive IA processes are integrated as Part of Normal Business
A balanced and targeted programme of annual information risk awareness training is instituted for all staff within the organisation, its Delivery Partners and 3rd party suppliers who have access to the organisation's information. A cultural change plan is implemented.	All members of the organisation undergo annual risk awareness training. A programme of targeted education and training is instituted for IA professionals and for middle and senior managers. Staff behaviours are measured and trends analysed. Progress against the organisation's cultural change goals is managed and reported to the SIRO.	As understanding across the organisation is raised, training becomes more targeted. Key staff are trained and take effective information risk management decisions. 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. The training is matched to the business need and action is taken to ensure specialist, corporate IA knowledge is retained. Evidence show that staff attitudes and behaviours towards assuring information are aligned to the needs of the business.	The need to assure the organisation's Information and that of its external stakeholders as a key business asset is fully embedded within the organisational 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 organisation that values information as a business asset.

Justification Without effective training, education and awareness staff within the organisation 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

1.1 General IRM Training [Cyber Category Type: Supporting]

1.1.1 Required Outcome: General staff awareness of the need to provide effective protection in terms of Confidentiality to the organisation's information, specifically, but not exclusively, to its personal data, has been raised. This applies to the members of the organisation and to those within the delivery chains that have access to the organisation's information.
[Links to 2.1.1; IAMM Tool Question Reference: 02.01.01 (v3.5/v4.0), QUES167755993825 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does every member of the organisation, its Delivery Partners and 3rd party suppliers (including, where appropriate, their supply chains) who have access to organisation's information and particularly its personal data, undergo an annual session of information risk awareness training stressing in particular the need to protect the confidentiality of the information? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H] • Is this training incorporated as part of the induction process? • Does the training include some form of assessment so that there is an improved	• 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	IS1&2 & IS6, GPGs 6, 19 & 28.	5.2.2 A.8.2.2

chance that the material is remembered? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: L]	training remember what they have been taught.		
Note: Organisations will wish to satisfy themselves that their Delivery Partners and 3rd party suppliers are discharging the training requirement satisfactorily. Organisations should make available the evidence that they are relying on to manage this risk and any assurance process that they have put in place to satisfy themselves that the training is adequate.			A.6.2.3 A.10.2.2

1.1.2 Required Outcome: The Business understands the need to improve its middle management's understanding of the requirement for effective IA controls (in terms of Availability and Integrity and not just Confidentiality). This applies to the members of the organisation and to those within the delivery chains who have access to the organisation's information
[Links to 2.1.2; IAMM Tool Question Reference: 02.01.04 (v3.5), 02.01.05 (v4.0), QUES167755993829 (v5.0); Recipient Type: Organisation, and Delivery Partners]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Has the organisation acknowledged the need for middle management to undergo additional training to supplement the catch-all message of the need to protect the Confidentiality of the organisation's information with the equally important need to maintain the Availability and Integrity of the information? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H] • Do plans exist to identify those who should receive this additional training? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M]	• Discussion papers (e.g. related to cultural change) relating to this need. • Details of the plans.	IS1&2 & IS6, GPGs 6, 19 & 28.	5.2.2 A.8.2.2

1.1.3 Required Outcome: The Business understands the need for middle and senior managers to improve their understanding of the need to balance protecting the organisation's information with the requirement to use and exploit that information for business benefit
[Links to 2.1.3; IAMM Tool Question Reference: 02.01.07 (v3.5), 02.01.08 (v4.0), QUES167755993832 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is the organisation aware of the IS6 Mandatory Requirement for the SIRO and IAOs to pass information risk management training on appointment? • Does the organisation accept the need for specific training to be given within the organisation to middle and senior managers of the business requirement to balance the need to protect the organisation's information with the need to use and exploit the information? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M] • Do plans exist to identify those who should receive this additional training?	• Plans detailing how the SIRO and IAOs are to receive appropriate training and how appropriate training is built into any succession planning. • Discussion papers relating to this need. • Details of the plans.	IS1&2 & IS6, GPGs 6, 19 & 28.	5.2.2 A.8.2.2

1.1.4 Required Outcome: The SIRO is content that all members of staff within the organisation, its Delivery Partners and its 3rd party suppliers receive adequate training in their responsibilities with regard to protecting the Confidentiality of the organisation's information
[Links to 2.1.4; IAMM Tool Question Reference: 02.01.10 (v3.5), 02.01.12 (v4.0), QUES167755993836 (v5.0); Recipient Type: Organisation, and Delivery Partners]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• How does the SIRO assure himself/herself that every member of staff within the organisation, its Delivery Partners and 3rd party suppliers (including, where appropriate, their supply chains) who have access to the organisation's information, receive effective information risk awareness training on induction and annually thereafter? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Details of the assurance process.	IS1&2 & IS6, GPGs 6, 19 & 28.	8.2 a) A.15.2.2

1.2 Specialist IRM Training [Cyber Category Type: Supporting]

1.2.1 Required Outcome: The need for staff who have IA management responsibilities and for those who manage or maintain the secure configuration of ICT systems to have targeted education and training is understood
[Links to 2.2.1; IAMM Tool Question Reference: 02.02.01 (v3.5/v4.0), QUES167755993840 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Has a training needs analysis has been undertaken to determine what education and training is needed for those who manage and/or maintain the secure configuration of ICT systems and for those who have IA management responsibilities? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M]	• Details of the training needs analysis.	IS1&2 & IS6, GPGs 6, 19 & 28.	5.2.2 a)
• Do plans exist to introduce appropriate education and training to meet the organisation's needs? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H]	• Details of the plans.		

1.3 Cultural Change [Cyber Category Type: Supporting]

1.3.1 Required Outcome: The senior management of the organisation understand that changing the behaviour of the organisation's staff so that they adequately protect the organisation's information is a long and complex process and they have charged the SIRO with establishing effective processes to deliver the required change and for ensuring that the outcomes are delivered
[Links to 2.3.1; IAMM Tool Question Reference: 02.03.01 (v3.5/v4.0), QUES167755993844 (v5.0); Recipient Type: Organisation, and Delivery Partners]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Has the SIRO, or SIRO equivalent in DPs, produced a plan to introduce processes within the organisation that assist in the aim of fostering a culture that values, protects and uses information for the public good within the organisation?	• Details of the SIRO's plans.	IS1&2 & IS6, GPGs 6, 19 & 28.	4.2.1
• Have the SIRO's plans been endorsed by the Main Board? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Main Board minutes.		
• Do the SIRO's plans include processes to address the following?:			A.8.2.1
• Effective and consistent HR arrangements to reward positive approaches to information risk and to penalise negative activity, HR arrangements make it clear that failure to apply the organisation's procedures is a serious matter and, in some situations, amounts to gross misconduct. [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M]	• Details of reward and retribution mechanisms.		A.8.2.3
• 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. [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: M]	• Details of mechanisms which command the confidence of staff.		A.13.1.2
• The insertion of questions in personnel surveys to give some indication of the effectiveness of the information risk cultural change processes in delivering changed attitudes in the organisation. [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: M]	• Details of planned survey questions and the responses derived.		7.2 b)
• Is the range of processes to be implemented comprehensive enough to affect the required cultural change?	• Details of the processes to be implemented.		8.2

LEVEL 2 – Established - IA Processes are Institutionalised

2.1 General IRM Training [Cyber Category Type: Supporting]

2.1.1 Required Outcome: General staff understanding of the need to provide effective protection for the organisation's information in terms of Confidentiality remains at a level that meets the needs of the business.
[Links from 1.1.1 and to 3.1.1; IAMM Tool Question Reference: 02.01.02 (v3.5/v4.0), QUES167755993826 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• What has been done to assess the efficacy of the annual IRM training given to staff in the organisation, its Delivery Partners and within its 3rd party suppliers to provide assurance that it meets the needs of the business? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M] • Has anything been done to target the training to address particular parts of the business that are subject to higher risk? • How the training material is refreshed and kept relevant to the needs of the staff and the business? • Has any analysis been undertaken to assess whether discrete IRM training is still required, or whether the message could be better delivered by incorporating it within other training modules?	• Details of any assessment undertaken that provides evidence to confirm that the training being given is having an effect on improving the Confidentiality of the organisation's information? • Details of any exercise undertaken to focus the training delivered to match the needs of the business. • Imaginative ideas to maintain staff interest and engagement with the subject. • Details of the analysis and any conclusions drawn.	IS1&2 & IS6, GPGs 6, 19 & 28.	A.8.2.2 8.2

2.1.2 Required Outcome: At the appropriate levels of middle management within the organisation the level of understanding of IRM has been raised so that the need to secure the Availability and Integrity of the organisation's information is understood
[Links from 1.1.2 and to 3.1.2; IAMM Tool Question Reference: 02.01.05 (v3.5), 02.01.06 (v4.0), QUES167755993830 (v5.0);
Recipient Type: Organisation, and Delivery Partners]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is additional IRM training available for middle management within the organisation which addresses the need to give appropriate protection to the organisation's information to assure its Availability and Integrity, in addition to its Confidentiality? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M] • What evidence does the organisation have that Delivery Partners are also delivering this training to their middle management? • Does the training include some form of assessment so that there is an improved chance that the material is remembered? • Is it clear who should receive this additional training? • Have those who have been identified as needing the training been trained? • As a result of the training received by middle managers is there evidence that IRM decisions are made not just to address the narrow issue of Confidentiality, but also to ensure the Availability and Integrity of information to meet the business need?	• Details of the material provided and how it is delivered. • Details of what the organisation knows about what is done to address this need in delivery partner organisations. • An effective mechanism exists to ensure that those who have undergone the training remember what they have been taught. • Clear criteria exist to determine who should receive this training. • Training statistics. • Details of how the efficacy of this training is assessed.	IS1&2 & IS6, GPGs 6, 19 & 28.	A.8.2.2 A.15.2.1

2.1.3 Required Outcome: Middle and senior management understand the need to balance the requirement to protect the organisation's information with the requirement to use and exploit that information for business benefit
[Links from 1.1.3 and to 3.1.3; IAMM Tool Question Reference: 02.01.08 (v3.5), 02.01.09 (v4.0), QUES167755993833 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Have the SIRO and the IAOs received and passed the mandatory IRM training? • Is a process in place to ensure that when the current SIRO or IAOs move post, the new incumbents will receive training? • What training has been given within the organisation to middle and senior managers of the business requirement to balance the need to protect the organisation's information with the need to use and exploit the information? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M] • As a result of the training received by middle and senior managers, is there evidence that they are able to set realistic information risk expectations for the business? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M] • Are the delivery and content of this information risk awareness training coordinated with the delivery and content of more generalised Information Management (IM) training?	• Training details. • Details of the process. • Details of the training (e.g. as a minimum for the AO, SIRO, IAOs and members of the Audit Committee) • Risk management decisions are made based on a sound rationale. • Details of how IRM training is coordinated with general IM training.	IS1&2 & IS6, GPGs 6, 19 & 28.	5.2.2 A.8.2.2

2.1.4 Required Outcome: The SIRO is content that the understanding of Information Risk Management at the appropriate levels of management within the organisation, its Delivery Partners and its 3rd party suppliers, is sufficient to meet the needs of the business and that any action needed to re-focus or reinvigorate training has been taken
[Links from 1.1.4 and to 3.1.4; IAMM Tool Question Reference: 02.01.11 (v3.5), 02.01.13 (v3.5/v4.0), QUES167755993837 (v5.0);
Recipient Type: Organisation, and Delivery Partners]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• How does the SIRO assure himself/herself that every member of staff within the Department, its Delivery Partners and 3rd party suppliers receive appropriate training on induction and annually thereafter? • 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? • How does the SIRO satisfy himself/herself that the information risk training being given across the organisation, its Delivery Partners and its 3rd party suppliers (including where appropriate their supply chains) is sufficient in terms of depth, breadth and coverage to produce the desired business benefit? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H] • Where appropriate, what assurance has been given to the SIRO that training has been re-focussed and re-invigorated to better align it to the needs of the business. [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M]	• Details of the assurance process. • 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. • Details of any review of training put in place by the SIRO. • Details of any action taken to keep the training material fresh and relevant to the needs of the business.	IS1&2 & IS6, GPGs 6, 19 & 28.	A.15.2.1

2.2 Specialist IRM Training [Cyber Category Type: Supporting]

2.2.1 Required Outcome: Specialist IRM training for IA management staff and for those who manage or maintain the secure configuration of ICT systems has been put in place
[Links from 1.2.1 and to 3.2.1; IAMM Tool Question Reference: 02.02.02 (v3.5/v4.0), QUES167755993841 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Are the DSO, ITSO and COMSO trained and competent to perform the roles? • Does a programme of targeted education and training exist for staff who manage/maintain the secure configuration of ICT systems or have IA responsibilities? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• The individuals are trained to discharge their duties in a competent manner. • Details of the training provided.	IS1&2 & IS6, GPGs 6, 19 & 28.	5.2.2 A.8.2.2
• Is an effective process in place to select staff for further education and/or training on IA matters? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: L]	• Details of the process and the numbers of staff who have undergone the education and/or training and details of its effectiveness.		
• How is the effectiveness of the education and/or training measured? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: L]	• Investment appraisal information. Course feedback of the applicability and suitability of the education and/or training		

2.3 Cultural Change [Cyber Category Type: Supporting]

2.3.1 Required Outcome: The SIRO is content that the actions resulting from the Cultural Change Processes are starting to deliver a change in staff attitudes with regard to the application of effective information risk management
[Links from 1.3.1 and to 3.3.1; IAMM Tool Question Reference: 02.03.02 (v3.5/v4.0), QUES167755993845 (v5.0); Recipient Type: Organisation, and Delivery Partners]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• How does the SIRO, or SIRO equivalent in DPs receive regular progress reports of how the cultural change processes are aiding the achievement of the required change in staff attitudes to IRM within the organisation? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Details of the cultural change management process. • Details of progress reports submitted to the SIRO.	IS1&2 & IS6, GPGs 6, 19 & 28.	4.2.2
• Is the SIRO, or his equivalent in DPs, satisfied that the processes which have been introduced to aid the achievement of effective IRM within the organisation are proportionate to the risk?	• Details of the SIRO's assessment and evidence on which he is basing his judgement.		4.2.3
• How effective are the HR processes put in place to promote information risk awareness in achieving the following?:			A.8.2.1
• Rewarding positive approaches to information risk and penalising negative activity. [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M]	• Details of reward and retribution mechanisms.		
• Ensuring a consistent application of disciplinary action across the organisation. [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: L]	• Details of how consistency is achieved.		
• Staff concerns about information risk are brought to the attention of senior management, or the Audit Committee, anonymously if necessary. [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: L]	• Details of mechanisms which command the confidence of staff. • Details of concerns and resulting action taken.		A.13.1.2
• Feedback from staff through personnel surveys about the effectiveness of the cultural change programme. [IAMM Tool Evidence Reference: 5 (v3.5/v4.0); Importance: L]	• Details of planned survey questions and the responses derived.		
• Does the system of Reward and Recognition to acknowledge those who adopt	• Evidence that the Reward and Recognition system is working and is proving		

the right approach to IA work in practice? • Is consistent disciplinary action taken, and is it seen to be taken, against those who flout IA requirements? • Are the responses to questions inserted in staff surveys being used to determine the effectiveness of the cultural change processes?	useful in promoting IA awareness. • Prompt, consistent and effective action is taken against those who break the IA rules. • Details of how feedback is used to maintain the effectiveness of the processes.		A.8.2.3 8.1

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

3.1 General IRM Training [Cyber Category Type: Supporting]

3.1.1 Required Outcome: The requirement for all staff to provide effective protection in terms of Confidentiality for the organisation's Business Critical information is so embedded within the culture of the organisation that Information Risk Management (IRM) training is not separate, but integrated as a module into all other relevant training
[Links from 2.1.1; IAMM Tool Question Reference: 02.01.03 (v3.5/v4.0), QUES167755993827 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is general IRM training still delivered to all, or is it more effectively targeted to meet the needs of the business? • Is the general IRM training still delivered as a discrete package, or is it integrated as a module into all other relevant training? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M] • What is being done to ensure that the more targeted approach to delivering the training is meeting the business need?	• Details of any consideration of introducing targeted training to those where the risk is greatest. • Evidence that delivering IRM modules within other training is better matched to the needs of the business. • Details of any risk assessments and risk based decisions to exclude or to apply a proportionate approach to the delivery of TE&A activity across Business Units.	IS1&2 & IS6, GPGs 6, 19 & 28.	A.8.2.2 A.15.2.1 4.3.1

3.1.2 Required Outcome: Decisions are being made by middle managers that show that IA controls are being implemented on Business Critical IS not just for Confidentiality, but also to ensure the Availability and Integrity of the organisation's information
[Links from 2.1.2; IAMM Tool Question Reference: 02.01.06 (v3.5) 02.01.07 (v4.0), QUES167755993831 (v5.0); Recipient Type: Organisation, and Delivery Partners]
[Modified in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• What evidence is there that middle managers take decisions concerning business critical IS and their related business processes that show they understand the need for effective controls to ensure the Availability and Integrity of the organisation's information and not just its Confidentiality? [IAMM Tool Evidence Reference: 1 & 2 (v3.5/v4.0); Importance: M] • Is this approach widespread across the organisation? • How embedded is this approach within delivery partner organisations (e.g. within delivery chains)? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M]	• Effective IA controls that protect the Confidentiality, Availability and Integrity of the organisation's business critical information are being applied by middle managers within the organisation. • More than one instance in different parts of the business. • Evidence to show effective IRM decision making.	IS1&2 & IS6, GPGs 6, 19 & 28.	5.1 A.6.2.3

3.1.3 Required Outcome: The needs of the business are being met by middle and senior managers who are making effective risk based decisions based on their deeper knowledge and understanding of IRM
[Links from 2.1.3; IAMM Tool Question Reference: 02.01.09 (v3.5), 02.01.10 (v4.0), QUES167755993834 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Are the processes in place to provide middle and senior managers with the appropriate information to enable them to take fully informed risk based decisions? • Are risk based decisions being taken by middle and senior management that show they understand how effective IA controls can be implemented to enable, rather than disable the business critical processes of the organisation. [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M] • What measures have been put in place to address the need for staff to value and use information for the public good as opposed to concentrating merely on protecting the information? • Has the effectiveness of the training provided for the, SIRO and IAOs been assessed?	• Details of the process by which decisions are elevated within the organisation. • Details of effective risk based decisions that have been taken by management. • Actions originating from the plan take a balanced approach that seeks to make best use of information for the public good. • Details of the validation process and any action taken to re-align the training to the needs of the business.	IS1&2 & IS6, GPGs 6, 19 & 28.	4.2.1 4.3.3 5.2.2 A.8.2.2

3.1.4 Required Outcome: The SIRO is content that the IRM training which is in place within the organisation and its supply chains, in terms of its depth, breadth and coverage, is such that effective risk management decisions are being made that enable the needs of the business.
[Links from 2.1.4 and to 4.1.1; IAMM Tool Question Reference: 02.01.12 (v3.5), 02.01.14 (v4.0), QUES167755993838 (v5.0);
Recipient Type: Organisation, and Delivery Partners]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• What information is the SIRO provided with to enable him to determine whether the training delivered within the organisation, its Delivery Partners and within its 3rd party suppliers is sufficient to meet the business need? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H] • Is the information comprehensive enough to enable effective decision making? • Is the SIRO content that the IRM training which is in place within the organisation and its delivery chains, in terms of its depth, breadth and coverage, is such that effective risk management decisions are being made that enable the needs of the business?	• Details of the information. • Assessment (based on experience) of the evidence provided. • Statement by the SIRO.	IS1&2 & IS6, GPGs 6, 19 & 28.	8.2 a) A.15.2.2

3.2 Specialist IRM Training [Cyber Category Type: Supporting]

3.2.1 Required Outcome: All those who need specialised IRM and IA training have received the appropriate training to enable them to discharge their duties in a way that meets the needs of the business
[Links from 2.2.1 and to 4.2.1; IAMM Tool Question Reference: 02.02.03 (v3.5/v4.0), QUES167755993842 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is there an effective IA training regime in place for all staff who hold key IA related appointments? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H] • Is this training undertaken on appointment? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: L] • How is this specialist training validated? • Is there a development programme for existing staff that enables them to maintain and develop their existing professional capabilities? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: M][Added in GPG40 Version 2.0]	• 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 on appointment. • Course feedback of the applicability of the training. • Evidence of the development programme for staff (e.g. career profiles, and training/development pathways to professional recognition).	IS1&2 & IS6, GPGs 6, 19 & 28.	5.2.2 A.8.2.2

3.3 Cultural Change [Cyber Category Type: Supporting]			
3.3.1 Required Outcome: The SIRO is content that the Cultural Change Processes have delivered a sustained change in staff attitudes and are starting to deliver a change in staff behaviours with regard to the application of effective information risk management [Links from 2.3.1 and to 4.3.1; IAMM Tool Question Reference: 02.03.03 (v3.5/v4.0), QUES167755993846 (v5.0); Recipient Type: Organisation, and Delivery Partners]			
Areas to Probe	**Evidence Expected**	**Policy Reference**	**ISO27001 Reference**
• How integrated is the activity and underlying processes introduced to deliver IRM cultural change integrated with other IM business objectives? • Is there evidence of effective data gathering to assess whether the desired changes in approach to IRM are being adopted into the culture of the organisation, its Delivery Partners and within its 3rd party suppliers? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: H]	• Details of the linkage, so that the achievement of effective IRM is viewed in its proper context alongside other IM initiatives. • Details of how the data is gathered.	IS1&2 & IS6, GPGs 6, 19 & 28.	
• Is the resultant data analysed and is action taken to re-adjust the approach to IRM education and training, and the supporting processes, to promote the desired cultural change? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Details of the analysis made and how this is used to change the approach to IRM training.		4.2.3
• Is there a sustained improvement in staff awareness of the importance of effective IRM to the business of the organisation as measured through a staff attitude survey, or similar mechanism? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: L]	• Details of how the efficacy of the cultural change processes are measured and what is done with the results.		4.2.4 b)
• After a possible initial rise, there is a downwards trend in the number of staff concerns about information risk being brought to the attention of senior management, or the Audit Committee, together with a downward trend in the number of reported IA incidents. [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: M]	• Analysis of the statistical data concerning staff issues and IA incidents.		

LEVEL 4 – Quantitatively Managed – The board has established its broader IA Road Map for all its information, systems and processes

4.1 General IRM Training [Cyber Category Type: Supporting]			
4.1.1 Required Outcome: The SIRO has evidence that a proportionate IRM training strategy is communicated to, and understood by, Delivery Partners and third party suppliers, and is matched to the current and future business need, and is reflected (e.g. IRM messages) in all appropriate training packages [Links from 3.1.1; IAMM Tool Question Reference: 02.01.04 (v4.0), QUES167755993828 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties] [Modified in GPG 40 Version 2.0]			
Areas to Probe	**Evidence Expected**	**Policy Reference**	**ISO27001 Reference**
• How is the SIRO provided with evidence in the effectiveness of IRM training strategy communications with Delivery Partners and third parties? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M] • Are the communication plans kept fresh and relevant? [IAMM Tool Evidence Reference: 2 (/v4.0); Importance: M] • Are accurate details of the members of staff (and appropriate contractors) who have been educated and trained, in IRM, within its Delivery Partners and its 3rd party suppliers reported to the SIRO? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: L]	• Reports on the response to IRM training strategy related communications (e.g. reports and summaries of minutes of IRM focussed meetings with Delivery Partners and third parties). • A training communication plan that not only meets the current business needs, but also helps to meet the future business needs. • Details of the education and training reports submitted to the SIRO relating to Delivery Partners and third parties.	IS1&2 & IS6, GPGs 6, 19 & 28.	A.8.2.2 4.2.3

4.1.2 Required Outcome: The SIRO has evidence, from within the organisation, its Delivery Partners and 3rd party suppliers, that the IRM training strategy (with regards to protecting, managing and exploiting information) is aligned to the needs of the business
[Links from 3.1.3; IAMM Tool Question Reference: 02.01.11 (v4.0), QUES167755993835 (v5.0); Recipient Type: Organisation][New in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• What evidence is provided to the SIRO, from the organisation, its Delivery Partners and 3rd party suppliers, to show that the IRM training strategy is aligned with the business needs? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M] • Is there a plan to take appropriate action in response to the IRM education and training assessments, where feedback indicates there should be an adjustment to the IRM training strategy? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: L] • Is the overall IRM training coordinated effectively with other aspects of IM training? [IAMM Tool Evidence Reference: 3 (v4.0); Importance: M]	• Evidence that all appropriate system IRM requirements are being considered when creating, and maintaining, the IRM training strategy. • Evidence that IAO's and managers are ensuring that appropriate future IRM training will be available for those that need it. • Details of any action taken to realign education and training requirements to the objectives of the cultural change goals, and any response through changes in the broader road map. • Details of how IRM training (and training plans/planning) is integrated with other IM related training.	IS1&2 & IS6, GPGs 6, 19 & 28.	A.8.2.2 4.2.3

4.1.3 Required Outcome: Plans are in place to assess training needs to support future strategic objectives, and there is robust evidence to support that there is effective monitoring of IRM training delivery across the organisation, its Delivery Partners and 3rd party suppliers
[Links from 3.1.4; IAMM Tool Question Reference: 02.01.15 (v4.0), QUES167755993839 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]
[New in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• How are future strategic objectives captured and fed into the IRM training needs analysis? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: H] • Is an assessment made of the coverage and effectiveness of the entire range of IRM education and training which is delivered against the requirements of the organisation's cultural change goals? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: M]	• Documentation showing the impact of strategic objectives on the skill requirements of IA resources (e.g. minutes of meetings, and/or documentation uplift), and how this information is being used to guide training needs planning and planned training content. • Details of the education and training analysis submitted to the SIRO. • Evidence that delivery partners and 3rd party suppliers' TE&A activities are assessed and remain aligned with the organisation's cultural change goals and their internal training delivery.	IS1&2 & IS6, GPGs 6, 19 & 28.	A.8.2.2 4.2.3 4.2.4 b)

4.2 Specialist IRM Training [Cyber Category Type: Supporting]

4.2.1 Required Outcome: The SIRO has evidence that IA capability, and knowledge, is being retained, developed and used effectively and pragmatically to support business needs
[Links from 3.2.1; IAMM Tool Question Reference: 02.02.04 (v4.0), QUES167755993843 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third parties]
[Modified in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Are there plans are in place to ensure the retention, and development, of key IRM knowledge and skills within the organisation? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M]	• Key personnel with specialist knowledge have been identified. • A clear understanding exists of the risk associated with each IA specialist role and its impact on the business. • Detailed succession (and development) planning exists. • Action is taken to ensure that specialist knowledge and training is not concentrated, but is spread between personnel and/or areas of the business. • Evidence of a co-ordinated cascading of specialist training and knowledge between the IA roles of the organisation.	IS1&2 & IS6, GPGs 6, 19 & 28.	A.8.1.1

4.3 Cultural Change [Cyber Category Type: Supporting]			
4.3.1 Required Outcome: Staff attitudes and behaviours, towards information, are monitored to ensure that these cultural aspects are aligned with the needs of the business [Links from 3.3.1 and to 5.1.1; IAMM Tool Question Reference: 02.03.04 (v4.0), QUES167755993847 (v5.0); Recipient Type: Organisation, and Delivery Partners] [Modified in GPG 40 Version 2.0]			
Areas to Probe	**Evidence Expected**	**Policy Reference**	**ISO27001 Reference**
• What evidence is available to show that staff can strike the right balance between the need to use information to further the business and the need to protect it? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M] • Is the positive trend established at Level 3, in the awareness of the importance of effective IRM to the business, by the organisation and delivery partner staff, being sustained? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: M] • What action is being taken to keep the IA message fresh and relevant to the needs of the business (e.g. in response to the communication's strategy)? [IAMM Tool Evidence Reference: 3 (v4.0); Importance: M]	• Feedback from managers and staff that a balanced approach is being adopted across the business. • Coordinated approach between IM and IA staff. • Trend information derived from the data gathering process adopted at Level 3 shows a year on year improvement, until meeting a sustainable (and appropriately reviewed) target • Details of the maintenance and reinvigoratation of the relevance of the IA message, and evidence of the effectiveness of the previous actions in this area.	IS1&2 & IS6, GPGs 6, 19 & 28.	4.2.3 4.2.4 b)

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

5.1 Cultural Change [Cyber Category Type: Supporting]			
5.1.1 Required Outcome: The need to assure the organisation's information and that of its external stakeholders as a key business asset is fully embedded within the organisational culture and is subject to a regime of continuous improvement [Links from 4.3.1; IAMM Tool Question Reference: 02.03.05 (v4.0), QUES167755993848 (v5.0); Recipient Type: Organisation, and Delivery Partners]			
Areas to Probe	**Evidence Expected**	**Policy Reference**	**ISO27001 Reference**
• Is there evidence to show that IRM is accepted to be part of normal business and that its effective application is ingrained in the culture of the organisation? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M] • What actions are taken to ensure that effective IA remains embedded within the culture of the organisation? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: M]	• Where appropriate, IRM is considered as an integral part of the standard processes within the organisation at all levels and within its Delivery Partners and 3rd party suppliers. • Evidence of engagement with other organisations to promote best practice. • Details of initiatives used to ensure that staff remain focussed on applying effective IA as a routine activity.	IS1&2 & IS6, GPGs 6, 19 & 28.	4.2.3 4.2.4 b) A.15.2.1

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 board has established its broader IA Road Map for all its information, systems and processes	**Level 5 – Optimised** Responsive IA processes are integrated as Part of Normal Business
A comprehensive information risk policy is in place. The organisation'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 ICT Systems 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 organisation's approach to addressing information risks is agreed with the organisation's external stakeholders, where applicable.	The Accreditation status of all existing ICT Systems is determined and the information risks are identified within Risk Registers for all accredited in-service ICT Systems. 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 organisation's management structure for effective decision making, within the organisation, its Delivery Partners, and with external stakeholders.	All ICT Systems that are critical to the business have been subject to Accreditation and the organisation has effective information risk management processes in place to manage the residual risks and the related, systemic IA risks.	For all ICT Systems, 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 organisation 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 organisation 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 organisation's information are kept under active review.

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

Justification Without effective IRM processes that enable the sensible aggregation of information risks being taken across the organisation, 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 organisation's business.

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

1.1 Information Risk Policy [Cyber Category Type: Peripheral]

1.1.1 Required Outcome: The organisation has clearly articulated in policy documents its approach to achieving comprehensive and effective information risk management and how compliance throughout the organisation and its delivery chains is to be achieved
[Links to 2.1.1; IAMM Tool Question Reference: 03.01.01 (v3.5/v4.0), QUES167755993849 (v5.0); Recipient Type: Organisation, Delivery Partners and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does the Department have an Information Risk Policy (including all aspects of information risk, not just security), either as a discrete document, or as part of the organisation's overall Risk Policy? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Organisational Risk Policy or discrete Information Risk Policy Statement.	IS1&2 & IS6, GPGs 6, 19 & 28.	4.2.1 4.2.4 A.15.2.1

• 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?
[IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H]
	• The Information Risk Policy must explicitly include:
	  • How the IS6 (reference [c]) measures are to be implemented in the organisation's activity and that of their Delivery Partners.
	  • How compliance with the policy is to be monitored.
	  • How its effectiveness is to be measured.
			A.6.2.1
			A.6.2.2
			A.6.2.3
			A.15.2.1

• Do the organisation's 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? [IAMM Tool Evidence Reference: Also 1 (v3.5/v4.0); Importance: H]	• Details of how the IA staff keep up to date with developing IA Guidance.		A.6.1.6 A.6.1.7
• Where a decision has been made not to apply CO guidance, is there evidence to show that a risk assessment has been undertaken?	• A valid risk assessment.		A.15.1.1 4.2.1 e)
• Have the organisation's Delivery Partners issued their own Information Risk Policies and are they aligned to the Risk Policy of the organisation? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: H]	• Details of what the organisation knows of their delivery partner's Information Risk Policy and any attempt made to ensure they are coherent with their own policy.		A.6.2
• Has the organisation provided a copy of their Information Risk Policy to their 3rd party suppliers? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: M]	• Confirmation that the 3rd party suppliers have a copy of the organisation's policy and how the detail they have is updated when changes are made.		A.10.2
• Have the 3rd party suppliers issued their own Information Risk Policies setting out how they and their supply chains will comply with the requirements of the Organisation's Policy and where applicable the minimum requirements of the SPF (reference [b]) [IAMM Tool Evidence Reference: 5 (v3.5/v4.0); Importance: H]	• Copies of the 3rd party suppliers Information Risk Policies and any attempt made to ensure they are coherent with the organisation's policy.		

1.2 Information Risk Appetite [Cyber Category Type: Supporting]

1.2.1 Required Outcome: The organisation's Statement of Information Risk Appetite is articulated in a way that is meaningful and can be used effectively by middle management to apply IA controls in a sensible and pragmatic way that enables the needs of the organisation's business and the wider needs of Government
[Links to 2.2.1; IAMM Tool Question Reference: 03.02.01 (v3.5/v4.0), QUES167755993854 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does a clear statement of the organisation's risk appetite exist? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• SIRO endorsed statement of the organisation's risk appetite.	IS1&2 & IS6, GPGs 6, 19 & 28.	4.2.1 f)
• Is this articulated in a way that enables it to be applied by the organisation's accreditors and to assist in the IRM process? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: H]	• Application of IRM processes are clearly linked to risk appetite statement.		A.8.2.2
• How is this made available to those who need to apply it?	• Details of where the organisation's Information risk appetite is detailed and how it is promulgated, particularly to the accreditation staff.		

• Does the organisation's Statement of risk appetite follow HMG best practice? • How has the organisation ensured that in setting its Information risk appetite it does not inadvertently have an adverse effect on other organisation's within government or on the delivery of pan-HMG programmes? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: L]	• Assessment of the alignment of the Information risk appetite with that of other government bodies, or any evidence that the organisation has engaged with the HMG CIO in formulating the organisation's information risk appetite statement.		A.6.1.6

1.3 Risk Assessment [Cyber Category Type: Business Critical]

1.3.1 Required Outcome: The organisation has a thorough and accurate understanding of the risk to its information, based on an up-to-date, generic threat and vulnerability assessment, and uses this to ensure that its approach to Information Risk Management throughout the organisation and its delivery chains is proportionate and is aligned to the needs of the business
[Links to 2.3.1; IAMM Tool Question Reference: 03.03.01 (v3.5/v4.0), QUES167755993858 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does the organisation have access to the generic Threat Assessment to HMG ICT systems? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M]	• Evidence of access to the Security Service Annual Threat Assessment and Threat Briefings (e.g. Technical Threat Briefing No.1 [TTB1]).	IS1&2 & IS6, GPGs 19, & 28, TTB1.	4.2.1 d) 2)
• Has the organisation undertaken the mandatory annual organisational Information risk assessment of the delivery chain, within the constraints of proportionality? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Organisational information risk report covering the entire delivery chain and an assessment of the risk policy.		4.2.1 e)
• Does the risk assessment include the effectiveness of the overarching policy and does this recognise the HMG Threat Assessment?			
• Does the risk assessment process involve the Knowledge and Information Management (KIM) function in considering risks resulting from the way information is managed? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: L]	• Evidence of reference to KIM strategy and risks		4.2.1 b)
• Is a process in place to produce an annual risk assessment of service, technology and changes in threat? [IAMM Tool Evidence Reference: Also 3 (v3.5/v4.0); Importance: L]	• Process of annual re-assessment.		4.2.3 d)

1.3.2 Required Outcome: The risk to ICT systems processing protectively marked information is assessed on an annual basis
[Links to 2.3.2; IAMM Tool Question Reference: 03.03.04 (v3.5), 03.03.05 (v4.0), QUES167755993862 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does the organisation conduct an annual technical risk assessment using HMG IA Standard No1 & 2, Information Risk Managment (reference [n]) on all ICT systems processing protectively marked information? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Details of the schedule of assessments.	IS1&2 & IS6, GPGs 19, & 28, Technical Threat Briefing No.1 (TTB1).	4.2.3 d) A.15.2.2
• Are such technical risk assessments and risk management decisions recorded in a Risk Management and Accreditation Documentation Set (RMADS), using IS1 & 2 (reference [n]) [IAMM Tool Evidence Reference: Also 1 (v3.5/v4.0); Importance: H]	• Evidence of the use of IS1&2 (reference [n])		4.3.3

1.3.3 Required Outcome: The views of external stakeholders are taken into account when managing the risk relating to shared information
[Links to 2.3.3; IAMM Tool Question Reference: 03.03.07 (v3.5), 03.03.08 (v4.0), QUES167755993865 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Have the risk assessments relating to external stakeholders, and especially those with whom the organisation will be required to share information, been agreed with them? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M]	• Evidence of agreed mitigation action. • Privacy Impact Assessments where personal data is involved.	IS1&2 & IS6, GPGs 6, 19, & 28.	4.2.1 e) A.6.2.1 A.6.2.3

1.4 Risk Management [Cyber Category Type: Business Critical]

1.4.1 Required Outcome: IA risks are captured on Risk Registers throughout the organisation and within its delivery chains, but are generally managed at a localised level
[Links to 2.4.1; IAMM Tool Question Reference: 03.04.01 (v3.5/v4.0), QUES167755993867 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Have significant information risks affecting the organisation, its Delivery Partners and 3rd party suppliers been recorded within the organisations corporate Risk Register? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: M]	• 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.	IS1&2 & IS6, GPGs 19 & 28.	4.2.1 h)
• Does the SIRO review an IA Risk Register and is there an effective methodology in place to address the risks? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: M]	• Clear governance framework, with procedures for the allocation of responsibilities and management of actions.		4.2.1 h) A.6.1.2
• Do the appropriate levels of management responsible for the delivery of IS services 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 configuration? [IAMM Tool Evidence Reference: 1 & 2 (v3.5/v4.0); Importance: 1-M, 2-H]	• Evidence to show that there is mutual agreement of the risk assessment relating to shared information.		4.2.1 h) A.6.1.2

1.5 Information Assets [Cyber Category Type: Supporting]

1.5.1 Required Outcome: The organisation has accurate details of the information it holds and who is accountable for ensuring that it is handled appropriately
[Links to 2.5.1; IAMM Tool Question Reference: 03.05.01 (v3.5/v4.0), QUES167755993872 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Are all of the Department's information assets (not just personal data) identified within an Information Asset List (inventory of assets)? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Sample Information Asset List.	IS1&2 & IS6, GPGs 19 & 28.	A.7.1.1
• Are IAOs allocated to every asset? IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: M]	• Details of the updating process.		A.7.1.2
• Is there an effective process to maintain the accuracy of the Asset List?	• 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?		A.7.1.1 4.2.1 d) 1) A.7.2.1
• Has the Department determined what personal information it and its delivery partner(s) hold in the IS6 (reference [c]) categories A & B? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H]			
• Have processes been put in place to ensure that personal information falling under the appropriate provisions of IS6 (reference [c]) are handled as at least PROTECT – PERSONAL DATA?	• Details of the process and what measures have been used to ensure compliance.		A.7.2.2 A.7.1.3

[IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: M]			

1.6 New Programmes and Related Contract [Cyber Category Type: Supporting]

1.6.1 Required Outcome: The need to incorporate effective and approved IA controls in any new acquisition of an ICT system or other system that processes information, is fully understood and processes are in place to ensure appropriate engagement with IA staff within the organisation
[Links to 2.6.1; IAMM Tool Question Reference: 03.06.01 (v3.5/v4.0), QUES167755993876 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is there a documented process for authorising the acquisition of a new information processing facility within the organisation?	• Details of the process.	IS1&2 & IS6, GPGs 6, 19, 20, 28 & 35.	A.6.1.4
• Are there credible plans and/or processes in place so that emerging new ICT requirements (including any technology that processes information i.e. a weapons system) are recognised early enough enabling a full range of information risk management processes to be applied from the outset? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M]	• 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.		4.2.3 d) A.6.1.4 A.12.1.1
• Are IRM processes and controls considered throughout the business process and not just in the initial stages? [IAMM Tool Evidence Reference: Also 1 (v3.5/v4.0); Importance: M]	• Details to show how IRM is considered in the context of existing service contracts and not just new procurements.		
• Does the organisation ensure that IA requirements are specified in ICT contracts and all new ICT contracts handling personal data have adequate clauses (e.g. building on the aspects that were outlined in what was previously available from 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, then such changes are approved personally by the SIRO? [IAMM Tool Evidence Reference: 2 & 3 (v3.5/v4.0); Importance: 2-H, 3-M]	• Details of contracts that follow the model terms. • Cases that have been made to the SIRO for changes.		A.6.2.3 A.10.2.2
• Do procurement processes (for IA measures) use HMG approved IA sources? • Where possible are newly negotiated contracts flexible enough to ensure that cost effective changes can be made to take account of changes in the IA environment? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: M]	• Measures selected from IA Directory of HMG IA Catalogue. • Contract change procedures.		A.15.1.6 A.10.2.3
• Where their use is appropriate, does the organisation ensure that Privacy Impact Assessments (PIAs) are used to assess the DPA compliance of all new policies, procedures and systems? [IAMM Tool Evidence Reference: 5 (v3.5/v4.0); Importance: H]	• Evidence of policy statement on PIA for a policy, process or IS.		4.3.1 c) A.15.2.2 A.15.1.1

1.7 Accreditation [Cyber Category Type: Supporting]

1.7.1 Required Outcome: The organisation has taken action to satisfy the SPF mandatory minimum requirement that all ICT systems handling protectively marked Government data within the organisation and within its delivery chains have effective IA controls in place so that the residual IA risks are within the risk appetite of the organisation
[Links to 2.7.1; IAMM Tool Question Reference: 03.07.01 (v3.5/v4.0), QUES167755993880 (v5.0); Recipient Type: Organisation, and Delivery Partners]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does the organisation understand the requirement for Accreditation and does it have access to Accreditation services, which meet national standards. • Are the Accreditors used by the organisation trained and proficient in the use of IS1&2 (reference [n])? Do they all meet the appropriate certification standards (e.g. the IISP specialist certification scheme, based on the IISP Skills Framework)? [IAMM Tool Evidence Reference: 2 & 3 (v3.5/v4.0); Importance: M]	• Details of how accreditation requirement is met. • Details of the Accreditation staff.	IS1&2 & IS6, GPGs 9, 13, 19, 28.	4.2.1 b) A.15.1.1 5.2.2 A.8.2.2

• Is the organisation aware of skills and competencies expected of Accreditors? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M]	• Organisations are aware of Accreditor Role Definitions detailed on Government IT Profession website and make use of them.		5.2.2 a) A.15.2.1
• What process is in place to ensure that all new ICT systems processing information requiring protection are subject to Accreditation? [IAMM Tool Evidence Reference: 6 (v3.5/v4.0); Importance: H]	• Details of how all new IS are subject to accreditation.		A.15.1.4 A.15.2.1 4.2.1 d) 4)
• Does the Organisation 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? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: M]	• Details of how Business Impact Levels are used as part of the accreditation process.		4.2.1 e) 1)
• Does the Organisation take adequate account of the affect of aggregation on determining Business Impact Levels? [IAMM Tool Evidence Reference: 5 (v3.5/v4.0); Importance: M]	• Details of where aggregation of data has been used.		4.2.1 d) 4) 4.2.1 e) 1)
• What plans exists to comply with the SPF (reference [b]) Mandatory Requirement that all ICT systems handling protectively marked information are accredited (including legacy) and for every such system to be re-accredited when they undergo significant change, and to have an agreed statement of when the system should be re-accredited? [IAMM Tool Evidence Reference: 7 (v3.5/v4.0); Importance: H]	• Plan to establish accreditation status of all ICT systems handling protectively marked information and to comply with SPF (reference [b]) Mandatory Requirements.		4.2.2 4.2.3
• 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 Organisation satisfying this requirement? [IAMM Tool Evidence Reference: Also 7 (v3.5/v4.0); Importance: H]	• Details of how annual reviews are undertaken.		A.15.2.1
• Do the Department and its Agencies have the ability to regularly audit information assets and ICT systems?	• Details of any audits carried out on information assets and ICT systems.		A.6.1.8 A.15.3.1 6
• Are regular compliance checks carried out by the Accreditor, ITSO or similarly qualified person? [IAMM Tool Evidence Reference: 8 (v3.5/v4.0); Importance: M]	• Details of any formal compliance checks undertaken.		A.6.1.8 5.2.2 b) 4.3.1 e)
• Are the results of these checks documented in the RMADS audit of the ICT system against configuration records? [IAMM Tool Evidence Reference: 9 (v3.5/v4.0); Importance: L]	• RMADS audit of the ICT system against configuration records.		

LEVEL 2 – Established - IA Processes are Institutionalised

2.1 Information Risk Policy [Cyber Category Type: Peripheral]

2.1.1 Required Outcome: The organisation's Information Risk Policy is subject to regular review to ensure that it is aligned to the needs of the business
[Links from 1.1.1 and to 3.1.1; IAMM Tool Question Reference: 03.01.02 (v3.5/v4.0), QUES167755993850 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Has the Information Risk Policy been subject to review in the last 12 months to ensure that it takes account of changes in the IA environment and that it is matched to the developing nature of the organisation's business? [IAMM Tool Evidence Reference: 1 & 2 (v3.5/v4.0); Importance: 1-H, 2-M]	• Details of the review process and its effective implementation.	IS1&2 & IS6, GPGs 19 & 28.	4.2.3

2.2 Information Risk Appetite [Cyber Category Type: Supporting]

2.2.1 Required Outcome: The organisation's Statement of Information Risk Appetite is subject to regular review to ensure that it is aligned to the needs of the business
[Links from 1.2.1 and to 3.2.1; IAMM Tool Question Reference: 03.02.02 (v3.5/v4.0), QUES167755993855 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Has the Statement of Information Risk Appetite been subject to review in the last 12 months to ensure that it takes account of changes in the IA environment and that it is matched to the developing nature of the organisation's business? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Details of the review process and its effective implementation.	IS1&2 & IS6, GPGs 19 & 28.	4.2.3

2.3 Risk Assessment [Cyber Category Type: Business Critical]

2.3.1 Required Outcome: To ensure that the annual risk assessment is comprehensive and is better matched to the specific business of the organisation and it is based on a tailored threat assessment
[Links from 1.3.1 and to 3.3.1; IAMM Tool Question Reference: 03.03.02 (v3.5/v4.0), QUES167755993859 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Has the organisation an up to date Threat Assessment specific to their business? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M]	• A tailored Threat Assessment specific to the organisation's business activity (i.e. not just the Security Service annual Threat Assessment and Technical Threat Briefing No. 1 ([TTB1])	IS1&2 & IS6, GPGs 19, & 28 & TTB1.	4.2.1 d) 2)
• Has the organisation engaged with external authorities such as CPNI, CESG and SOCA in the construction of this Assessment? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M]	• Evidence of effective engagement such as Threat Workshops.		A.6.1.6 A.6.1.7
• Does the annual organisation's Information Risk Assessment recognise this specific Threat Assessment?	• There is clear documentary evidence that there is direct linkage between the Risk Assessment and the Threat Assessment.		4.2.1 d) 3)

2.3.2 Required Outcome: Whenever there is a significant change in a risk component (threat, vulnerability, impact etc.) a technical risk assessment is initiated for the relevant IS
[Links from 1.3.2 and to 3.3.2; IAMM Tool Question Reference: 03.03.05 (v3.5), 03.03.06 (v4.0), QUES167755993863 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• 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? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M]	• Details of Assessments that have been undertaken in response to a change in a risk component.	IS1&2 & IS6, GPGs 19, & 28, & TTB1	4.2.3 d)

2.3.3 Required Outcome: A collaborative approach is taken to managing risk relating to shared information
[Links from 1.3.3; IAMM Tool Question Reference: 03.03.08 (v3.5), 03.03.09 (v4.0), QUES167755993866 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Are effective bi-lateral and multi-lateral arrangements in place to manage IA risks which relate to external stakeholders? [IAMM Tool Evidence Reference: 1 & 2 (v3.5/v4.0); Importance: M]	• Evidence to show that the views and opinions of external stakeholders are taken into account when managing Departmental level IA risks.	IS1&2 & IS6, GPGs 6, 19, 28.	A.6.2.1 A.6.2.2 A.6.2.3

2.4 Risk Management [Cyber Category Type: Business Critical]

2.4.1 Required Outcome: Significant IA risks are escalated within the organisation and its delivery chains so that they are owned and managed at a level appropriate to their potential impact on the business of the organisation
[Links from 1.4.1 and to 3.4.1; IAMM Tool Question Reference: 03.04.02 (v3.5/v4.0), QUES167755993868 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Do the escalated IA risks have risks owners and managers allocated and are they appropriate to the significance of the risk being considered? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H] • Is the Department's IA risk governance structure merely a reporting mechanism, or does it take effective action? • Is the SIRO aware of the residual risks that have been accepted and 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? • 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? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M]	• 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. • Endorsement of the residual risks. • Details of the process. • Documentary evidence to show the process that should be followed, together with evidence that the process works (i.e. transfer of risk to the organisation from its delivery chain)	IS1&2 & IS6, GPGs 6, 19, 28.	4.2.2 a) 7 & 8 4.2.2 b) 4.2.1 h) 4.2.3 c) 4.2.2 c) 4.2.1 h)

2.5 Information Assets [Cyber Category Type: Supporting]

2.5.1 Required Outcome: IAOs understand the risk to their information assets arising from how they are stored, moved and used. They also know which information assets they must retain to meet the organisation's statutory obligations and its business needs
[Links from 1.1.1 and to 2.7.1; IAMM Tool Question Reference: 03.05.02 (v3.5/v4.0), QUES167755993873 (v5.0); Recipient Type: Organisation]
[Modified in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Do the IAOs know where all of its information assets are located, both logically and physically? [IAMM Tool Evidence Reference: 3 (v4.0); Importance: M] • Do the IAOs understand how and when their information is carried by the ICT infrastructure and to where? [IAMM Tool Evidence Reference: 4 (v4.0); Importance: M] • Does the Information Asset List, in accordance with the organisation's Plan to address Digital Continuity, include details of the retention requirements based on its statutory obligations under the Public Records Act and the business value of the information? [IAMM Tool Evidence Reference: 1 & 2 (v3.5/v4.0); Importance: M]	• IAO engagement with the ICT and IA communities to understand the risks associated with the storage, movement and processing of their information assets. • Information lifecycle maps • Accurate register of information assets and owners, and retention schedules based on business value, with procedures for implementation.	IS1&2 & IS6, GPGs 6, 9, 19, 28.	4.2.1 d) 4.2.1 d) 4) A.7.1.1

2.6 New Programmes and Related Contracts [Cyber Category Type: Supporting]

2.6.1 Required Outcome: The organisation has confidence that proposals from 3rd party suppliers for new ICT systems or other systems that process information are aligned to the organisation's security architecture and incorporate effective IA controls. IA considerations are factored in to all modifications to existing ICT systems [Links from 1.6.1 and to 3.6.1; IAMM Tool Question Reference: 03.06.02 (v3.5/v4.0), QUES167755993877 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is there evidence that the process for authorising the acquisition of a new information processing facility within the organisation is used effectively? • How is the organisation preparing for any change in business procedures which are consequent on the deployment of new ICT programmes? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: H] • To what extent does the organisation rely on 3rd party suppliers to design the information security features of new programmes (including any technological programme that involves the processing of information i.e. in a weapons system)? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M] • How does the organisation assess the quality of the information security design of new programmes? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M] • How does it ensure that such designs are aligned to the organisation's enterprise security architecture? [IAMM Tool Evidence Reference: Also 3 (v3.5/v4.0); Importance: M] • How are contract risks as they relate to IA managed?	• 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. • Where the organisation 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 CESG. • Evidence of effective engagement of the IA staff with the programme staff to ensure effective management of IA risks. • IA clauses in the contracts.	IS1&2 & IS6, GPGs 6, 19, 20, 28, 30 & 35.	A.6.1.4 4.2.3 a) 3) 4.2.3 d) 3) 5.2.2 a) A.10.2 5.2.2 a) 4.2.1 g) A.6.1.7 A.6.1.6 A.6.2.3

2.7 Accreditation [Cyber Category Type: Supporting]

2.7.1 Required Outcome: The organisation has a programme of work in place to satisfy the SPF (reference [b]) mandatory minimum requirement that all ICT systems handling protectively marked Government data within the organisation; and within its delivery chains are accredited and that such accreditation is subject to annual review [Links from 1.7.1 and to 3.7.1; IAMM Tool Question Reference: 03.07.02 (v3.5/v4.0), QUES167755993881 (v5.0); Recipient Type: Organisation, and Delivery Partners]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does the SIRO know which of the Department's IS and key information assets are business critical? • Does the Department have a centralised record of the Accreditation status of the Department's IS? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H] • Has the list of un-accredited IS been prioritised in terms of business risk and is a programme of work in place to accredit these systems? [IAMM Tool Evidence Reference: Also 2 and 3 (v3.5/v4.0); Importance: H] • Are Accreditors assessed against the standards recommended in the Accreditor Role Definitions and is the work assigned to them consistent with their competency and skill levels? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H] • Does a systematic process of accreditation and re-accreditation exist? • 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?	• Criteria for establishing business criticality and a definitive list of business critical systems and key information assets exist. • Details of the records • Prioritised list endorsed by the SIRO. • Details of the accreditor assessments made against the skill and competency levels recommended in the Accreditor Role Definitions. • Accreditor work portfolios reflect their competency and skill levels Details of the process. • Details of how accreditation is maintained through-life.	IS1&2 & IS6, GPGs 6, 9, 13, 19, 20, 28 & 35.	A.7.1.1 4.2.1 d) 4.3.3 4.2.1 f) 5.2.2 c) 5.2.2 a) 4.2.3

[IAMM Tool Evidence Reference: 5 & 6 (v3.5/v4.0); Importance:5- L, 6-H] • 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? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: L]	• Evidence to show that the organisation does not just accept the status quo when it has the potential to impact on its business, but takes action to affect change.		A.15.1.6 4.2.1 e) 4)

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

3.1 Information Risk Policy [Cyber Category Type: Peripheral]

3.1.1 Required Outcome: The organisation's Information Risk Policy is mature enough to cater for a tailored approach to IRM which is matched to the business criticality of the information assets and their supporting infrastructure
[Links from 2.1.1 and to 4.1.1; IAMM Tool Question Reference: 03.01.03 (v4.0), QUES167755993851 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does the business apply a one size fits all approach to IRM, or do they tailor their approach depending on the business criticality of the information and the supporting infrastructure? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M] • If the business adopts a flexible approach to IRM matched to the business risk, how is this communicated to those who have to apply the policy, such as middle managers in the organisation, 3rd party suppliers and especially Accreditors? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: M]	• In the application of the Information Risk Policy it is clear that the willingness of the business to tolerate risk is a function of business criticality. • The policy provides clear guidelines which establish where more leeway can be applied by staff, such as Accreditors, when making risk management decisions.	IS1&2 & IS6, GPGs 19 & 28.	4.2.1 e)

3.2 Information Risk Appetite [Cyber Category Type: Supporting]

3.2.1 Required Outcome: Application of the organisation's Information Risk Appetite is tailored to the needs of the business in line with the maturing Information Risk Policy
[Links from 2.2.1 and to 4.2.1; IAMM Tool Question Reference: 03.02.03 (v4.0), QUES167755993856 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does the Statement of Risk Appetite include effective guidance on the circumstances under which a risk that exceeds the risk appetite must be escalated to senior management? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M] • Rather than slavishly enacting controls to reduce the residual risk to below the organisation's stated risk appetite, are appropriate risk balance cases escalated for senior management decision? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: M]	• Clear guidance is provided in the Statement of Information Risk Appetite to guide those who have to apply it on its sensible and pragmatic application. • Business cases supporting risk decisions that exceed the organisation's risk appetite, with evidence to show how and why the management decision was made.	IS1&2 & IS6, GPGs 19 & 28.	4.2.3

3.3 Risk Assessment [Cyber Category Type: Business Critical]

3.3.1 Required Outcome: Critical parts of the business and the processes that underpin them are subject to discrete risk assessments based on tailored threat assessments
[Links from 2.3.1 and to 4.3.1; IAMM Tool Question Reference: 03.03.03 (v3.5/v4.0), QUES167755993860 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• In addition to the generic Threat Assessment for the organisation have Threat Assessments been developed for critical parts of the business? • Have these tailored Threat Assessments been used to conduct Information Risk Assessments for critical areas of the business, particularly when a new threat or vulnerability is detected? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Tailored Threat Assessments and related Risk Assessments exist for specific ICT systems that service critical business functions and this is evidenced in IS1&2 (reference [n]) calculations.	IS1&2 & IS6, GPGs 19, 28 & 35, Technical Threat Briefing No.1 (TTB1).	4.2.1 d) 2) 4.2.3 d)

3.3.2 Required Outcome: A systematic process is in place to subject business critical IS, their related business policies and processes and key information assets to operational and technical risk reviews
[Links from 2.3.2; IAMM Tool Question Reference: 03.03.06 (v3.5), 03.03.07 (v4.0), QUES167755993864 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is a systematic process in place within the organisation, its Delivery Partners and within its 3rd party suppliers so that regular operational and technical risk reviews are conducted of **business critical IS,** their related business policies and processes, and key information assets? [IAMM Tool Evidence Reference: 1 & 2 (v3.5/v4.0); Importance: 1-H, 2-H] • Are the requirements for remedial action satisfied in a timely manner? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: M]	• Schedule of reviews and action plans to conduct remedial work. • Threat assessments for business critical key information assets.	IS1&2 & IS6, GPGs 19 & 28, Technical Threat Briefing No.1 (TTB1).	4.2.1 4.2.3 d)

3.4 Risk Management [Cyber Category Type: Business Critical]

3.4.1 Required Outcome: A consolidated view of the tolerated IA risks across the business critical IS and information assets, together with the systemic IA risks that could impact on business critical processes have been created. This is used to take effective and timely action to mitigate such risks, should conditions change that cause the risks to be in excess of the organisation's stated Information Risk Appetite
[Links from 2.4.1 and to 4.4.1; IAMM Tool Question Reference: 03.04.03 (v3.5/v4.0), QUES167755993869 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Are the significant IA risks managed at a level appropriate to their impact to the business critical systems? • Is the SIRO is aware of the residual risks that have been accepted and is the SIRO satisfied that these are within the risk appetite of the business as articulated in the Statement of Information Risk Appetite? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M]	• Evidence to show that the significant IA risks to business critical systems are escalated to the SIRO. • Documentation exists to show that the residual risks have been accepted as being within the risk appetite.	IS1&2 & IS6, GPGs 9, 17, 19, 28 & 35.	4.2.1 i)
• Where the decision has been taken to tolerate particular risks, is there a process is in place to monitor changes which would require the decision to be re-examined? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H]	• Evidence of the process to monitor changes appropriately (so that where appropriate, the risks may be actively managed, rather than tolerated by default).		
• Are processes in place for capturing the systemic IA risks facing the organisation (e.g. those relating to network vulnerabilities) and for assessing the overall effect on the delivery of the organisation's business critical outputs? [IAMM Tool Evidence Reference: 3 & 4 (v3.5/v4.0); Importance: 3-M, 4-H]	• 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 organisation's business critical outputs.		4.2.3 b)
• Is the Management Board made aware of the key IA risks affecting business critical systems and information assets, together with the systemic IA risks that impact on the delivery of the organisation's outputs?	• Main Board papers showing submission of data and subsequent actions being taken		7 4.2.1 i)

[IAMM Tool Evidence Reference: 5 (v3.5/v4.0); Importance: M]			

3.5 Information Assets [Cyber Category Type: Supporting]

3.5.1 Required Outcome: IAOs know which of their information assets are business critical, where they are located and which parts of the infrastructure are key to maintain their availability for the business
[Links from 2.5.1 and to 4.5.1; IAMM Tool Question Reference: 03.05.03 (v4.0), QUES167755993874 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does an effective dialogue exist between IAOs and the owners of the ICT infrastructure so that business critical information assets are managed in a way that supports the business of the organisation? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M]	• Joint meetings that show clear engagement and understanding from both parties.	IS1&2 & IS6, GPGs 6, 9, 19 & 28.	4.2.1 d)
• Have potential single points of failure within the infrastructure been identified and work commissioned to reduce the potential business impact? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: M]	• Business orientated analysis of the infrastructure and any resulting work plans.		4.2.1 d) 4) A.14.1
• Are IAOs who are responsible for business critical information assets content that any remediation of single points of failure are being addressed in a way, and at a pace, that is matched to their importance to the business? [IAMM Tool Evidence Reference: 3 (v4.0); Importance: M]	• Clear evidence that the business understands and supports any work plans to improve the resilience of the infrastructure.		

3.6 New Programmes and Related Contracts [Cyber Category Type: Supporting]

3.6.1 Required Outcome: New ICT systems that process business critical information assets conform to the organisation's security architecture and incorporate effective IA controls before they go live
[Links from 2.6.1 and to 4.6.1; IAMM Tool Question Reference: 03.06.03 (v4.0), QUES167755993878 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• What has the organisation done to confirm the quality of the design of any new ICT system or any technological programme (i.e. in a weapons system) that involves the processing of business critical information? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M]	• Clear evidence that they have sought external verification of the design from bodies such as CESG.	IS1&2 & IS6, GPGs 6, 19, 20, 28, 30 & 35.	A.6.1.7 A.6.1.6 A.6.1.4
• Has the Enterprise Security Architecture Board (or similar body) endorsed the design as conforming to the enterprise security architecture? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M]	• Minutes of the Enterprise Security Architecture Board, or similar body.		4.2.3 a) 3)
• How does the organisation confirm that the security controls are effective before authorising that the ICT system goes live? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M]	• Details of the process employed.		A.10.2 4.2.1 g)

3.7 Accreditation [Cyber Category Type: Supporting]

3.7.1 Required Outcome: All of the ICT systems that are involved in business critical aspects of the business are accredited by proficient Accreditors
[Links from 2.7.1 and to 4.7.1; IAMM Tool Question Reference: 03.07.03 (v4.0), QUES167755993882 (v5.0); Recipient Type: Organisation, and Delivery Partners]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• 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? [IAMM Tool Evidence Reference: 2 & 3 (v3.5/v4.0); Importance: 2-H, 3-M]	• 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.	IS1&2 & IS6, GPGs 6, 9, 13, 19, 20, 28 & 35.	4.2.1 g)
• Are there sufficient qualified and trained Accreditors to manage the workload?	• Details of the accreditation work-oad		5.2.2 c) A.8.2.2

[IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M]	• Details of the Accreditor assessments made against the skill and competency levels recommended in the Accreditor Role Definitions.		

LEVEL 4 – Quantitatively Managed –
The board has established its broader IA Road Map for all its information, systems and processes

4.1 Information Risk Policy [Cyber Category Type: Peripheral]

4.1.1 Required Outcome: The Information Risk and other relevant policies (e.g. KIM, HR and procurement) are fully aligned and consistent
[Links from 3.1.1 and to 5.1.1; IAMM Tool Question Reference: 03.01.04 (v4.0), QUES167755993852 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties][Modified in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• What has the organisation done to ensure alignment between the Information Risk Policy and other corporate policies so that there is a consistency in approach? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M]	• Details of any successful alignment activity undertaken (and completed) and details of exceptions and their remediation.	IS1&2 & IS6, GPGs 19 & 28.	4.2.1

4.2 Information Risk Appetite [Cyber Category Type: Supporting]

4.2.1 Required Outcome: A balanced approach, in terms of corporate drivers to risk appetite, shows evidence of consideration and alignment
[Links from 3.2.1; IAMM Tool Question Reference: 03.02.04 (v4.0), QUES167755993857 (v5.0); Recipient Type: Organisation][Modified in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Has a review been undertaken of the effect that applying a tailored approach to information risk appetite, which was introduced at Level 3, has had on the conduct of business? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M] • Has the Main Board engaged on this matter and provided direction? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: M] • Has the Statement of Information Risk Appetite been adjusted accordingly to provide better guidance to those who have to apply it? [IAMM Tool Evidence Reference: 3 (v4.0); Importance: M]	• Details of the Review (e.g. producing evidence of a methodology, and its consistent application across corporate driver considerations). • Main Board minutes. • Revised Information Risk Appetite Statement.	IS1&2 & IS6, GPGs 19 & 28.	7.2 5.1 h) 7.3 c) 6)

4.3 Risk Assessment [Cyber Category Type: Business Critical]

4.3.1 Required Outcome: Discrete risk assessments, based on tailored assessments, are conducted for all appropriate ICT systems
[Links from 3.3.1; IAMM Tool Question Reference: 03.03.04 (v4.0), QUES167755993861 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]
[Modified in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is a systematic process in place to conduct operational and technical risk reviews of **all appropriate ICT systems** and their related business policies and processes? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M]	• Schedule of reviews and action plans to conduct remedial work. • Details of the application of a broader systematic methodology (that incorporates an element to help identify the "appropriate" ICT systems), which includes appropriate tailored threat assessments.	IS1&2 & IS6, GPGs 19, 28 & 35, Technical Threat Briefing No.1 (TTB1).	4.2.1 4.2.3 d)

4.4 Risk Management [Cyber Category Type: Business Critical]

4.4.1 Required Outcome: The board has accepted the aggregated information risk that it carries, and the way that it is managed
[Links from 3.4.1 and to 5.2.1; IAMM Tool Question Reference: 03.04.04 (v4.0), QUES167755993870 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties][Modified in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Has the regime set up to manage the Information risk to business critical ICT systems been extended to embrace all systems and information assets? Is there an effective process in place to aggregate the individual ICT system Information risks to produce a corporate Information risk picture of the residual risks that have been accepted? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M]	• 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 ICT systems.	IS1&2 & IS6, GPGs 9, 17, 19, 28 & 35.	4.2.1 i) 4.2.3 b) 4.2.1 d) 3)
• Are key vulnerabilities that are common to more than one ICT system captured with a view to assessing the overall impact to the organisation if that vulnerability were to be exploited? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: M]	• Details of the process and its effective use.		4.2.1
• 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? [IAMM Tool Evidence Reference: 3 (v4.0); Importance: M]	• Details of the process and its effective use.		7.1 4.2.1
• Is the Management Board made aware of, and accept, the key, and aggregated, IA risks affecting all systems, together with the systemic IA risks that impact on the delivery of the organisation's outputs? [IAMM Tool Evidence Reference: 4 (v4.0); Importance: H]	• Main Board papers showing submission of data. • Main Board acceptance of the key and aggregated information risk, and details of subsequent actions being taken.		
• What is being done to integrate Information Risk into general business risk, so that it is not seen as a discrete specialised activity, but one that is a mainstream corporate activity? [IAMM Tool Evidence Reference: 5 (v4.0); Importance: M]	• Evidence shows that business risks have, as an integral part, coverage of the related information risks.		

4.5 Information Assets [Cyber Category Type: Supporting]

4.5.1 Required Outcome: IAO's fully understand the risk exposure of their assets and the potential impact on the business
[Links from 3.5.1; IAMM Tool Question Reference: 03.05.04 (v4.0), QUES167755993875 (v5.0); Recipient Type: Organisation][Modified in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Do the IAOs know which of their information assets in storage, transport or processing are subject to risks that the organisation has decided to tolerate rather than deal with? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M]	• Evidence of full engagement of the IAOs with those responsible for the ICT infrastructure so they understand the impacts.	IS1&2 & IS6, GPGs 6, 9, 19 & 28.	4.2.1 d)
• Is there a mentoring network for the IAO's (e.g. mentoring of less experienced IAO's by more experience IAO's)? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: M]	• Evidence of knowledge sharing between IAOs, i.e. between the experienced IAO's responsible for critical assets to the other IAO's (e.g. related to risks tolerated on their assets, and the underlying justification).		
• What evidence is there that the IAOs have taken account of the effect of aggregation of information assets on the risk profile of their assets? • [IAMM Tool Evidence Reference: 3 (v4.0); Importance: M]	• Risk assessments that take account of aggregation.		

4.6 New Programmes and Related Contracts [Cyber Category Type: Supporting]

4.6.1 Required Outcome: Effective governance has been independently validated for all contracts, or agreements, such that their IRM impact has been addressed before any agreement is made
[Links from 3.6.1; IAMM Tool Question Reference: 03.06.04 (v4.0), QUES167755993879 (v5.0); Recipient Type: Organisation][Modified in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Are their effective governance processes in place to ensure that the IRM impact of any contract, MOU, SLA or any other form of agreement is properly assessed before the agreement is signed? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M] • Have all shared service agreements been subject to this process? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: M] • Are the resultant risks associated with the shared service agreement being properly managed? [IAMM Tool Evidence Reference: 3 (v4.0); Importance: M] • Where 3rd party service providers, or Delivery Partners, are involved, are the risks properly identified and being managed? [IAMM Tool Evidence Reference: 4 (v4.0); Importance: M]	• Details of the process (including a SIRO supported independent review) and any assessment of its effectiveness, and follow-up actions. • All the responsibilities of all the appropriate roles are clearly defined, e.g. for shared-services, the lead organisation (or lead provider) responsibilities are clearly defined. • Details of the evidence of the SIRO's involvement in, and support for, the use of the process for shared service agreements. • Details of the IRM reviews for shared services being sent to the SIRO, with support for remedial action, where appropriate. • Details of the risk management process applied to 3rd party service providers Delivery Partners (e.g. outsourced ICT arrangements), and the reports on it its effectiveness and remedial actions taken.	IS1&2 & IS6, GPGs 6, 19, 20, 28, 30 & 35.	A.6.2 A.10.2

4.7 Accreditation [Cyber Category Type: Supporting]

4.7.1 Required Outcome: The organisation has full and accurate details of the extent of the aggregated information risk it faces
[Links from 3.7.1; IAMM Tool Question Reference: 03.07.04 (v4.0), QUES167755993883 (v5.0); Recipient Type: Organisation, and Delivery Partners]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does the organisation understand the accreditation status of all ICT systems? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M] • Are accurate details available of where accreditation, or planned re-accreditation not taken place? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: M] • Have these details been made available to the SIRO? [IAMM Tool Evidence Reference: 3 (v4.0); Importance: H] • Have all of the significant, through-life (from concept to disposal) Information Risks been captured? [IAMM Tool Evidence Reference: 4 (v4.0); Importance: M] • As a result, does the organisation understand the nature and extent of the aggregated Information Risk? [IAMM Tool Evidence Reference: 5 (v4.0); Importance: M] • In particular, are Accreditors alert to cases where an IA weakness in a non-business critical system could undermine the Integrity, Availability or Confidentiality of a business critical system? [IAMM Tool Evidence Reference: 6 (v4.0); Importance: H]	• Details of the accreditation status of all ICT systems. • Accreditation and re-accreditation plan and whether it is up to date. • Report to the SIRO and details of his consequent actions. • Evidence to show that all significant Information Risks are captured, particularly those relating to an in-service system. • Information to show that the organisation is aware of the aggregated risk and its effect, or potential effect, on the business. • Evidence to show that Accreditors do not consider ICT systems in isolation, but are alert to how systems and hence risks interrelate. • Knowledge sharing between Accreditors where possible to learn from issues arising from other cases.	IS1&2 & IS6, GPGs 6, 9, 13, 19, 20, 28 & 35.	4.2.1 d) 4.2.1 h) 4.2.1 e)

LEVEL 5 – Optimised - Responsive IA processes are integrated as part of normal business

5.1 Information Risk Policy [Cyber Category Type: Peripheral]

5.1.1 Required Outcome: Information Risk Policy is an integral part of overall corporate policy and is used to inform the organisation's business strategy
[Links from 4.1.1; IAMM Tool Question Reference: 03.01.05 (v4.0), QUES167755993853 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• How integrated into corporate decision making is the consideration of the need to manage information risk? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M]	• Normal business planning activity takes due account of the business need to ensure effective information risk management.	IS1&2 & IS6 GPGs 19 & 28.	7.3 c)

5.2 Risk Management [Cyber Category Type: Business Critical]

5.2.1 Required Outcome: The organisation carries the optimum information risk exposure
[Links from 4.4.1; IAMM Tool Question Reference: 03.04.05 (v4.0), QUES167755993871 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is the Main Board regularly presented with an accurate picture of the Information Risk exposure of the organisation? • Does the Main Board regularly review the Information Risk exposure and risk appetite of the organisation? • Are the organisation's external stakeholders and particularly those with whom it shares information, content with the IA risk exposure of the organisation?	• Main Board papers and Annual Report on the organisation. • Evidence that decisions have been made based on expert guidance. • Internal and external audit reports and other assessments. • Main Board papers. • Main Board papers.	IS1&2 & IS6, GPGs 9, 17, 19, 28 & 35.	4.2.3 7.1 4.2.3 7.1 A.6.2.2

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 board has established its broader IA Road Map for all its information, systems and processes	**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 organisation has a Forensic Readiness Policy.	The status of the through-life IA measures employed across the organisation 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 organisation'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.	Where there is a business justification, Level 3 processes are extended to embrace all of the organisation'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 organisation 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

1.1 General Measures [Cyber Category Type: Business Critical]
1.1.1 Required Outcome: Although IA controls are in place to protect protectively marked information, the organisation does not have a coordinated view of the breadth, depth or efficacy of these controls. To redress this situation realistic plans have been made to determine the status of all IA controls [Links to 2.1.1; IAMM Tool Question Reference: 04.01.01 (v3.5/v4.0), QUES167755993884 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Are strong and effective arrangements in place to safeguard unencrypted personal information collected, held, processed or transferred within the organisation, its Delivery Partners and its 3rd party suppliers? [IAMM Tool Evidence Reference: 5 (v3.5/v4.0); Importance: H]	• Details of the process by which unencrypted personal information is subject to strong safeguards.	IS1&2, IS4 & IS6, GPGs 6, 17, 19 & 28.	A.7.2.2 A.10.7.3 A.15.1.4
• Where applicable, does the organisation comply with HMG IA Standard No.4 – Management of Cryptographic Systems (e.g. supplement 13) for the protection of protectively marked material? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Details of measures employed by the ComSO.		A.12.3.1
• 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? [IAMM Tool Evidence Reference: 2 & 3 (v3.5/v4.0); Importance: H]	• Details of any decision making relating to the use of cryptographic protection.		A.15.1.6
• Where applicable, are the cryptographic key management arrangements satisfactory and do they meet the needs of the business?	• Details of the key management arrangements.		A.12.3.2
• Where applicable, is the requirement for specified levels of personnel security clearance for individuals handling cryptographic items understood by the organisation and is it complied with? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: H]	• Vetting details.		A.8.1.2
• Does the organisation have plans to determine the status of the IA control measures in use on all existing IS? [IAMM Tool Evidence Reference: Also 1 (v3.5/v4.0); Importance: H]	• Details of the plans.		4.2.3 c)

1.1.2 Required Outcome: Realistic plans are in place to implement through-life IA controls in a co-ordinated way across the organisation and its delivery chain
[Links to 2.1.2; IAMM Tool Question Reference: 04.01.03 (v3.5), 04.01.05 (v4.0), QUES167755993888 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does the organisation understand the need to take a coordinated and systematic approach to IA measures throughout the delivery chain for both information assets and the related ICT systems through their whole life? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Evidence to show that IRM is not just considered from the technical standpoint and there is coordination with the staff responsible for the organisation's KIM function • Plans to show that a coordinated view is being taken to establish and maintain effective through-life IA control measures.	IS1&2 & IS6, GPGs 6, 19, 20, 28 & 35.	4.2.1 a) 4.2.1 b) 4.2.1 c) 4.2.2 d) 4.2.3 d)
• Do plans exist to determine the ongoing status of the IA measures?	• Analysis of the current through life measures.		4.2.1
• At the ICT level, what evidence is there to suggest that the organisation is implementing through-life IA measures in a co-ordinated way, rather than on a system-by-system basis? [IAMM Tool Evidence Reference: Also 1 (v3.5/v4.0); Importance: H]	• Taking a coordinated approach. • Implementing cross-cutting measures that impact on more than one system.		4.2.2 4.2.3
• Does the organisation make best use of the knowledge and experience of its commercial partners drawing on their internal best practice? [IAMM Tool Evidence Reference: Also 1 (v3.5/v4.0); Importance: L]	• Details of engaging with commercial Delivery Partners to implement best practice.		A.6.1.7

1.2 Physical & Environmental Security Measures [Cyber Category Type: Peripheral]			
1.2.1 Required Outcome: The organisation has implemented adequate physical security measures to protect its information in whatever form it exists throughout its delivery chain and these measures have been tested [Links to 2.2.1; IAMM Tool Question Reference: 04.02.01 (v3.5/v4.0), QUES167755993891 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]			
Areas to Probe	**Evidence Expected**	**Policy Reference**	**ISO27001 Reference**
• Are physical protection measures and access controls to sites, buildings and equipment rooms adequate to protect the information contained irrespective of whether these facilities belong to the organisation, its Delivery Partners or to its 3rd party suppliers? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Details of physical protection measures employed.	IS1&2 & IS6, GPGs 6, 14, 19, 20 & 28.	A.9.1 A.9.2
• In particular, are adequate physical security measures in place to safeguard PROTECT level information held in both paper and electronic form? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H]			
• Does the organisation follow the specific Government procedures to manage the risk posed by eavesdropping and electro-magnetic emanations (where the impact warrants the implementation of such measures)? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: M]	• Details of the number of trained individuals available, the procedures used and when last they were employed.		A.15.1.1
• Are arrangements in place to test and validate these measures? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: M]	• Details of how these arrangements are validated.		
1.3 Personnel Security Measures [Cyber Category Type: Peripheral]			
1.3.1 Required Outcome: The organisation makes use of an effective security checking and/or vetting process that is appropriate to the needs of the business and applies this before access is given to the organisation's information. When any staff move within, or leave the organisation, their access rights to information or assets are removed [Links to 2.3.1; IAMM Tool Question Reference: 04.03.01 (v3.5/v4.0), QUES167755993893 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]			
Areas to Probe	**Evidence Expected**	**Policy Reference**	**ISO27001 Reference**
• Does the organisation apply a security checking and/or vetting process to its own staff and to the staff of Delivery Partners and 3rd party suppliers, before they are given access to sensitive information? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H]	• Details of the security checking and vetting process, to include lead times and backlog.	IS1&2, & IS6, GPGs 6, 19 & 28.	A.8.1.2
• Is the vetting process rigorous enough to meet the business need? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: M]	• Details of how staff are employed before their vetting comes through.		A.8.1.2
• 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? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: H]	• Details of the process used to ensure all such uses are of the appropriate vetting status.		A.8.1.2
• Are members of the organisation, 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? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M]	• Details of the process and any results of assessments as to whether it is sufficient to meet the needs of the business.		A.6.1.5 A.8.1.3
• Is there a process in place to ensure that all employees, contractors and 3rd party users of the organisation's information surrender all of the organisation's information assets in their possession upon the termination of their employment, contract, or	• Details of the process and any results of assessments as to whether it is sufficient to meet the needs of the business.		A.8.3.1 A.8.3.2

agreement? [IAMM Tool Evidence Reference: 5 (v3.5/v4.0); Importance: M] • Are the access rights of all employees, contractors and 3rd party users, to the organisation's information and information processing facilities removed upon the termination of their employment, contract, or agreement? [IAMM Tool Evidence Reference: Also 5 (v3.5/v4.0); Importance: M]	• Details of the process and any results of assessments as to whether it is sufficient to meet the needs of the business.		A.8.3.3

1.4 Acceptable Use Policy [Cyber Category Type: Supporting]

1.4.1 Required Outcome: The organisation has assurance that staff within the organisation, its Delivery Partners and in 3rd party suppliers who have access to the organisation's ICT systems, only use them for authorised purposes
[Links to 2.3.1; IAMM Tool Question Reference: 04.04.01 (v3.5/v4.0), QUES167755993895 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is there an effective Acceptable Use Policy in use within the organisation, its Delivery Partners and within its 3rd party suppliers? [IAMM Tool Evidence Reference: 1, 2, 3 & 4 (v3.5/v4.0); Importance: 1-H, 2 to 4-M]	• Policy exists with effective sanctions and a method exists to assess compliance with policy. Evidence that users are informed of the policy.	IS1&2, & IS6, GPGs 6, 13, 19, 20 & 28.	A.7.1.3 A.15.1.5

1.5 Remote Working, Portable Devices and Removable Media [Cyber Category Type: Business Critical]

1.5.1 Required Outcome: An SPF compliant policy is in place covering remote working within the organisation, its Delivery Partners and within its 3rd party suppliers. The Policy is based on effective control measures which are designed to reduce the risk to the organisation's information to an acceptable level
[Links to 2.5.1; IAMM Tool Question Reference: 04.05.01 (v3.5/v4.0), QUES167755993897 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does the organisation have a remote working (e.g. home or mobile) policy that complies with the requirements of HMG SPF (reference [b])? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: H]	• Details of the policy and details of how the policy is communicated to staff.	IS1&2, IS4 & IS6, GPGs 5, 6, 7, 10, 13, 19, 20, 28 & 35.	A.9.2.5 A.10.7.3 A.10.7.1
• Is there a policy covering the control of portable devices and removable media, to include laptops, removable disks, CDs, USB memory sticks, PDAs and media card formats? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: H]	• Details of the policy and how staff are made aware of it.		
• Do the Delivery Partners and 3rd party suppliers have similar policies in place?			
• Is the organisation's Remote Working Policy aligned to the Mandatory Requirements of HMG SPF (reference [c]) (e.g. IS 6)? In particular, does it specifically prohibit the handling, storage or processing of protectively marked information on unprotected privately owned computers? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: H]	• Evidence that the HMG SPF (e.g. IS6) Mandatory Requirements are reflected in the policy.		A.15.1.1 A.10.7.3

1.6 IA Incident Management [Cyber Category Type: Supporting]

1.6.1 Required Outcome: The organisation has policies and processes in place for reporting, managing and resolving IA incidents. These policies and processes make a clear distinction between what is required for post-event response and what is required to manage a real-time event, such as a cyber attack
[Links to 2.6.1; IAMM Tool Question Reference: 04.06.01 (v3.5/v4.0), QUES1677559938100 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does the organisation 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?	• Policy document	IS1&2, IS4 & IS6, GPGs 6, 13, 18, 19, 20, 24 & 28.	A.13.1 A.13.2 A.6.1.3

[IAMM Tool Evidence Reference: 1 & 2 (v3.5/v4.0); Importance: H] • Is the policy fit for purpose? • How are staff made aware of the policy? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: M] • Are all security incidents reported routinely to: a) The appropriate security authorities in the organisation, 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 GSS within the Cabinet Office for significant actual or possible losses of personal data? [IAMM Tool Evidence Reference: 5 & 6 (v3.5/v4.0); Importance: M] • Does the organisation have a Forensic Readiness Policy (FRP) which is designed to maximise the ability of the organisation 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? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: M]	• 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.		6 d) A.15.2.1 A.8.2.2 A.15.1.1 A.13.1.1 A.13.2.3

1.7 ICT Service Management [Cyber Category Type: Supporting]

1.7.1 Required Outcome: Effective IA requirements are embedded in the ICT service management procedures for all new ICT systems and work is in hand to replicate this approach across the organisation's ICT estate
[Links to 2.7.1; IAMM Tool Question Reference: 04.07.01 (v3.5/v4.0), QUES1677559938105 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Are those responsible for ICT service management aware of the need to exercise effective management of the security aspects of their role? [IAMM Tool Evidence Reference: 6 (v3.5/v4.0); Importance: M]	• There is a clear understanding and commitment, by those responsible for ICT service management within the organisation and within the 3rd party suppliers, that they have a responsibility to exercise the security aspects of their role, and this is expressed in ICT service management documentation and in plans to apply this in a proportionate manner to legacy operational ICT systems.	IS1&2 & IS6, GPGs 6, 17, 19, 20, 28 & 35.	A.6.1.2
• Is there an inventory of properly labelled ICT system assets for new IS and is the ownership understood? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: M]	• ICT system asset registers are maintained and used effectively.		A.7.1.1 A.7.1.2
• Is IA embedded within IT service management procedures for all new ICT systems so that they are operated and administered in accordance with Security Operating Procedures (Sy Ops), including effective configuration management? [IAMM Tool Evidence Reference: 1, 2, & 3 (v3.5/v4.0); Importance: 1-M, 2 to 3-H]	• 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.		4.2.2 A.10.1.2 A.12.5.1
• Are 3rd party suppliers held adequately accountable for the IA of new IS? [IAMM Tool Evidence Reference: 5 (v3.5/v4.0); Importance: M]	• Legally binding contract and service level agreements are in place that hold 3rd parties adequately accountable (e.g. via an effective audit regime), related to IA responsibilities, for all new ICT.		A.6.2.3
• Is the organisation, its Delivery Partners and its 3rd party suppliers aware of the current off-shoring policy (specifically that relating to personal data contained in IS6, reference [c]) and the current guidance (contained in GPG No. 6 (reference [o]), and the Cabinet Office CIO Council Government ICT Offshoring [International Sourcing] Guidance), particularly the requirement to gain Cabinet Office clearance before entering into any new off-shoring arrangements involving personal data? [IAMM Tool Evidence Reference: 7 (v3.5/v4.0); Importance: M]	• Appropriate internal directives ensuring that the security risks of new IS procurements are managed in accordance with current policy.		A.15.1.1 A.15.1.4 A.12.5.5 A.10.8.1

1.8 Business Continuity (BC) & Disaster Recovery (DR) [Cyber Category Type: Supporting]

1.8.1 Required Outcome: Appropriate BC & DR measures are in place for all new ICT systems and key weaknesses on existing ICT systems are addressed
[Links to 2.8.1; IAMM Tool Question Reference: 04.08.01 (v3.5/v4.0), QUES1677559938110 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Are the appropriate BC & DR measures in place for all new IS? • Are back-up processes institutionalised for all new IS? [IAMM Tool Evidence Reference: 1 & 2 (v3.5/v4.0); Importance: 1-H, 2-M] • Is there a systematic methodology for testing BC & DR measures for all new IS? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: M] • Are effective arrangements in place to safeguard unencrypted personal information contained on back up media? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: L]	• Evidence of BC & DR measures. • Details of corporate policy and its implementation for new IS. • Recent BC & DR test report. • Details of the process by which back-up media is safeguarded.	IS1&2 & IS6, GPGs 6, 17, 19, 24 & 28.	A.14.1 A.10.5.1 A.14.1.5 A.10.7.1 A.10.7.2 A.10.7.3
1.9 Digital Continuity [Cyber Category Type: Peripheral]			
1.9.1 Required Outcome: The organisation is aware of the need to address digital continuity [Links to 2.9.1; IAMM Tool Question Reference: 04.09.01 (v3.5/v4.0), QUES1677559938114 (v5.0); Recipient Type: Organisation]			
Areas to Probe	**Evidence Expected**	**Policy Reference**	**ISO27001 Reference**
• Has the organisation recognised in their corporate IA Risk Register the risks to continuity of access to their business information assets arising from digital continuity (previously referred to as digital obsolescence)? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M]	• Risk detailed in the SIRO's IA Risk Register.	IS1&2 & IS6.	4.2.1 d) A.10.7
1.10 Access Management [Cyber Category Type: Business Critical]			
1.10.1 Required Outcome: The organisation has some identification and authentication controls in place on legacy ICT systems, but it ensures that all new ICT systems have a thorough and compliant identification and authentication regime in place and has plans to raise the capability of legacy systems [Links to 2.10.1; IAMM Tool Question Reference: 04.10.01 (v3.5/v4.0), QUES1677559938119 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]			
Areas to Probe	**Evidence Expected**	**Policy Reference**	**ISO27001 Reference**
• 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? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H] • Is there an identification and authentication methodology established for new systems and is it effective? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H] • Are plans in place to raise the identification and authentication controls of legacy systems to a commensurate level? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: M] • Has the organisation a plan to link access control mechanisms to HR processes so that accounts are created and cancelled to match staff turnover? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: M] • 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? [IAMM Tool Evidence Reference: 5 (v3.5/v4.0); Importance: M] • Is a process in place whereby these logs are sampled within the organisation, its	• Details of the identification and authentication controls used. • Identification and authentication methodology follows guidance from NTA. • Details of the plans • 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 the correct	IS1&2, IS6 & IS7 (IG 3, User Authentication Systems) GPGs 10, 13, 19, 20, 28 & 35.	A.11.2 A.11.4.2 A.11.5.1 A.11.5.2 A.11.2 A.11.5.2 A.8.3.3 A.11.1.1 A.11.3.1 A.11.4.2 A.11.5.2 A.10.10.1 A.10.10.2 A.10.10.4 A.10.10.2

Delivery Partners and its 3rd party suppliers to check that the access policy is being applied correctly and take remedial action where applicable? [IAMM Tool Evidence Reference: 6 & 7 (v3.5/v4.0); Importance: L] • How are the specific SPF (IS6) minimum measures for preventing unauthorised access to personal information contained on existing IS applied?	application of the access policy and what remedial action has been taken. • Details of how compliance with the minimum measures has been achieved and is assured.		A.11.2.4 A.15.1.4 A.15.2.1

1.11 Vulnerability Detection [Cyber Category Type: Business Critical]

1.11.1 Required Outcome: Some penetration testing is undertaken on an adhoc basis, but plans are in place to determine ICT system vulnerabilities on a more systematic basis, particularly for new ICT systems
[Links to 2.11.1; IAMM Tool Question Reference: 04.11.01 (v3.5/v4.0), QUES1677559938124 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is there a process for detecting IA vulnerabilities for new systems? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: M] • Have all in-service systems processing information relating to identifiable individuals been subjected to appropriate IS6 (reference [c]) testing (e.g. for numbers above 100,000 an IT Health Check [e.g. independent penetration testing])? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H] • Has any action been taken to rectify any serious vulnerabilities detected as a result of the IT Health Check (or penetration tests)? [IAMM Tool Evidence Reference: 2 & 3 (v3.5/v4.0); Importance: 2-H, 3-M]	• Details of the process and its reach. • IT Health Check (e.g. penetration test) report. • Details of any resulting action plan (e.g. to undertake a more comprehensive approach to determining ICT system vulnerabilities).	IS1&2 & IS6, GPGs 7, 20, 28, 30, 35.	A.12.6.1 A.15.1.1 8.2 8.3 A.12.6.1

1.12 Patching [Cyber Category Type: Business Critical]

1.12.1 Required Outcome: The organisation has a patching policy and some patching is undertaken on an adhoc basis, but plans are in place to introduce a comprehensive patching regime, particularly for new ICT systems
[Links to 2.12.1; IAMM Tool Question Reference: 04.12.01 (v3.5/v4.0), QUES1677559938129 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does the organisation have a patching policy covering all ICT systems, including operating systems and applications, used within its delivery chain to reduce the risk of known vulnerabilities? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H] • Do plans exist to put in place a comprehensive patching regime? [IAMM Tool Evidence Reference: 5 (v3.5/v4.0); Importance: L] • Is a patching process specified for new ICT systems with a distinction being made between routine, critical and emergency patches? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: H] • 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? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: M] • Is the patching regime for new ICT systems 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? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H]	• Details of the Policy. • Details of the plans. • 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.	IS1&2 & IS6, GPGs 6, 7, 8, 10, 17, 19, 20, 28 & 35.	A.10.1.1 A.10.1.2 A.12.5.1 A.12.6.1 4.2.4 8.1 A.12.6.1 A.6.2.3 A.10.2.1 A.15.2.1 A.6.1.6 A.10.1.2 A.15.2.2

1.13 Lock-Down [Cyber Category Type: Business Critical]

1.13.1 Required Outcome: The organisation has a lockdown policy, which is applied to some ICT systems, but plans are in place to introduce a comprehensive lockdown regime, particularly for new ICT systems
[Links to 2.13.1; IAMM Tool Question Reference: 04.13.01 (v3.5/v4.0), QUES1677559938134 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does the organisation have a lockdown policy to restrict unnecessary services and ensure that no user has more privileges (access and functionality) than required? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Details of the lockdown policy and how it is implemented.	IS1&2 & IS6, GPGs 6, 17, 19, 20, 28 & 35.	A.11.1 A.11.2.2 A.11.4.4
• Is work is in hand to create a plan to put in place a comprehensive lockdown regime? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: L]			
• Is the process for locking down new IS to a secure configuration agreed with an Accreditor? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: M]	• Evidence of the process and its effective application to restrict user privileges to those required by the business.		A.10.1.2 A.15.2.2
• 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? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M]	• Evidence of the process and its effective application.		A.11.4.2 A.11.4.4

1.14 Anti-Malware Services [Cyber Category Type: Business Critical]

1.14.1 Required Outcome: The organisation has a malicious software policy, which is applied to some ICT systems, but plans are in place to introduce a comprehensive regime to counter malicious software, particularly for new ICT systems
[Links to 2.14.1; IAMM Tool Question Reference: 04.14.01 (v3.5/v4.0), QUES1677559938139 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does the organisation have a policy to manage the risk posed by all forms of malicious software including viruses, spyware and phishing etc.? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Details of the malware policy and how it is implemented	IS1&2 & IS6. GPGs 7, 8, 10, 13, 24, 28, 29 & 35.	A.10.4 A.10.4.1 A.10.4.2 A.10.4
• Is work in hand to create a plan to put in place a comprehensive AVS regime? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: L]			
• Is an effective process in place to ensure that all remote computers processing personal data have up to date anti-virus software? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M]	• Evidence of the process and its effective application.		

1.15 Re-Use and Controlled Disposal [Cyber Category Type: Peripheral]

1.15.1 Required Outcome: The risk posed by the re-use or disposal of ICT equipment and electronic media which has been used for protected information or by the disposal of protected information in paper form is minimised within the organisation and its delivery chain by the effective application of compliant controls
[Links to 2.15.1; IAMM Tool Question Reference: 04.15.01 (v3.5/v4.0), QUES1677559938144 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Do the organisation, its Delivery Partners and its 3rd party suppliers have effective processes in place for the controlled disposal (incineration, pulping or shredding) of protected information in paper form so that reconstruction is unlikely? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: H] • Do the organisation, its Delivery Partners and its 3rd party suppliers have effective processes in place for the controlled re-use and eventual 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 (reference [p])? [IAMM Tool Evidence Reference: 1 & 2 (v3.5/v4.0); Importance: 1-M, 2-H]	• Details of the processes used, including retention schedules, and how effectiveness is determined. • Details of the processes used and how its effectiveness is determined.	IS1&2 & IS5. GPGs 6, 18, 19, 24 & 28.	A.7.2.2 A.10.7.2 A.10.7.3 A.10.7.1 A.9.2.6 A.7.2.2 A.10.7.2 A.10.7.3

LEVEL 2 – Established - IA Processes are Institutionalised

2.1 General Measures [Cyber Category Type: Business Critical]

2.1.1 Required Outcome: An accurate picture has been established of the status of IA control measures in use across the organisation and its delivery chain, and resulting from this specific attention is given to the responsibilities of users, and a programme of work is put in place to address deficiencies in IA controls
[Links from 1.1.1 and to 3.1.1; IAMM Tool Question Reference: 04.01.02 (v3.5/v4.0), QUES167755993885 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• What has been done to ensure that the arrangements put in place at Level 1 to safeguard unencrypted personal information collected, held, processed or transferred within the organisation, its Delivery Partners and its 3rd party suppliers are followed by all staff within the delivery chain?	• Details of the compliance arrangements put in place to ensure that unencrypted personal information is subject to strong safeguards by all staff within the delivery chain.		A.7.2.2 A.10.7.3
• Does the organisation understand the IA status of its information and related ICT systems and is it taking a whole-life, coordinated and systematic approach to IA measures?	• Status reports and details of a systematic approach.		4.2.1 a)-c) 4.2.2 d) 4.2.3 d)
• Does an accurate picture exist of the status of the IA control measures in use across the organisation, its Delivery Partners and its 3rd party suppliers? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Details of the IA control measures in use.		7.1
• Does a gap analysis exist of the deficiency in IA control measures in use across the organisation? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H]	• Gap analysis report.		7.2 7.3
• Does a risk based programme of work exist to address the issues raised in the gap analysis? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: H]	• Details of the plans that exist to address the identified weaknesses in IA control measures needed to support the business need.		8.2
• Has the organisation established effective methodologies to make all users of ICT systems familiar with the Security Operating Procedures governing their use at induction and annually thereafter? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: H]	• Details of the process and its efficacy.		5.2.2 A.8.2.2

2.1.2 Required Outcome: The organisation understands the IA status of its information and the related ICT and is taking a whole-life, coordinated and systematic approach to the implementation of effective IA measures
[Links from 1.1.2 and to 3.1.2; IAMM Tool Question Reference: 04.01.04 (v3.5), 04.01.06 (v4.0), QUES167755993889 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is the organisation implementing through-life IA measures in a co-ordinated way? [IAMM Tool Evidence Reference: 1 & 2 (v3.5/v4.0); Importance: 1-H, 2-M]	• Evidence of the implementation of cross-cutting measures that impact on more than one system, rather than on a system by system basis.		4.2.1 4.2.2 4.2.3

2.2 Physical & Environmental Security Measures [Cyber Category Type: Peripheral]

2.2.1 Required Outcome: The organisation has audit assurance that it is compliant with the SPF mandatory minimum measures for ensuring the physical security of information within its delivery chain
[Links from 1.2.1; IAMM Tool Question Reference: 04.02.02 (v3.5/v4.0), QUES167755993892 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Do the organisation, 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 (reference [b])? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H] • Are the processes that were put in place at Level 1, to test and validate the physical protection measures and access controls to sites, buildings and equipment rooms, assured by audit (internal or external audit)? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M] • If such audits identify any weaknesses, is there evidence that these are rectified by prompt action? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: M]	• Details of the processes. • Details of the processes and any assurance activity undertaken. • Details of any remedial action taken.	SPF	A.6.2.3 A.9.1 A.9.2 A.15.2.1

2.3 Personnel Security Measures [Cyber Category Type: Peripheral]

2.3.1 Required Outcome: The organisation has audit assurance that it is compliant with the SPF mandatory minimum personnel security measures for those staff who have access to the organisation's information within the organisation itself and within its delivery chain
[Links from 1.3.1; IAMM Tool Question Reference: 04.03.02 (v3.5/v4.0), QUES167755993894 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Do the personnel security measures in use by the organisation, its Delivery Partners and its 3rd party suppliers, particularly in terms of security checking and vetting, meet HMG SPF Tier 3 requirements? [IAMM Tool Evidence Reference: 1 & 2 (v3.5/v4.0); Importance: M] • Has the process been assured by audit? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: H] • If any weaknesses have been identified, have they been rectified by prompt action? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: M]	• Details of any security checking and vetting assurance activity undertaken, together with details of any remedial action taken.	SPF	A.8.1.1 A.8.1.2

2.4 Acceptable Use Policy [Cyber Category Type: Supporting]

2.4.1 Required Outcome: Staff compliance with the organisation's Acceptable Use Policy has been assessed by audit and the risk posed to the business by unauthorised use is acceptable
[Links from 1.4.1; IAMM Tool Question Reference: 04.04.02 (v3.5/v4.0), QUES167755993896 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Has the risk to the organisation's information resulting from unauthorised use of its ICT facilities been assessed to determine whether it is acceptable to the business? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M]	• Risk assessment report		4.2.1 e)
• Has any action been taken to amend the Acceptable Use Policy (AUP) as a result of the risk assessment?	• Details of any revisions made as a result of the risk assessment.		A.7.1.3 A.15.1.5
• Has compliance with the (AUP) been assessed and have any weaknesses identified rectified by prompt action? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Compliance assessment (e.g. audit) report.		A.15.2.1

2.5 Remote Working, Portable Devices and Removable Media [Cyber Category Type: Business Critical]

2.5.1 Required Outcome: The organisation has assurance that effective control measures are in place within the organisation, its Delivery Partners and within its 3rd party suppliers to reduce the risk from all aspects of remote working to a level acceptable to the business
[Links from 1.5.1 and to 3.2.1; IAMM Tool Question Reference: 04.05.02 (v3.5/v4.0), QUES167755993898 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties][Modified in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Are effective controls in place across the organisation, its Delivery Partners and its 3rd party suppliers to limit the risk posed by portable devices and removable media? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Details of the controls applied and how the organisation plans to ensure compliance.		A.10.7.1 A.15.2.1
• Has the organisation, its Delivery Partners and its 3rd party suppliers implemented their policies on Remote Working? [IAMM Tool Evidence Reference: Also 1 (v3.5/v4.0); Importance: H]	• Details of the Remote Working Policy implementation.		A.9.2.5 A.10.7.3
• Have effective mechanisms been devised to ensure compliance? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M]	• Details of any planned compliance activity.		A.15.2.1

2.6 IA Incident Management [Cyber Category Type: Supporting]

2.6.1 Required Outcome: The organisation responds effectively to all IA incidents taking timely and decisive real-time action to limit the immediate business impact and by subsequently enacting preventative measures, prevents their recurrence
[Links from 1.6.1 and to 3.3.1; IAMM Tool Question Reference: 04.06.02 (v3.5/v4.0), QUES1677559938101 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• To cater for the need to take timely and decisive action in the event of an incident such as a cyber attack, is there a nominated IA Incident Manager and is the individual trained and competent to perform the role? [IAMM Tool Evidence Reference: 5 & 6 (v3.5/v4.0); Importance: 5-H, 6-H]	• TORs are established and the individual is trained to discharge their duty in a competent manner.		A.13.2.1
• Is there an effective IA Incident Management Plan to reduce the business impact of any incident (including cyber attack)?	• A workable process exists to reduce the business impact of any incident, to learn lessons and maintain forensic information, where this is appropriate.		A.13.2.1

[IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H] • Does it include an escalation process? • Does the IA Incident Management Plan take account of the Forensic Readiness Policy? [IAMM Tool Evidence Reference: Also 1 (v3.5/v4.0); Importance: H] • Has the plan been tested? [IAMM Tool Evidence Reference: 2 & 3 (v3.5/v4.0); Importance: M] • Is root-cause analysis performed and is an analysis of any trends established? [IAMM Tool Evidence Reference: 8 & 9 (v3.5/v4.0); Importance: M] • Lessons are learned and shared across HMG IA community. [IAMM Tool Evidence Reference: Also 9 & 10 (v3.5/v4.0); Importance: M] • Is adequate training in IA incident management given? [IAMM Tool Evidence Reference: 7 (v3.5/v4.0); Importance: L] • Are all users made aware of the IA incident management and reporting procedures? • Where staff negligence is involved in IA incidents have appropriate sanctions been considered and, where appropriate, imposed? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: M]	• A process is in place to escalate the response to IA incidents appropriately. • Evidence of appropriate Forensic Readiness aspects in the IA incident management plan. • Date of when the effectiveness of the plan has been evaluated and any resulting remedial activity. • 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 efficacy of dissemination. • Details of any disciplinary action taken as a direct result of IA incidents.		A.13.2.3 8.2 b) A.13.2.2 A.8.2.2 A.8.2.3

2.7 ICT Service Management [Cyber Category Type: Supporting]

2.7.1 Required Outcome: IA good practice is institutionalised within the ICT Service Management function so that systems are operated and administered in accordance with corporate security operating procedures and the organisation has assurance that effective IA measures are being employed
[Links from 1.7.1 and to 3.4.1; IAMM Tool Question Reference: 04.07.02 (v3.5/v4.0), QUES1677559938106 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Do those who are responsible for ICT service management recognise the need for an institutionalised approach to the management of IA? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• 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.		A.6.1.2
• Do those responsible for ICT service management allocate sufficient resource and funding to tackle IA issues? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: M]	• The resolution of IA issues is given appropriate priority in the programme to address IT service management requirements.		5.2.1
• Have the organisation, its Delivery Partners and its 3rd party suppliers catalogued and assessed the ownership, business criticality and IA requirements of all ICT system assets? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: M]	• ICT system asset registers are accurate and are used to determine the priority of work to rectify IA issues		A.7.1.1 A.7.1.2
• 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? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H]	• Evidence of the application of clearly documented processes and procedures.		4.2.2 A.10.1.2 A.12.5.1
• Are 3rd party suppliers applying effective IA measures and are they being held accountable for non-compliance? [IAMM Tool Evidence Reference: 5 & 6 (v3.5/v4.0); Importance: M]	• 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 organisation employing alternative ways of achieving desired outcome.		6 8.3 A.6.2.3

2.8 Business Continuity (BC) & Disaster Recovery (DR) [Cyber Category Type: Supporting]

2.8.1 Required Outcome: The requirement for the delivery and testing of BC & DR measures for ICT systems is institutionalised, with priority being given to business critical ICT systems. The organisation has appropriate BC and DR Plans for all locations where information and ICT System assets (including cryptographic items) are kept

[Links from 1.8.1 and to 3.5.1; IAMM Tool Question Reference: 04.08.02 (v3.5/v4.0), QUES1677559938111 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does the organisation have appropriate Business Continuity and Disaster Recovery Plans for all locations where information and system assets (including cryptographic items) are kept?	• Organisational BC & DR policy complies with HMG SPF (reference [b]). • Evidence planning for the implementation of effective BC & DM measures.		A.14.1
• Is the need for effective back-up processes understood and do plans exist to implement appropriate BC & DR measures for all IS? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M]	• Details of corporate policy and its implementation.		A.10.5.1
• Is a systematic methodology in place for testing BC & DR measures for all IS? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H]	• Recent BC & DR test report and schedule of tests.		A.14.1.5

2.9 Digital Continuity [Cyber Category Type: Peripheral]

2.9.1 Required Outcome: Appropriate policy is in place that addresses digital continuity and a plan exists to assess the business risk

[Links from 1.9.1 and to 3.6.1; IAMM Tool Question Reference: 04.09.02 (v3.5/v4.0), QUES1677559938115 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Do organisational strategies and policies for IT, IA and Information Management reflect the need to identify and mitigate digital continuity risks in a proportionate manner? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M]	• Strategy and Policy documentation reflect theneed to manage digital continuity risks.		4.2.1 d) A.10.7 A.6.2.3
• Has the organisation engaged its 3rd party ICT providers in digital continuity (e.g. obsolescence) risk management? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: M]	• Organisations have met 3rd party suppliers and have agreed that they need to be involved in plans to deal with the organisation's digital continuity risks.		A.10.2 4.2.1 b)
• Is there a documented plan for undertaking a risk assessment process to identify the specific digital continuity risks to the department, with timescales, resources and a board-level SRO? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M]	• Details of the Risk Assessment Plan, which is consistent with the Digital Continuity approach and Guidance from The National Archives (TNA).		4.2.3 d)

2.10 Access Management [Cyber Category Type: Business Critical]

2.10.1 Required Outcome: The organisation has assurance that the NTA compliant, corporate identification and authentication methodology which has been established throughout the organisation and its delivery chain is fit for purpose

[Links from 1.10.1 and to 3.7.1; IAMM Tool Question Reference: 04.10.02 (v3.5/v4.0), QUES1677559938120 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Has a corporate identification and authentication methodology, which follows NTA guidance, been effectively established, and been independently assessed, throughout the organisation and its delivery chain? [IAMM Tool Evidence Reference: 1 & 2 (v3.5/v4.0); Importance: 1-M, 2-H]	• Identification and authentication methodology follows guidance from the NTA.		A.11
• Is an audit regime in place for access control? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: L]	• Audit logs and related management processes (e.g. remedial action, where necessary).		A.10.10.1
• Are access lists kept up-to-date and are they aligned to personnel security and HR processes? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: M]	• Documented processes exist, together with evidence of accounts being created and cancelled to match staff turnover.		A.11.2.4
• How are they assured? [IAMM Tool Evidence Reference: Also 2 (v3.5/v4.0); Importance: H]	• Details of assurance of the process.		A.15.2.1

2.11 Vulnerability Detection [Cyber Category Type: Business Critical]

2.11.1 Required Outcome: The process for detecting IA vulnerabilities within the organisation is institutionalised and a plan to detect the IA vulnerabilities for all ICT systems and information assets has been produced
[Links from 1.11.1 and to 3.8.1; IAMM Tool Question Reference: 04.11.02 (v3.5/v4.0), QUES1677559938125 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is the process for detecting IA vulnerabilities institutionalised and does the organisation have a plan to detect the IA vulnerabilities for all systems? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Details of the clearly documented processes and procedures and their reach. • Details of the plan.		A.12.6.1
• Are specific objectives set for reducing vulnerabilities based upon threats, ease of exploitation and potential impact? [IAMM Tool Evidence Reference: Also 1 (v3.5/v4.0); Importance: H]	• Details of objectives and plan for reducing vulnerability.		A.12.6.1
• Are penetration tests regularly undertaken by an approved authority and recommendations acted upon? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: L]	• A comprehensive schedule of penetration tests to be undertaken by approved authorities (where appropriate CHECK certified) has been drawn up.		A.15.1.1
• What access to up-to-date sources of publicly available, and where appropriate NTA provided, vulnerability information does the organisation have? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M]	• Details of accesses available and use made of the data. • Details of the tools and the training given to the personnel who use them		A.6.1.7 5.2.1
• What vulnerability analysis tools are available and are the staff trained to use them?			5.2.2

2.12 Patching [Cyber Category Type: Business Critical]

2.12.1 Required Outcome: A comprehensive patching regime has been introduced and is being applied to appropriate ICT systems. The organisation has assurance that patches are applied in a timely manner
[Links from 1.12.1 and to 3.9.1; IAMM Tool Question Reference: 04.12.02 (v3.5/v4.0), QUES1677559938130 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Has a comprehensive patching regime been introduced within the organisation's delivery chain and has work started to apply it to legacy ICT systems? [IAMM Tool Evidence Reference: 1 & 3 (v3.5/v4.0); Importance: 1-M, 3-H] • If a 3rd party supplier is involved, are the audit arrangements sufficient to	• 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.	SPF	A.10.1.1 A.10.1.2 A.10.2.1 A.10.2.2

establish that patching is applied in compliance with policy? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M]			A.15.2

2.13 Lock-Down [Cyber Category Type: Business Critical]

2.13.1 Required Outcome: A comprehensive plan exists to lockdown all aspects of the organisation's ICT systems to secure configurations and this is being implemented in line with business priorities
[Links from 1.13.1 and to 3.10.1; IAMM Tool Question Reference: 04.13.02 (v3.5/v4.0), QUES1677559938135 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is the plan for locking down ICT systems to a secure configuration agreed with an Accreditor institutionalised? [IAMM Tool Evidence Reference: 1 & 2 (v3.5/v4.0); Importance: 1-H, 2-L]	• Evidence of the plan and its effective application to restrict user privileges to those required by the business.		A.15.2.1 A.6.1.6

2.14 Anti-Malware Services [Cyber Category Type: Business Critical]

2.14.1 Required Outcome: A plan exists to implement a comprehensive Anti Virus Service (AVS) across the organisation
[Links from 1.14.1 and to 3.11.1; IAMM Tool Question Reference: 04.14.02 (v3.5/v4.0), QUES1677559938140 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Do plans exist to replace the piecemeal, system by system approach to anti-malware controls with the provision of a comprehensive Anti Virus Service (AVS) covering all ICT systems in use across the organisation? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Details of the Plan.		A.10.4.1&2 A.15.2

2.15 Re-Use and Controlled Disposal [Cyber Category Type: Peripheral]

2.15.1 Required Outcome: The organisation has assurance that the controls governing the reuse and disposal of electronic equipment and media and the destruction of paper based information within its delivery chain are effective
[Links from 1.15.1; IAMM Tool Question Reference: 04.15.02 (v3.5/v4.0), QUES1677559938145 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Has the effectiveness of the controlled disposal (incineration, pulping or shredding) of protected information in paper form within the organisation and its delivery chain been assured by either internal or external audit? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M]	• Audit Report detailing whether the procedures in place are sufficient to meet the needs of the business, together with details of any remedial action.	IS5	6 A.15.2
• Has the effectiveness of the controlled re-use and eventual disposal of electronic media that have been used for protected information within the organisation and its delivery chain been assured by either internal or external audit? [IAMM Tool Evidence Reference: Also 1 (v3.5/v4.0); Importance: M]	• Audit Report detailing whether the procedures in place are sufficient to meet the needs of the business, together with details of any remedial action.		6 A.15.2

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

3.1 General Measures [Cyber Category Type: Business Critical]

3.1.1 Required Outcome: The SIRO is content to accept the risk associated with any specified deficiencies in the application of IA control measures to business critical ICT systems
[Links from 2.1.1 and to 4.1.1; IAMM Tool Question Reference: 04.01.03 (v4.0), QUES167755993886 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties][Modified in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Has a review been undertaken of the arrangements put in place to safeguard unencrypted personal information collected, held, processed or transferred within the organisation, its Delivery Partners and its 3rd party suppliers to ensure that the arrangements meet the business need? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: H]	• Details of the review and any subsequent remedial action.		7.2 f) A.7.2.2 A.10.7.3
• Have all of the deficiencies in IA control measures applicable to business critical systems identified in the gap analysis at Level 2 been addressed to the satisfaction of the SIRO? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: H] • How has the organisation assessed compliance of staff with the requirement to make themselves aware of the security operating procedures governing their use of ICT systems at induction and annually thereafter? [IAMM Tool Evidence Reference: 3 (v4.0); Importance: H]	• Confirmation that the organisation has taken a systematic, enterprise approach to IA measures and that these are applied to all business critical ICT systems • Details of how the deficiencies have been addressed, or risk balance cases presented to the SIRO for acceptance of the tolerated risks. • Details of the compliance process.		7.1, 7.2, 7.3 8.2 5.2.2 A.8.2.2 A.15.2.1

3.1.2 Required Outcome: All business critical ICT systems are subject to the organisation's systematic approach to IA measures
[Links from 2.1.2; IAMM Tool Question Reference: 04.01.07 (v4.0), QUES167755993890 (v.5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Are all business critical information assets and related ICT systems subject to the regime of systematic IA measures initiated at level 2? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: H]	• Confirmation that the organisation has taken a systematic, enterprise approach to IA measures and that these are applied to all business critical information assets and related ICT systems.		4.2.1 a)-c) 4.2.2 d) 4.2.3 d)

3.2 Remote Working, Portable Devices and Removable Media [Cyber Category Type: Business Critical]

3.2.1 Required Outcome: The risk posed to critical Information Assets, by remote working, has been assessed, and is acceptable to the business
[Links from 2.5.1; IAMM Tool Question Reference: 04.05.03 (v4.0), QUES167755993899 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• How has the organisation assessed compliance with its policy on the use of portable devices and removable media? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M]	• Details of the compliance method used and any resultant remedial action taken.		A.10.7.1 A.15.2.1
• Has the organisation implemented effective control measures to protect its business critical information assets from the increased risk posed by remote working? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: H]	• Details of the control measures put in place on all ICT systems that could impact on the assurance of business critical information assets.		A.9.2.5 A.10.7.3 A.15.2.1
• Are effective measures in place to ensure compliance with the organisation's policy? [IAMM Tool Evidence Reference: 3 (v4.0); Importance: M]	• Details of the compliance regime		

3.3 IA Incident Management [Cyber Category Type: Supporting]

3.3.1 Required Outcome: The organisation's senior management are content that the mechanisms in place to handle IA incidents affecting critical business processes are proportionate to the threat
[Links from 2.6.1 and to 4.2.1; IAMM Tool Question Reference: 04.06.03 (v3.5/v4.0), QUES1677559938102 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Are metrics available for all IA related incidents and problems relating to business critical ICT systems? [IAMM Tool Evidence Reference: 1 & 2 (v3.5/v4.0); Importance: H]	• Comprehensive data is available and is reported to senior managers in a way that enables effective action to be taken.		A.13.2.2

3.4 ICT Service Management [Cyber Category Type: Supporting]

3.4.1 Required Outcome: IA is embedded within the IT Service Management procedures for all business critical ICT systems and this includes effective configuration management
[Links from 2.7.1 and to 4.3.1; IAMM Tool Question Reference: 04.07.03 (v3.5/v4.0), QUES1677559938107 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• 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 (including shared-services, where appropriate)? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Details of the objectives, priorities and qualitative performance targets.		5.1 A.6.1.3
• Have the process or service owners for IT service management been made responsible for delivering specific levels of improvement in IA? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: L]	• Details of the targets that have been set and the method by which they are reporting against them.		5.1 A.6.1.1
• Is IA is embedded within IT service management procedures for all business critical ICT systems?	• Evidence of clearly documented processes and procedures. Comprehensive and consistent SyOps (Security Operating Procedures) are applied across the organisation to business critical ICT systems.		A.10.1.1 A.10.1.2
• Are the IA elements of 3rd party ICT services relating to business critical IS actively monitored and managed, particularly the restrictions on off-shoring? [IAMM Tool Evidence Reference: 3 & 4 (v3.5/v4.0); Importance: 3-M, 4-L]	• The IA performance of 3rd party ICT suppliers is qualitatively assessed and they are held to account for any deficiencies. Where applicable, they are contracted to do so, but when no legally binding agreement can be put in place an SLA exists that is proving effective in covering IA responsibilities.		A.6.2.3 A.10.2.2

3.5 Business Continuity (BC) & Disaster Recovery (DR) [Cyber Category Type: Supporting]

3.5.1 Required Outcome: Effective BC & DR measures are in place for all business critical ICT systems. The organisation has appropriate and effective BC and DR measures in place for all locations where information and ICT system assets (including cryptographic items) related to business critical ICT systems are kept
[Links from 2.8.1 and to 4.4.1; IAMM Tool Question Reference: 04.08.03 (v3.5/v4.0), QUES1677559938112 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Are the appropriate BC & DR measures in place for all business critical ICT systems?	• Evidence of BC & DR measures.		A.14.1
• Are appropriate BC & DR measures in place for all locations where information and ICT systems IS assets are kept and these are subject to regular and effective testing? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: M]	• Evidence of BC & DR measures.		A.14.1
• Are back-up processes institutionalised for all business critical ICT systems?	• Details of corporate policy and its implementation for all business critical IS.		A.10.5.1

[IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H] • Is there a systematic methodology for testing BC & DR measures for all business critical ICT systems? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M]	• Recent BC & DR test report.		A.14.1.5

3.6 Digital Continuity [Cyber Category Type: Peripheral]

3.6.1 Required Outcome: Work is in hand to address the specific digital continuity risks relating to the organisation's business critical information assets and to put in place a systematic process to maintain an appropriate digital continuity posture
[Links from 2.9.1 and to 4.5.1; IAMM Tool Question Reference: 04.09.03 (v3.5/v4.0), QUES1677559938116 (v.5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Has a risk assessment been undertaken to identify the organisation's specific digital Continuity 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? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H] • Is the organisation undertaking any initial, priority digital continuity 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 continuity mitigation activity? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M] • Has a systematic process been created to review digital obsolescence risks and their mitigation actions as part of a digital information lifecycle management process? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: L]	• 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. • Organisations 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. • A review of digital obsolescence risks and their mitigation actions is part of the digital information lifecycle management process.		4.2.1 c) 4.2.3 d) 4.2.3 h) 4.2.3 i) A.6.1.6 4.2.1 e) 4.2.1 f) 4.2.1 g) 4.2.2 a)-d) 4.2.2 b) 4.2.2 c) A.10.2.3

3.7 Access Management [Cyber Category Type: Business Critical]

3.7.1 Required Outcome: The efficacy of the access control mechanisms being applied to all business critical ICT systems has been assessed by audit
[Links from 2.10.1 and to 4.6.1; IAMM Tool Question Reference: 04.10.03 (v3.5/v4.0), QUES1677559938121 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is there an identification and authentication methodology established for all business critical systems and is it effective? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M] • Is an audit regime in place for access control for all business critical ICT systems? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M]	• Identification and authentication methodology follows guidance from theNTA. • Audit logs and related management process. • Work in place to address any identified shortfalls in the access control mechanisms.		A.11 A.15.2.1

3.8 Vulnerability Detection [Cyber Category Type: Business Critical]

3.8.1 Required Outcome: IA vulnerabilities for all business critical ICT systems and key information assets are reduced to a level that is acceptable to the business
[Links from 2.11.1 and to 4.7.1; IAMM Tool Question Reference: 04.11.03 (v3.5/v4.0), QUES1677559938126 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is the process for detecting IA vulnerabilities for business critical systems and key information assets institutionalised? • Are specific objectives set for reducing vulnerabilities based upon threats, ease of exploitation and potential impact? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H] • Are penetration tests regularly undertaken by an approved authority and recommendations acted upon? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M]	• Details of the process and its reach. • Details of objectives and plan for reducing vulnerability. • Penetration reports and subsequent action plans.		A.12.5.2 A.12.6.1 A.12.6.1 A.15.1.1

3.9 Patching [Cyber Category Type: Business Critical]

3.9.1 Required Outcome: Patches are applied to all business critical ICT systems in a timescale that is acceptable to the business
[Links from 2.12.1 and to 4.8.1; IAMM Tool Question Reference: 04.12.03 (v3.5/v4.0), QUES1677559938131 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is the patching process for all business critical ICT systems institutionalised within the organisation's delivery chain with the patches being applied in a timescale that is acceptable to the business, and with a distinction being made between routine, critical and emergency patches? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H] • If a 3rd party supplier is involved, are the audit arrangements sufficient to establish that patching is applied in compliance with policy? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: M] • Is the patching regime for all business critical IS agreed with the Accreditor? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M]	• A comprehensive patching regime is in existence and evidence exists (e.g. an Enterprise Maintenance Management System) 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.		A.10.1.1 A.10.2.2 A.10.1.1 A.10.2.2 A.15.2 A.15.2.1 A.6.1.6

3.10 Lock-Down [Cyber Category Type: Business Critical]

3.10.1 Required Outcome: All business critical ICT systems are locked down to a secure configuration that meets the needs of the business
[Links from 2.13.1 and to 4.9.1; IAMM Tool Question Reference: 04.13.03 (v3.5/v4.0), QUES1677559938136 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is the process for locking down all business critical ICT systems to a secure configuration agreed with an Accreditor, institutionalised? [IAMM Tool Evidence Reference: 1 & 2 (v3.5/v4.0); Importance: 1-H, 2-L]	• Evidence of the process and its effective application to restrict user privileges to those required by the business.		A.15.2.1 A.6.1.6

3.11 Anti-Malware Services [Cyber Category Type: Business Critical]

3.11.1 Required Outcome: All business critical ICT systems are subject to a robust anti-malware regime that meets the needs of the business
[Links from 2.14.1 and to 4.10.1; IAMM Tool Question Reference: 04.14.03 (v3.5/v4.0), QUES1677559938141 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Are all business critical ICT systems subject to a robust anti-malware regime that has been agreed with the Accreditor? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H] • Are AVS processes institutionalised for all business critical ICT systems? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M]	• Evidence of the process and its effective application to meet the needs of the business. • Details of the process and methodology for assessing compliance.		A.10.4 A.10.4.1&2 A.6.1.6 A.10.4.1 A.15.2.2

LEVEL 4 – Quantitatively Managed –
The board has established its broader IA Road Map for all its information, systems and processes

4.1 General Measures [Cyber Category Type: Business Critical]

4.1.1 Required Outcome: The business impact of Information System vulnerabilities is known and the SIRO is content to accept the risk
[Links from 3.1.1; IAMM Tool Question Reference: 04.01.04 (v4.0), QUES167755993887 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Do accurate details exist of the status of IA control measures which impact on all information systems and assets in use across the organisation? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: H] • Is the SIRO and hence the Main Board aware of those information systems 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? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: H]	• Management reports detailing how the organisation is complying with HMG corporate guidance. • Details of any formal assessment made such as ISO 27001 audits. • Details of any business impact assessment undertaken and presented to the SIRO.		6 A.15.2.1 7.1 7.3 b)

4.2 IA Incident Management [Cyber Category Type: Supporting]

4.2.1 Required Outcome: Senior management are demonstrating a proportionate and risk based response to IA incidents
[Links from 3.3.1 and to 5.1.1; IAMM Tool Question Reference: 04.06.04 (v4.0), QUES1677559938103 (v5.0); Recipient Type: Organisation]
[Modified in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Are metrics available for all IA related incidents and problems within the organisation? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: H]	• Comprehensive data is available and is reported to senior managers in a way that enables effective action to be taken. • Reporting of best practice and lessons learnt (e.g. beyond what is required by statute).		A.13.2.1 A.13.2.2

4.3 ICT Service Management [Cyber Category Type: Supporting]

4.3.1 Required Outcome: ICT service management take a proactive approach to delivering secure ICT facilities that are matched to the business need
[Links from 3.4.1 and to 5.2.1; IAMM Tool Question Reference: 04.07.04 (v4.0), QUES1677559938108 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Have metrics been developed to assess the IA aspects of ICT service management across the organisation to ensure that the service provided meets the business need with an acceptable level of information risk? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: H]	• 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.		4.2.3 5.1 h)
• Is the ICT service management organisation able to predict the service demand from the business and posture secure ICT services to meet the business need in a timely manner? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: L]	• The likely service demand is quantified and processes are in place to provide secure ICT services to meet the needs of the business.		4.2.3 d) A.10.3.1
• Is IA embedded within ICT service management procedures for all ICT systems? [IAMM Tool Evidence Reference: 3 (v4.0); Importance: H]	• Evidence of clearly documented processes and procedures. Comprehensive and consistent SyOps (Security Operating Procedures) are applied across the organisation to all IS.		A.10.1.1 A.10.1.2
• Are the IA elements of 3rd party ICT services relating to all ICT systems actively monitored and managed? [IAMM Tool Evidence Reference: 4 (v4.0); Importance: M]	• The IA performance of 3rd party ICT suppliers is qualitatively assessed and they are held to account for any deficiencies. • Evidence of a mature relationship (e.g. contracts were written to allow the 3rd party to be "proactive" to support the evolving needs of IA, ideally as "business as usual").		A.6.2.3 A.10.2.2 A.10.2.3

4.4 Business Continuity (BC) & Disaster Recovery (DR) [Cyber Category Type: Supporting]

4.4.1 Required Outcome: Effective BC & DR measures, including effective testing, are in place for the systems where this is warranted
[Links from 3.5.1; IAMM Tool Question Reference: 04.08.04 (v4.0), QUES1677559938113 (v5.0); Recipient Type: Organisation][Modified in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Where the business need warrants it, are the appropriate BC & DR measures in place for all ICT systems (including shared-services, where appropriate)? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M]	• Evidence of BC & DR measures.		A.14.1
• Are back-up processes institutionalised for such ICT systems? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: H]	• Details of corporate policy and its implementation for all applicable ICT systems.		A.10.5.1
• Is there a systematic methodology for testing BC & DR measures that are in place for such ICT systems? [IAMM Tool Evidence Reference: 3 (v4.0); Importance: M]	• Recent BC & DR test report, including low level testing (with lessons learnt being fed back into the BC & DR strategy).		A.14.1.5

4.5 Digital Continuity [Cyber Category Type: Peripheral]

4.5.1 Required Outcome: A proportionate approach to digital continuity has been taken that is matched to the needs of the business
[Links from 3.6.1 and to 5.3.1; IAMM Tool Question Reference: 04.09.04 (v4.0), QUES1677559938117 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is the organisation undertaking digital continuity risk mitigation action, as identified in their Risk Mitigation Plan, to ensure continuity of access to all relevant business information assets? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M]	• Details of risk mitigation interventions at the policy, procedural and technical levels and evidence of business outcomes and benefits being tracked and realised.		4.2.2 b) 4.2.2 c) A.10.2.3
• Are all information assets subject to regular digital continuity risk reviews and mitigation schedules, with exceptions and legacy systems/assets identified and agreed? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: H]	• Evidence that information asset owners are aware of digital continuity risks to their information assets. • Exceptions to risk mitigation actions and plans to address these gaps are documented in SIRO/board-level reporting.		4.2.1 c) 4.2.2 a) 4.2.3 d)
• Has digital continuity and incidents affecting the continuity of access to business information assets been incorporated into incident reporting procedures? [IAMM Tool Evidence Reference: 3 (v4.0); Importance: M]	• Detail of incident reporting procedures and incident reports, if any.		A.13.1.1 A.13.2.2
• Are the organisation's 3rd party suppliers fulfilling contractual obligations around digital Continuity and is there a mechanism to monitor compliance? [IAMM Tool Evidence Reference: 4 (v4.0); Importance: M]	• SLA agreements and relevant KPIs, with contract management or service review processes.		A.10.2.2 A.15.2.1
• Do parent Department's take responsibility for managing the Digital Continuity of that Department's potentially "ephemeral" institutions (e.g. Non-Departmental Public Bodies (NDPBs))? [IAMM Tool Evidence Reference: 5 (v4.0); Importance: H]	• Evidence that the relevant institutions digital continuity aspects are considered an integral part of the parent Department's digital continuity, and is addressed proportionately.		A.15.2.1

4.6 Access Management [Cyber Category Type: Business Critical]

4.6.1 Required Outcome: The business has determined the required access control mechanisms for all ICT systems and this has been assured by audit
[Links from 3.7.1 and to 5.4.1; IAMM Tool Question Reference: 04.10.04 (v4.0), QUES1677559938122 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties][Modified in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Where it is assessed as necessary, is there an identification and authentication methodology established for all IS and is it effective? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M]	• Identification and authentication methodology follows guidance from the NTA.	IS7	A.11
• Is an audit regime in place for access control for all such IS? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: M]	• Audit logs and related management process.		A.15.2.1

4.7 Vulnerability Detection [Cyber Category Type: Business Critical]

4.7.1 Required Outcome: IA vulnerabilities for all information systems have been risk managed to a level that is acceptable to the business
[Links from 3.8.1 and to 5.5.1; IAMM Tool Question Reference: 04.11.04 (v4.0), QUES1677559938127 (v5.0); Recipient Type: Organisation]
[Modified in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is the process for detecting IA vulnerabilities for all IS institutionalised? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: H]	• Details of the process and its reach.		A.12.6.1
• Are specific objectives set for reducing vulnerabilities based upon threats, ease of exploitation and potential impact? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: H]	• Details of objectives and plan for reducing vulnerability.		A.12.6.1
• Are penetration tests regularly undertaken by an approved authority and recommendations acted upon? [IAMM Tool Evidence Reference: 3 (v4.0); Importance: M]	• Penetration reports and subsequent action plans.		A.15.1.1

4.8 Patching [Cyber Category Type: Business Critical]

4.8.1 Required Outcome: Patches are applied to all ICT systems in a timescale that is acceptable to the business
[Links from 3.9.1 and to 5.6.1; IAMM Tool Question Reference: 04.12.04 (v4.0), QUES1677559938132 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is the patching process for all IS institutionalised with a distinction being made between routine, critical and emergency patches? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: H]	• A comprehensive patching regime is in existence and evidence exists that new IS patches are applied in a time scale applicable to the seriousness of the vulnerability.		A.10.1.1 A.10.2.2
• If a 3rd party supplier is involved, are the audit arrangements sufficient to establish that patching is applied in compliance with policy? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: M]	• Details of audit of 3rd party supplier patching compliance.		A.10.1.1 A.10.2.2 A.15.2
• Is the patching regime for all IS agreed with the Accreditor? [IAMM Tool Evidence Reference: 3 (v4.0); Importance: M]	• Details exist of the Accreditor's agreement to the patching regime agreed for all IS. • Where patching is not possible, evidence of the Accreditor's agreement of the appropriate mitigations, which have then been applied in those circumstances.		A.15.2.1 A.6.1.6 A.6.1.6

4.9 Lock-Down [Cyber Category Type: Business Critical]

4.9.1 Required Outcome: Has the lockdown configuration for all systems been adapted to meet the needs of the business in a risk managed way
[Links from 3.10.1 and to 5.7.1; IAMM Tool Question Reference: 04.13.04 (v4.0), QUES1677559938137 (v5.0); Recipient Type: Organisation]
[Modified in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is the process for locking down all IS to a configuration agreed with an Accreditor institutionalised? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: H]	• Evidence of the process and its effective application to restrict user privileges to those required by the business. • Evidence that the business representative, and the Accreditor, have reviewed the lockdown adaptations (although not necessarily both attending the same review meetings, if the content needs to be focussed to the appropriate audience).		A.15.2.1 A.6.1.6 A.6.1.6

4.10 Anti-Malware Services [Cyber Category Type: Business Critical]

4.10.1 Required Outcome: All ICT systems are subject to an anti-malware regime that meets the needs of the business
[Links from 3.11.1 and to 5.8.1; IAMM Tool Question Reference: 04.14.04 (v4.0), QUES1677559938142 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Are all IS subject to a malware regime agreed with the Accreditor? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: H] • Are AVS processes institutionalised for all IS? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: M] • Are details of malware incidents for all IS collated and reported to senior management? [IAMM Tool Evidence Reference: 3 (v4.0); Importance: M]	• Evidence of the process and its effective application. • Details of the process and methodology for assessing compliance. • Details of recent reports submitted to senior management.		A.10.4 A.10.4.1&2 A.6.1.6 A.10.4.1 A.15.2.2 7.1 7.3 b)

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

5.1 IA Incident Management [Cyber Category Type: Supporting]

5.1.1 Required Outcome: The organisation has the processes in place to enable it to take proactive action to avoid IA incidents, where this is possible
[Links from 4.2.1; IAMM Tool Question Reference: 04.06.05 (v4.0), QUES1677559938104 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is the organisation capable of identifying warning signs for potential incidents and taking action to avoid or prevent the incident from occurring? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: H] • Is there effective engagement with external stakeholders so that the organisation learns from the experience of others? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: M]	• Details of the process and successful interventions. • Details of the engagement process and action taken to avoid potential incidents.		8.3 A.13.1 A.6.1.6 A.6.1.7 A.13.2.2

5.2 ICT Service Management [Cyber Category Type: Supporting]

5.2.1 Required Outcome: IA measures are enacted by the ICT service management organisation as part of normal business
[Links from 4.3.1; IAMM Tool Question Reference: 04.07.05 (v4.0), QUES1677559938109 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is IA embedded within the culture of the IT service management organisation? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: H] • Is there evidence of action being taken by the IT service management organisation to promote IA as an enabler of the business? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: M]	• 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.		A.10.1.1 A.10.1.2 A.6.1.1

5.3 Digital Continuity [Cyber Category Type: Peripheral]

5.3.1 Required Outcome: The business need to maintain access to information over time is met
[Links from 4.5.1; IAMM Tool Question Reference: 04.09.05 (v4.0), QUES1677559938118 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is there a systematic process embedded for reviewing digital continuity risks and mitigation actions on a regular basis, as part of digital information lifecycle management processes? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M]	• Details of policies and procedures, evidence that these processes are implemented.		4.2.1 c) 4.2.2 a) 4.2.3 d)
• Are procedures in place to test accessibility of data over 5 years old to ensure continuity of access to information assets? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: M]	• Details of procedures for testing and reports created post testing.		A.14.1.2 A.15.1.1
• Are policies and procedures in place to ensure that any new IS is assessed for impact on digital continuity and continuity of access to information assets, prior to implementation? [IAMM Tool Evidence Reference: 3 (v4.0); Importance: M]	• Details of policies and procedures for implementing new IS, including change control. • Evidence of relevant staff training and objectives to demonstrate capability.		A.14.1.1
• Has digital continuity risk management been embedded as a key task within the organisation's IA, IT and IM teams as business as usual processes? [IAMM Tool Evidence Reference: 4 (v4.0); Importance: H]	• All IA, IT and IM policies and procedures include digital continuity risk management. • Evidence that retention schedules are being properly implemented.		4.2.1 c)
• Is the organisation sharing best practice and lessons learned about Digital Continuity risk management across government? [IAMM Tool Evidence Reference: 5 (v4.0); Importance: L]	• Evidence of shared experiences amongst relevant communities, feedback to the National Archives.		A.6.1.6 A.6.1.7

5.4 Access Management [Cyber Category Type: Business Critical]

5.4.1 Required Outcome: A cost effective access management regime, that meets the business need, is implemented across the organisation
[Links from 4.6.1; IAMM Tool Question Reference: 04.10.05 (v4.0), QUES1677559938123 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is investment in access management optimised across personnel, physical, procedural and technical aspects and against functional delivery? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M]	• 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.		7 8 A.6.1.1 A.11.1

5.5 Vulnerability Detection [Cyber Category Type: Business Critical]

5.5.1 Required Outcome: Timely action is taken to address vulnerabilities that have potential to disrupt the business
[Links from 4.7.1; IAMM Tool Question Reference: 04.11.05 (v4.0), QUES1677559938128 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does the organisation foster and develop the expertise to detect vulnerabilities in the business context and is effective action taken to act on reports made? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M]	• Details of process to assess vulnerabilities in the business context. • Details of timely remedial action taken to act on vulnerability reports.		A.12.6.1

5.6 Patching [Cyber Category Type: Business Critical]

5.6.1 Required Outcome: Patches are applied in an optimum manner across the ICT estate to safeguard the conduct of the business
[Links from 4.8.1; IAMM Tool Question Reference: 04.12.05 (v4.0), QUES1677559938133 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]
[Modified in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• 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? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: H]	• Details of the automated process and the exception reporting mechanism.		A.10.1.1 A.10.1.2 A.10.10.1
5.7 Lock-Down [Cyber Category Type: Business Critical]			
5.7.1 Required Outcome: ICT infrastructure is locked down to secure configurations that are matched to the business need [Links from 4.9.1; IAMM Tool Question Reference: 04.13.05 (v4.0), QUES1677559938138 (v5.0); Recipient Type: Organisation]			
Areas to Probe	**Evidence Expected**	**Policy Reference**	**ISO27001 Reference**
• Is there a process to continually refine lock-down configurations and processes to minimise IA vulnerabilities? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M]	• Evidence of the process and its effective application.		8.1 A.11
5.8 Anti-Malware Services [Cyber Category Type: Business Critical]			
5.8.1 Required Outcome: The optimum configuration of anti-malware services is enacted to preserve the secure discharge of the organisation's business [Links from 4.10.1; IAMM Tool Question Reference: 04.14.05 (v4.0), QUES1677559938143 (v5.0); Recipient Type: Organisation]			
Areas to Probe	**Evidence Expected**	**Policy Reference**	**ISO27001 Reference**
• Are objectives set for eliminating the root causes of malware incidents and is there an effective funded programme of continuous improvement? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M]	• Realistic objectives are in place with an effective implementation programme.		8.3 A.10.4.1 A.10.4.2

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 board has established its broader IA Road Map for all its information, systems and processes	**Level 5 – Optimised** Responsive IA processes are integrated as Part of Normal Business
The requirement to define and manage how information is shared across the organisation's boundaries is identified. Arrangements are in place to work with external stakeholders to achieve shared IA objectives. The need to understand and control how ICT systems 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 and managing information across these boundaries are defined and implemented, including those with Delivery Partners and 3rd party suppliers. The organisation takes an enterprise-wide approach to the security of new ICT systems and a systematic method is used to implement the control measures needed to mitigate problems when inter-connecting ICT systems.	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 organisation 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 organisational and collective, shared exposure to information risk.

Goal - Information is readily shared within the organisation and with external stakeholders in an assured and cost effective way that maximises the benefits delivered by the Government ICT Strategy 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 ICT system 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

1.1 Information Sharing – Internal [Cyber Category Type: Peripheral]

1.1.1 Required Outcome: The organisation has effective policy and processes in place to manage the risks associated with sharing information within the organisation
[Links to 2.1.1; IAMM Tool Question Reference: 05.01.01 (v3.5/v4.0), QUES1677559938146 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is the business need to share information internally within the organisation understood and is this need embodied in policy statements? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H] • Are the risks associated with sharing information within the organisation understood and managed appropriately? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M]	• Information Sharing Policy statement. • Process exists to assess and manage the risks associated with internal information sharing.	IS1&2 & IS6, GPGs 7, 8, 9, 13, 17, 19, 24, 28, 29 & 35.	A.10.7.3 A.10.8.1 A.10.9.1 4.2.1 d)-g) A.6.2.1

1.2 Information Sharing – External [Cyber Category Type: Business Critical]

1.2.1 Required Outcome: The organisation has effective policies in place that detail how information sharing risks with external parties are to be managed in a collaborative manner
[Links to 2.2.1; IAMM Tool Question Reference: 05.02.01 (v3.5/v4.0), QUES1677559938149 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Are the risks associated with sharing information 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? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H] • Does a mechanism exist to take into account the IA needs of OGDs and stakeholders when handling their information? [IAMM Tool Evidence Reference: 3 & 4 (v3.5/v4.0); Importance: H] • 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? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H]	• Processes exist to assess and manage the risks associated with internal and external information sharing. • Information Sharing Policy statement. • Where inter-organisational working is involved there is evidence that the organisation 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.	IS1&2 & IS6, GPGs 7, 8, 9, 13, 17, 19, 24, 28, 29 & 35.	4.2.1 d)-g) A.6.2.1 A.10.7.3 A.10.8.1 A.10.9.1 A.10.7.3 A.10.8.1 A.10.8.2 A.6.1.3 A.8.1.1

1.3 Information Transfer [Cyber Category Type: Business Critical]

1.3.1 Required Outcome: The organisation has assurance that processes are in place to reduce the risk posed by a failure to secure the transfer of personal data in whatever form throughout the delivery chain
[No links; IAMM Tool Question Reference: 05.03.01 (v3.5/v4.0), QUES1677559938154 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Where an information solution requires the transfer of data, in whatever form, from one system to another, or from one site to another are effective mechanisms in place to protect the information in transit using approved devices in accordance with the IS6 Mandatory Requirements? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H]	• Details of how such remote access links are protected and how assurance is provided of the effectiveness of the protection.	IS1&2, IS4 & IS6, GPGs 3, 5, 7, 9, 10, 19 & 28, Technical Threat Briefing No.1 (TTB1).	A.11.4.2 A.11.5.1 A.15.1.1 A.10.7.3
• Is an effective process in place to ensure the following IS6 Mandatory Requirements are met where portable devices and removable media are used for personal data: a. The minimum necessary information is transferred to meet the business need. [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: M] b. Portable devices and removable media are encrypted in accordance with the standards shown in IS4 (reference [q]) and it is protected by an authentication mechanism such as a password. [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: M] c. User rights to transfer data to portable devices and removable media must be minimised. [IAMM Tool Evidence Reference: 5 (v3.5/v4.0); Importance: M] d. Individuals involved must have completed the mandatory training for handling personal protected data. [IAMM Tool Evidence Reference: 6 (v3.5/v4.0); Importance: M]	• Details of the effective application of policy.		A.10.8.3&4 A.10.7.1 A.10.7.3 A.15.1.1
• How are all staff (within the organisation, its Delivery Partners and its 3rd party suppliers) who are involved in implementing information solutions made aware of the data handling Mandatory Requirements for securing information in transit as detailed in IS6 (reference [c])? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Details of how the policy and arrangements are promulgated to all areas.		5.2.2 A.8.2.1 A.8.2.2
• What assurance mechanism is in place to ensure that the data handling Mandatory Requirements are being applied in all areas? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: M]	• Details of the assurance mechanism in place together with any reports that have been made.		4.2.3 e) 6 A.15.2.1

1.4 Delivery of Services to the Citizen [Cyber Category Type: Business Critical]

1.4.1 Required Outcome: Appropriate and proportionate measures are in place to secure the delivery of services to members of the public
[No links; IAMM Tool Question Reference: 05.04.01 (v3.5/v4.0), QUES1677559938155 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does the organisation understand the need to secure the delivery of citizen facing services (face-to-face, post, e-mail or web based transactions)? Are these requirements embodied in standards that are clearly explained? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M]	• Details of the policies and standards which the organisation has chosen to apply for the delivery of secure services to the citizen.	IS1&2 & IS6, GPGs 7, 8, 9, 19, 28, 43, 44, & 45, Technical Threat Briefing No.1 (TTB1).	A.10.9.1 A.10.9.2 A.10.9.3 A.15.1.4 A.10.7.3 A.10.8.1 A.10.8.2 A.10.8.3 A.10.8.4 A.10.9
• Are the protection measures used, when transacting business with individual citizens, proportionate when compared with the internal protective measures? If not, is there a valid reason for this? [IAMM Tool Evidence Reference: 2 & 3 (v3.5/v4.0); Importance: M]	• Details of the protective measures used and the analysis of why they have been chosen (e.g. the assurances gained are consistent with the organisational requirements from RSDOPS (e.g. IAMM Level 1 organisational maturity for RSDOPS Level 0, IAMM level 2 organisational maturity for RSDOPS Level 1, or IAMM Level 3 organisational maturity for RSDOPS Level 2)).		

1.5 Enterprise-Wide, Architectural Approach to IA [Cyber Category Type: Supporting]

1.5.1 Required Outcome: The organisation is committed to taking an enterprise-wide, coordinated approach to IA based on a defined security architecture that meets the business need
[Links to 2.3.1; IAMM Tool Question Reference: 05.05.01 (v3.5/v4.0), QUES1677559938156 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does the SIRO understand the operational and financial benefit of adopting an enterprise wide, coordinated approach to IA based on a defined security architecture rather than implementing piecemeal controls on a system by system basis? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Policy papers examining the need for an enterprise-wide, architectural approach exist.	IS1&2 & IS6, GPGs 6, 7, 8, 13, 17, 19, 28, 29 & 35.	4.2.1 A.12.1.1
• Does a plan exist for the organisation to migrate its infrastructure to a security architecture that meets the business need? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M]	• Details of the plan of how the organisation is to migrate from the status quo to an architecturally compliant regime.		4.2.2

1.6 Network Security Management [Cyber Category Type: Business Critical]

1.6.1 Required Outcome: The organisation, its Delivery Partners and its 3rd party suppliers have implemented all of the mandatory security controls required by codes-of-connection; bilateral agreements and/or community or shared service security policies. In addition, the organisation has plans to gain assurance throughout its delivery chain that the implementation is effective
[Links to 2.4.1; IAMM Tool Question Reference: 05.06.01 (v3.5/v4.0), QUES1677559938160 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does the organisation, its Delivery Partners and its 3rd party suppliers comply with all codes-of-connection, bilateral agreements and/or community or shared service security policies to which they are signatories. [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Details of how compliance is achieved.	IS1&2 & IS6, GPGs 6, 7, 8, 9, 13, 17, 19, 28, 29 & 35.	A.10.6 A.10.8.5 A.11.4.6
• Are the specific technical policies covering; patching, malware, boundary security devices, content checking/blocking and lockdown applicable to such agreements implemented effectively? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H]	• Evidence that the mandatory technical controls relating to such agreements are applied correctly.		A.10.4.1&2 A.11.4 A.12.6.1
• Similarly, are the required physical and personnel measures applicable to such agreements implemented effectively?	• Evidence that the mandatory physical and personnel controls relating to such agreements are applied correctly.		A.15.2 A.8 A.9
• Is the need to assure the compliance and effectiveness of these arrangements understood and is there a plan to introduce the necessary arrangements? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: M]	• Evidence of plans to assure the compliance and effectiveness of all Codes of Connection.		A.15.2.1 A.15.2.2

1.7 Protective Monitoring (e.g. IPS, IDS etc.) [Cyber Category Type: Business Critical]

1.7.1 Required Outcome: A limited view of cyber related events is provided by a rudimentary protective monitoring (IDS, IPS etc.) capability
[Links to 2.5.1; IAMM Tool Question Reference: 05.07.01 (v3.5/v4.0), QUES1677559938165 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is the organisation aware of CESG GPG No: 8, Protecting External Connections to the Internet (reference [r])and CESG GPG No:13, Protective Monitoring for HMG ICT Systems (reference [s]) • What protective monitoring capabilities does the organisation employ? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M] • Are they effective and are the events generated audited and incidents responded to? [IAMM Tool Evidence Reference: Also 1 (v3.5/v4.0); Importance: M] • Does the organisation rely exclusively on boundary devices, or are protective monitoring resources deployed internally to detect anomalous activity? • If protective monitoring resources are deployed internally, are they applied at all appropriate levels of computer and data access (i.e. applications, infrastructure as well at the networks)? • Has a risk analysis been conducted to identify weaknesses in the existing protective monitoring regime? • Does the SIRO understand the benefits of investing in protective monitoring? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H] • Does a plan exist to investigate the introduction of a comprehensive, corporate protective monitoring regime? [IAMM Tool Evidence Reference: Also 2 (v3.5/v4.0); Importance: H]	• Understanding of the principles and practice of effective protective monitoring. • Details of current capability. • Details of how the capabilities are used. • Deployment details of existing resources indicating their use in an effective manner to detect anomalous activity. • An understanding that for optimum monitoring protective monitoring, resources need to be deployed throughout the information stack. • Risk analysis. • Policy papers examining the need for enhancing protective monitoring. • Details of the plan.	IS1&2 & IS6, GPGs 6, 7, 8, 9, 13, 17, 19, 24, 28, 29 & 35.	A.15.2.1 4.2.2 h) A.10.6.1 8.2 & 8.3 A.10.10 A.13.2.2 A.10.4 A.11.4 A.11.5 A.11.6 4.2.1 e) 5.2.1 8.1

LEVEL 2 – Established - IA Processes are Institutionalised

2.1 Information Sharing – Internal [Cyber Category Type: Peripheral]

2.1.1 Required Outcome: The risks associated with sharing business critical Information within the organisation are known and are managed effectively
[Links from 1.1.1 and to 3.1.1; IAMM Tool Question Reference: 05.01.02 (v3.5/v4.0), QUES1677559938147 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is the process to manage information sharing risks within the organisation been applied effectively to the business critical activities? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Clear evidence of its application, together with plans to provide the information needed at Level 3.	IS1&2 & IS6, GPGs 7, 8, 9, 13, 17, 19, 24, 28, 29 & 35.	4.2.1 d)-g)

2.2 Information Sharing – External [Cyber Category Type: Business Critical]

2.2.1 Required Outcome: Information sharing agreements are underpinned by joint information risk management processes and the effective implementation of technical controls at all boundary points
[Links from 1.2.1 and to 3.2.1; IAMM Tool Question Reference: 05.02.02 (v3.5/v4.0), QUES1677559938150 (v5.0); Recipient Type: Organisation]
[Modified in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does the organisation understand the need to, and value of, keeping the stakeholders with whom they share information informed of how they apply IRM and manage information generally? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M]	• Information sharing agreements with other organisations contain evidence to show an open and collaborative approach to dealing with IRM and IM issues.	IS1&2 & IS6, GPGs 7, 8, 9, 13, 17, 19, 24, 28, 29 & 35.	5.1.d) A.6.1.6 A.6.1.7

• Is an effective assurance regime in place to ensure that the organisation's information sharing policy is being applied in a way that meets the business needs of the organisation? • Has that assurance regime been endorsed by the SIRO and/or the Main Board? • Are all network boundaries with the organisation's ICT systems throughout the delivery chain clearly identified and defined? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H] • Are the policies for sharing information across these boundaries clearly defined? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: H] • Are there boundary control devices (e.g. firewalls) installed on all ICT systems with untrusted networks, such as the Internet? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: H] • 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? [IAMM Tool Evidence Reference: 5, 6, 7 & 8 (v3.5/v4.0); Importance: 5,6-H, 7,8-M] • 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 relevant boundaries? IAMM Tool Evidence Reference: 9 (v3.5/v4.0); Importance: M]	• Details of the assurance regime and how it works in practice. • Senior management engagement that establishes that they understand the risks. • 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		A.15.2.1 6 c) A.10.6 A.10.8.1 A.10.8.2 A.10.8.5 A.11.4.6 A.6.1.4 A.9.2.4 A.10.10.1 A.10.10.2 A.10.10.3 A.13.1 A.11.2.2 A.11.6.1

2.3 Enterprise-Wide, Architectural Approach to IA [Cyber Category Type: Supporting]

2.3.1 Required Outcome: The organisation has defined a target security architecture that is aligned to the needs of the business. Where appropriate, ICT infrastructure is being brought into architectural compliance
[Links from 1.5.1 and to 3.3.1; IAMM Tool Question Reference: 05.05.02 (v3.5/v4.0), QUES1677559938157 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Has an enterprise-wide security architecture been specified that accurately reflects what the organisation needs in order to discharge its business both now and in the future, particularly as it seeks to take account of HMG ICT initiatives? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H] • Is the enterprise-wide security architecture being used as a goal against which future programmes are specified? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M] • Is the security architecture endorsed by the business? • Are new initiatives checked for compliance with the architecture before implementation? • Is architectural compliance specified when procuring new ICT systems? • Do plans exist to migrate the existing ICT infrastructure to a state of architectural compliance? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: L]	• Details of enterprise security architecture and the methodology used to create the architecture, including how it relates to business drivers and HMG ICT initiatives. • Endorsement of an enterprise-wide, architectural approach by the Main Board. • Details of how the enterprise security architecture is used in new initiatives. • Details of how the enterprise security architecture is used in practice. • Details of the plans to bring the whole of the legacy ICT infrastructure into architectural compliance.	IS1&2 & IS6, GPGs 6, 7, 8, 13, 17, 19, 28, 29 & 35.	4.2.1 g) A.12.1.1 A.6.1.7 4.2.2 A.12.1.1 A.6.1.4 8.2

2.4 Network Security Management [Cyber Category Type: Business Critical]

2.4.1 Required Outcome: The organisation's data networks are proactively managed so that security issues are addressed in a comprehensive and timely manner, thereby minimising the disruption to the business
[Links from 1.6.1 and to 3.4.1; IAMM Tool Question Reference: 05.06.02 (v3.5/v4.0), QUES1677559938161 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does the organisation have a Network Management Board, or similar body, with clear lines of authority that takes decisions on key network issues, such as those relating to architecture? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: H]	• TORs and minutes of Network Management Board.	IS1&2 & IS6, GPGs 7, 8, 9, 13, 17, 19, 24, 28, 29 & 35.	7 A.6.1.2
• Are significant network management policies endorsed by the SIRO? [IAMM Tool Evidence Reference: Also 3 (v3.5/v4.0); Importance: H]	• Details of how the SIRO interacts with the Network Management Board.		A.6.1.3
• Are all codes-of-connection, bilateral agreements and/or community or shared service security policies subject to an effective regime to assure compliance? [IAMM Tool Evidence Reference: 1 & 2 (v3.5/v4.0); Importance: 1-H, 2-M]	• Details of the compliance methodology and any measures of its effectiveness e.g. audit.		A.11.4.6 A.15.2
• Are processes for controlling access and configuration institutionalised and do these follow established change control procedures? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: M]	• Evidence that Network Security Management is an accepted discipline in the working practices of the Organisation.		A.11.4.1

2.5 Protective Monitoring (e.g. IPS, IDS etc.) [Cyber Category Type: Business Critical]

2.5.1 Required Outcome: The organisation has confidence that its existing protective monitoring resources are deployed in a way that maximises their potential and that their output is exploited in a way that gives the organisation a good understanding of cyber events. Where the business risk warrants it, plans are in place to implement a more comprehensive protective monitoring capability
[Links from 1.7.1 and to 3.5.1; IAMM Tool Question Reference: 05.07.02 (v3.5/v4.0), QUES1677559938166 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Has the organisation assessed what it does to address the twelve protective monitoring controls listed in GPG 13 (reference [s]) and whether this is adequate to meet the needs of the business?	• Details of an assessment undertaken by the organisation that indicates they have assessed what they do against the GPG.	IS1&2 & IS6, GPGs 6, 7, 8, 9, 13, 17, 19, 24, 28, 29 & 35.	A.15.2.1 7.2 c) A.10.6.1
• Are objectives set for the use of existing protective monitoring resources? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: L]	• Evidence of systematic employment of protective monitoring devices to achieve a desired effect.		8.2 8.3
• Are processes in place to make effective use of protective monitoring resources at network boundaries and are these processes institutionalised? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M]	• Evidence that the use of protective monitoring devices deployed at the boundaries is built into the working practices of the organisation.		A.10.6.1 A.10.10.2
• Where protective monitoring resources are deployed internally to detect anomalous activity, are similar processes in place to make effective use of them and are these processes institutionalised?	• Evidence that the use of protective monitoring devices deployed internally is built into the working practices of the organisation.		
• Are the outputs from the protective monitoring devices being monitored? Is this done in real, or near real-time?	• Evidence that there is a quick and effective response by the monitors.		A.13.2.1
• Are the staff who monitor the outputs from the protective monitoring resources trained effectively to interpret the results? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H]	• Details of the skills levels and turnover of the staff involved in interpreting the data.		5.2.2 A.8.2.2
• Where the business risk warrants the investment, has a plan to implement a comprehensive, corporate protective monitoring regime been endorsed, funding allocated, and being taken forward? [IAMM Tool Evidence Reference: 5 (v3.5/v4.0); Importance: H]	• Details of the plan to implement a holistic protective monitoring scheme.		8.1
• Has use been made of the CESG Intrusion Detection Service (IDS)? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: L]	• Details of any reports provided by CESG, together with details of any resulting action taken.		A.6.1.6 A.6.1.7

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

3.1 Information Sharing – Internal [Cyber Category Type: Peripheral]

3.1.1 Required Outcome: The risks to information flows and the information assets involved in supporting business critical processes are known and are managed to minimise their impact
[Links from 2.1.1; IAMM Tool Question Reference: 05.01.03 (v3.5/v4.0), QUES1677559938148 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Are the information flows that support critical business activities known? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M] • Have these information flows been analysed to determine where there are key dependencies on specific elements of the infrastructure? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M] • Has a risk analysis been undertaken to minimise the risk posed by potential single points of failure? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: H] • Is there sufficient linkage between the need to maintain information flow to support the business and the IA situational awareness activity, so that the IA response is driven by the needs of the business? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: H]	• Documentary evidence that the critical information flows are known, together with the details of the information assets that flow through them. • 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.	IS1&2 & IS6, GPGs 7, 8, 9, 13, 17, 19, 24, 28, 29 & 35.	4.2.1 d) A.10.8.5 A.12.1.1 4.2.1 e) A.10.3.1 A.11.4.7 A.12.6.1 A.14.1.2 A.6.1.2 A.10.6 A.11.4.7

3.2 Information Sharing – External [Cyber Category Type: Business Critical]

3.2.1 Required Outcome: The SIRO has assurance that the risks associated with external information sharing are acceptable to the business
[Links from 2.2.1 and to 4.1.1 and 4.1.2; IAMM Tool Question Reference: 05.02.03 (v3.5/v4.0), QUES1677559938151 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• How does the SIRO gain assurance that the risks associated with external information sharing are acceptable to the business? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M]	• Assurance reports detailing the effectiveness of the IA controls implemented to control external information sharing risks.	IS1&2 & IS6, GPGs 7, 8, 9, 13, 17, 19, 24, 28, 29 & 35.	4.2.3 a) 3)

3.3 Enterprise-Wide, Architectural Approach to IA [Cyber Category Type: Supporting]

3.3.1 Required Outcome: ICT security controls are implemented in a coordinated, cost-effective and architecturally compliant way across the organisation providing a layered defence that increases the protection afforded to business critical ICT systems
[Links from 2.3.1; IAMM Tool Question Reference: 05.05.03 (v3.5/v4.0), QUES1677559938158 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Are key parts of the organisation's ICT infrastructure compliant with the target security architecture, thereby enabling the organisation to respond to cyber threats in a proportionate way that maintains the integrity of business critical ICT systems? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H] • Does a central authority exist to control the granting of waivers to non compliant IS? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: L]	• Evidence to show that those parts of the ICT infrastructure that support business critical processes are compliant with the target security architecture. • Details of the control exercised to maintain compliance with the enterprise security architecture.	IS1&2 & IS6, GPGs 6, 7, 8, 13, 17, 19, 28, 29 & 35.	A.15.2.1 4.3.1 c) A.15.2.1

• Is the level of compliance with the security architecture known and managed? [IAMM Tool Evidence Reference: 2 and 3 (v3.5/v4.0); Importance: 2-M, 3-L] • Where there is a business justification, has the organisation initiated work to bring other parts of the ICT estate into architectural compliance? • Is there a process for sharing the organisation's approach to security architecture with external stakeholders and particularly with the members of the CTO Council? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: L]	• Non-compliances are known and are managed through the central authority. • Details of the plan. • Details of liaison with external stakeholders and any assessment of the compatibility of the organisation's architectural approach with the approach that has been endorsed by the CTO Council.		A.15.2.2 8.1 A.6.1.6 A.6.1.7

3.4 Network Security Management [Cyber Category Type: Business Critical]

3.4.1 Required Outcome: The design of the organisation's networks is compliant with the security architecture and they are managed in a way that preserves the operation of business critical ICT systems in the event that the organisation suffers a cyber attack
[Links from 2.4.1 and to 4.3.1; IAMM Tool Question Reference: 05.06.03 (v3.5/v4.0), QUES1677559938162 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Are network security management policies implemented in a structured manner to provide defence in depth? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M] • Is the planning of change based on a sound understanding of network vulnerabilities and the potential business impacts? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H] • Are attempts to intrude, whether successful or not, detected and managed? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: M]	• 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 ICT capability. • Evidence of detection of live threats and results of penetration testing of capability.	IS1&2 & IS6, GPGs 6, 7, 8, 9, 13, 17, 19, 28, 29 & 35.	A.5.1.1 A.10.1.1 A.10.6 A.10.1.2 A.10.6.2 A.11.4.6 A.12.6.1

3.5 Protective Monitoring (e.g. IPS, IDS etc.) [Cyber Category Type: Business Critical]

3.5.1 Required Outcome: The organisation is able to take timely, effective and proportionate action to preserve its business critical operations through the provision of enhanced situational awareness of the cyber environment
[Links from 2.5.1 and to 4.4.1; IAMM Tool Question Reference: 05.07.03 (v3.5/v4.0), QUES1677559938167 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Where the business risk warrants it, does a comprehensive, corporate protective monitoring capability exist? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H] • Does it provide situational awareness, not only of the network, including all boundary points, but also at all appropriate levels of computer and data access (i.e. applications, infrastructure)? [IAMM Tool Evidence Reference: Also 1 (v3.5/v4.0); Importance: H]	• Details of the corporate protective monitoring capability and how it provides effective situational awareness.	IS1&2 & IS6, GPGs 6, 7, 8, 9, 13, 17, 19, 24, 28, 29 & 35.	A.10.6.1 8.2 & 8.3 A.10.10.1 A.13.2.2 A.10.6.2
• Are anomaly detection techniques used to determine when and where preventative action needs to be taken to preserve the security of business critical operations? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M]	• Details of how anomaly detection is used.		A.12.6.1
• Is there effective engagement with CESG regarding the collection and supply of Intrusion Detection System (IDS) threat signatures? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: M]	• Details of the engagement and the use being made of the information supplied.		A.6.1.6
• 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 across HMG?	• Details of the interaction with OGDs with similar capabilities, together with external sources of expertise.		A.6.1.7 A.10.8.2

[IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: H]			

LEVEL 4 – Quantitatively Managed –
The board has established its broader IA Road Map for all its information, systems and processes

4.1 Information Sharing – External [Cyber Category Type: Business Critical]

4.1.1 Required Outcome: Relationships with external information sharers are such that they are prepared to expose the true nature of the information risk they pose to the organisation
[Links from 3.2.1; IAMM Tool Question Reference: 05.02.04 (v4.0), QUES1677559938152 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Experience shows that an information sharing assurance regime that relies solely on compliance checking is only partially effective. Has the organisation learned that to expose the true risks created by information sharing, it is necessary to work with external parties in a collaborative way to engender trust? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M]	• The compliance regime is augmented by mechanisms to engender trust so that there is a greater willingness by external parties to reveal the true nature of the information risk they pose to the organisation. • Evidence of mature processes that allow information sharing.	IS1&2 & IS6, GPGs 7, 8, 9, 13, 17, 19, 24, 28, 29 & 35.	A.6.2

4.1.2 Required Outcome: Formal arrangements are in place to allow adequate levels of assurance with (commercial and public service) information sharers
[Links from 3.2.1; IAMM Tool Question Reference: 05.02.05 (v4.0), QUES1677559938153 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]
[New in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Are there appropriate contracts, or appropriate "Memoranda of Understanding" (MoU), in place? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M]	• Adequate documentation of the information sharing arrangements in appropriate contracts, or MoU.	IS1&2 & IS6, GPGs 6, 7, 8, 13, 17, 19, 24, 28, 29 & 35.	A.6.2

4.2 Enterprise-Wide, Architectural Approach to IA [Cyber Category Type: Supporting]

4.2.1 Required Outcome: The organisation's architectural approach remains aligned to the changing needs of the business and the changing threat environment
[Links from 3.3.1; IAMM Tool Question Reference: 05.05.04 (v4.0), QUES1677559938159 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Has the organisation's architectural approach to security been critically examined to ensure that it meets the continuing needs of the business (and aligned with the defined risk appetite) and is responsive to the requirements that stem from the latest threats? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: H]	• Details of the review process (that are occurring periodically) and any changes that resulted from it.	IS1&2 & IS6, GPGs 6, 7, 8, 13, 17, 19, 24, 28, 29 & 35.	7

4.3 Network Security Management [Cyber Category Type: Business Critical]

4.3.1 Required Outcome: The design of the organisation's networks is compliant with the security architecture and they are managed in a way that preserves the operation of all relevant ICT systems in the event that the organisation suffers an attack (e.g. a cyber attack)
[Links from 3.4.1 and to 5.1.1; IAMM Tool Question Reference: 05.06.04 (v4.0), QUES1677559938163 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties][New in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Are the organisation's networks security managed such that they preserve, in accordance with the risk appetite, the operation of relevant ICT systems in the event of an attack (e.g. cyber attack)? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M] • Is a process in place to collate all data on system and network incidents and problems? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: M] • Are the organisation's networks compliant with the security architecture? [IAMM Tool Evidence Reference: 3 (v4.0); Importance: M] • Is there an effective post incident and problem analysis process? [IAMM Tool Evidence Reference: 4 (v4.0); Importance: M] • Are the lessons identified in this analysis used effectively to tune the response to future situations? [IAMM Tool Evidence Reference: 5 (v4.0); Importance: L] • Is there effective reporting to the SIRO and the Main Board? [IAMM Tool Evidence Reference: 6 (v4.0); Importance: H] • Is the investment in network security management perceived by the Main Board as providing value-for-money? [IAMM Tool Evidence Reference: 7 (v4.0); Importance: M] • Is the organisation engaged in an effective interchange of data with external stakeholders? [IAMM Tool Evidence Reference: 8 (v4.0); Importance: M] • Are network security management policies implemented in a structured manner to provide defence in depth? [IAMM Tool Evidence Reference: 9 (v3.5/v4.0); Importance: M] • Is the planning of change (e.g. including those to new, or existing, shared-services) based on a sound understanding of network vulnerabilities and the potential business impacts? [IAMM Tool Evidence Reference: 10 (v3.5/v4.0); Importance: H] • Are attempts to intrude, whether successful or not, detected and managed? [IAMM Tool Evidence Reference: 11 (v3.5/v4.0); Importance: M]	• Documentation, and testing results, depict the aspects of the network security management facilities that preserve system operation (e.g. effective when live threats are detected, and during penetration testing of this capability). • Details of the collation process and evidence of the effective use of the process. • Evidence of compliance, and how the network security management organisation interacts with those delivering new and existing (including non-critical, but relevant) ICT capability. • Evidence of effective use of the processes. • Evidence that lessons are "learned" and appropriate action taken. • Evidence of SIRO engagement. • Reports presented to the Main Board to demonstrate how network security management enables the business. • Evidence of a willingness to be open and share data and experience with external stakeholders. • 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 ICT capability. • Evidence of detection of live threats and results of penetration testing of capability.	IS1&2 & IS6, GPGs 6, 7, 8, 9, 13, 17, 19, 24, 28, 29 & 35.	8.3 A.13.2 A.13.2 8.1 8.2 8.3 A.13.2.2 7.1 7.2 7.3 A.6.1.6 A.6.1.7

4.4 Protective Monitoring (e.g. IPS, IDS etc.) [Cyber Category Type: Business Critical]

4.4.1 Required Outcome: Timely Action is taken to manage cyber events in a way that maintains the delivery of business outputs
[Links from 3.5.1 and to 5.2.1; IAMM Tool Question Reference: 05.07.04 (v4.0), QUES1677559938168 (v5.0); Recipient Type: Organisation]
[New in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does the protective monitoring regime provide a 24/7 incident management capability? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M] • Are the processes and procedures in place to take advantage of real-time indicators and warnings, so that proactive defensive action can be taken? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: M] • Is a process in place to collate all data on system and network incidents and problems? [IAMM Tool Evidence Reference: 3 (v4.0); Importance: M]	• 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.	IS1&2 & IS6, GPGs 6, 7, 8, 9, 13, 17, 19, 24, 28, 29 & 35.	8.3 A.13.2 A.13.2 8.1 8.2 8.3 A.13.2.2 7.1 7.2

• Is this data used to provide real-time incident and problem management? [IAMM Tool Evidence Reference: 4 (v4.0); Importance: M] • Is there an effective post incident and problem analysis process? [IAMM Tool Evidence Reference: 5 (v4.0); Importance: M] • Are the lessons identified in this analysis used effectively to tune the response to future situations? [IAMM Tool Evidence Reference: 6 (v4.0); Importance: L] • Is there effective reporting to the SIRO and the Main Board? [IAMM Tool Evidence Reference: 7 (v4.0); Importance: H] • Is the investment in protective monitoring perceived by the Main Board as providing value-for-money? [IAMM Tool Evidence Reference: 8 (v4.0); Importance: M] • Is the organisation engaged in an effective interchange of data with external stakeholders? [IAMM Tool Evidence Reference: 9 (v4.0); Importance: M]	• Evidence of the effective use of the data to act proactively when problems arise and react in a timely manner to incidents. • Evidence of effective use of the processes. • Evidence that lessons are "learned" and appropriate action taken. • 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.		7.3 A.6.1.6 A.6.1.7

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

5.1 Network Security Management [Cyber Category Type: Business Critical]

5.1.1 Required Outcome: The organisation's Network Security measures are routinely updated and refreshed to cater for changes in the threat
[Links from 4.3.1; IAMM Tool Question Reference: 05.06.05 (v4.0), QUES1677559938164 (v5.0); Recipient Type: Organisation][New in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is there a continuous improvement plan to update the network security management environment to match the changing threat environment? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M] • Are measures in place to measure the effectiveness of the investment in network security management, as a means to facilitating the trust needed for effective information sharing? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: M]	• Plan to maintain the effectiveness of the capability. • Metrics to establish value for money.	IS1&2, IS6, GPG 6, 7, 8, 9, 13, 17, 19, 28, 29, 35.	8.1 8.2 8.3 A.13.2.2 8.1 8.2 8.3

5.2 Protective Monitoring (e.g. IPS, IDS etc.) [Cyber Category Type: Business Critical]

5.2.1 Required Outcome: The organisation's Protective Monitoring measures are routinely updated and refreshed to cater for changes in the threat
[Links from 4.4.1; IAMM Tool Question Reference: 05.07.05 (v4.0), QUES1677559938169 (v5.0); Recipient Type: Organisation][New in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is there a continuous improvement plan to update the protective monitoring processes and equipment to match the changing threat environment? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: M] • Are measures in place to measure the effectiveness of the investment in protective monitoring to be seen as an enabler for information sharing? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: M]	• Plan to maintain the effectiveness of the capability. • Metrics to establish value for money.	IS1&2, IS6, GPG 6, 7, 8, 9, 13, 17, 19, 28, 29, 35.	8.1 8.2 8.3 A.13.2.2 8.1 8.2 8.3

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 board has established its broader IA Road Map for all its information, systems and processes	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 Main Board's Audit Committee ensures that it receives comprehensive assurance on IRM and challenges assurance, where required. The organisation reports annually on IA issues.	The organisation 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 and standards.	Critical IA Review and internal audit recommendations are actioned and progress tracked.	IA practices are fully assured by internal audit. Main Board is aware of the significant areas of the organisation's non-compliance with the HMG SPF and national policy and standards. Remedial action has been undertaken.	There are no critical or significant IA audit issues. Independent assessment of the organisation's approach to IA shows that it is aligned with the relevant Strategies (e.g. the National Security Strategy) and it is fully compliant with the HMG SPF and national policy and standards. It is considered to be an exemplar of best practice across HMG.

Goal - Effective compliance mechanisms provide positive assurance that organisational 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 organisation's information.

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

1.1 Establishing a Compliance Regime [Cyber Category Type: Peripheral]

1.1.1 Required Outcome: The organisation knows and accepts its obligation to implement all appropriate laws relating to IRM throughout its delivery chain and it has established a compliance regime to provide assurance that it is not in breach of its statutory obligations
[No links; IAMM Tool Question Reference: 06.01.01 (v3.5/v4.0), QUES1677559938170 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• What action has the organisation taken to understand what it needs to do to comply with all relevant information related legislation? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H] • Has the organisation put in place a compliance regime throughout its delivery chain to assure itself that it is not in breach of its statutory obligations? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H]	• Translation of legislative requirements into the policy, plans and procedures of the organisation. • Details of the IRM compliance regime.	IS1&2 & IS6. GPGs 6, 19 & 28	4.2.3 a)-f) A.15.1

1.1.2 Required Outcome: The organisation knows and accepts the mandatory HMG security policy requirements that it must implement to establish effective IRM throughout its delivery chain. It has established a compliance regime to provide assurance that it is not in breach of its obligations
[Links to 2.1.1; IAMM Tool Question Reference: 06.01.02 (v3.5/v4.0), QUES1677559938171 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• What action has the organisation taken to understand what it needs to do to comply with mandatory HMG information security policy? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H] • Has the organisation put in place a compliance regime throughout its delivery chain to assure itself that it is not in breach of its mandatory obligations? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H]	• Translation of mandatory HMG Information security policy requirements into the policy, plans and procedures of the organisation. • Details of the IRM compliance regime.	IS1&2 & IS6. GPGs 6, 19 & 28	4.2.3 a)-f) A.15.2

1.1.3 Required Outcome: The organisation's IRM policy builds on the legal and HMG mandatory security requirements to establish an IRM policy which is matched to the needs of the business. It has established a compliance regime to provide assurance that its IRM policy is being implemented satisfactorily
[No links; IAMM Tool Question Reference: 06.01.03 (v3.5), 06.01.04 (v4.0), QUES1677559938173 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• What form of compliance regime exists within the organisation and throughout its delivery chain to assure itself that all actions are in compliance with the endorsed IRM policy? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Details of the IRM compliance regime.	IS1&2 & IS6. GPGs 6, 19 & 28	4.2.3 a)-f) A.15

1.2 Assurance Activities [Cyber Category Type: Supporting]

1.2.1 Required Outcome: A series of internal and, where appropriate, external audits of the organisation's IA control measures are undertaken to assess their efficacy
[Links to 2.2.1; IAMM Tool Question Reference: 06.02.01 (v3.5/v4.0), QUES1677559938174 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does the organisation 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). [IAMM Tool Evidence Reference: 1, 2 & 3 (v3.5/v4.0); Importance: 1-H, 2-L, 3-L] • Where considered appropriate, has an external audit been undertaken of the efficacy of the organisation's IA control measures (e.g. ISO/IEC 27001:2005 Assessment, or alternative)? Are the control measures compliant with national policy? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: M]	• Details of compliance checks • Sample RMADS • Audit report or ISO/IEC 27001:2005 assessment report.	IS1&2 & IS6. GPGs 6, 13, 19, 28 & 30	6 4.3 6 A.6.1.8 A.15.2.1

1.2.2 Required Outcome: The SIRO is content that the compliance regime which is in place is sufficient to assure IRM legislative compliance and where required, work is in hand to address deficiencies regarding compliance with mandatory HMG policy requirements. In both instances, the compliance regime requirement applies throughout the organisation's delivery chain
[Links to 2.2.2; IAMM Tool Question Reference: 06.02.04 (v3.5), 06.02.06 (v4.0), QUES1677559938179 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• How does the SIRO satisfy themselves that the organisation, its Delivery Partners and its 3rd party suppliers are compliant with relevant legislation? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M]	• Details of any assessment that has been undertaken.	IS1&2 & IS6. GPGs 6, 13, 19, 28 & 30	A.15.1
• Has this compliance been independently tested?	• Evidence of Legal Advisor involvement with the Assessment Report.		A.6.1.8
• Is the organisation, its Delivery Partners and its 3rd party suppliers fully compliant with the SPF Mandatory Requirements, including those data handling measures detailed in IS6? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H]	• Reports to the SIRO on SPF compliance.		8.2 A.15.1.1 A.15.1.4
• If it is not, does the SIRO know which SPF mandatory measures have not been met and is he content to accept the risk? [IAMM Tool Evidence Reference: Also 2 (v3.5/v4.0); Importance: H]	• Details of risk assessments supporting decision.		5.1 f)
• How does the SIRO ensure the effectiveness of the compliance regime? [IAMM Tool Evidence Reference: Also 1 (v3.5/v4.0); Importance: M]	• Details of any assessments undertaken on the sufficiency of the compliance regime.		4.2.3 a)-f)

1.3 Assuring the Compliance Regime [Cyber Category Type: Peripheral]

1.3.1 Required Outcome: The Audit Committee considers IRM as an integral part of the organisation's overall risk management regime and provides an informed judgement of its efficacy in its annual report to the Accounting Officer
[Links to 2.3.1; IAMM Tool Question Reference: 06.03.01 (v3.5/v4.0), QUES1677559938184 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does a process exist to provide the Audit Committee with details of the key information risks facing the organisation? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M]	• Details of the process.	IS1&2 & IS6. GPGs 19, 28 & 30	4.2.3 d)
• Do members of the Audit Committee, particularly the NEDs, take action to gain a full understanding of the implications to the business of the key information risks facing the organisation? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M]	• Informed engagement by the Audit Committee and the NEDs.		5.1 f)
• Does the Audit Committee consider IRM as an integral part of the organisation's overall risk management regime? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: H]	• Audit Committee minutes.		5.1
• Has the organisation's Information Risk Assessment been shared with, and discussed by the Audit Committee and the Main Board as required by IS6 (reference [c])? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: H]	• Main Board Minutes and briefing notes.		4.2.1 h) 4.2.3 c) 4.2.3 d) 4.2.3 e)
• How does the Audit Committee gain positive assurance of the statements on Information Risk which are included in the Governance Statement and the organisation's Annual Report? [IAMM Tool Evidence Reference: 5 (v3.5/v4.0); Importance: M]	• Details of audits used to provide assurance of annual Governance Statement and Annual Report information.		
• Is the summary, or equivalent material, concerning information risk contained set out in the departmental annual report, compliant with the IS6 (reference [c]) requirement? [IAMM Tool Evidence Reference: 6 (v3.5/v4.0); Importance: L]	• Annual Report on the organisation includes summary, or equivalent, material on information risk, covering the overall judgement in the annual Governance Statement, 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.		A.15.1.1

LEVEL 2 – Established - IA Processes are Institutionalised

2.1 Establishing a Compliance Regime [Cyber Category Type: Peripheral]

2.1.1 Required Outcome: There are periodic reviews of the compliance regime to identify new areas of compliance that require establishment
[Links from 1.1.2; IAMM Tool Question Reference: 06.01.03 (v4.0), QUES1677559938172 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties]
[New in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• What action has the organisation taken to understand what it needs to do to comply with the evolution of all relevant information related legislation? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: H]	• Maintenance of the translation of mandatory HMG Information security policy requirements into the policy, plans and procedures of the organisation.	IS1&2 & IS6. GPGs 6, 19 & 28	4.2.3 a)-f) A.15.1.1
• Has the organisation reviewed its compliance regime, throughout its delivery chain, to assure itself that it maintains its statutory obligations? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: H]	• Details of the changes to the IRM compliance regime in response to relevant change in statutory obligations.		
• Has the organisation considered the impact on the compliance regime due to changes in endorsed IRM policy (e.g. in response to utilising shared services)? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: H]	• Details of the changes to the IRM compliance regime.		
• Has the compliance regime been adjusted to account of organisational changes (e.g. a reorganisation, and/or maintenance of the skills base to ensure the health of the compliance regime)? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: H]	• Evidence that the compliance regime has been reviewed, and if required it was adapted, in response to organisational changes, so that it remains effective.		

2.2 Assurance Activities [Cyber Category Type: Supporting]

2.2.1 Required Outcome: Independent internal and, where appropriate, external audits of the IA control measures within the organisation and its delivery chain are undertaken to assess their efficacy
[Links from 1.2.1 and to 3.1.1; IAMM Tool Question Reference: 06.02.02 (v3.5/v4.0), QUES1677559938175 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Has an independent assessment been conducted of the effectiveness of the IRM regime within the organisation, its Delivery Partners and its 3rd party suppliers? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M]	• Assessment Report.	IS1&2 & IS6. GPGs 6, 13, 19, 28 & 30	6 A.6.1.8
• Did this independent assessmentinclude an assessment of the compliance of the organisation and its delivery partner's and 3rd party suppliers with the mandatory measures contained in Tier 3 of the SPF, particularly those relating to IA? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H]	• Assessment Report of SPF compliance.		A.15.1.1 A.10.2.1 A.10.2.2
• Was that assessment conducted by suitably qualified personnel and where industry is involved, from a legally separate organisation? [IAMM Tool Evidence Reference: Also 1 (v3.5/v4.0); Importance: H]	• Details of who conducted the assessment.		A.15.1.1 A.6.2.3 5.2.2
• Was the assessment comprehensive enough in terms of its breadth, depth to ensure that the IRM measures that are put in place comply with endorsed policy? [IAMM Tool Evidence Reference: Also 1 (v3.5/v4.0); Importance: H]	• Details of the scope of the assessment.		4.2.3 a)-f) 6 & 7
• 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? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: M]	• Details of what action has been taken.		A.15.2.1 8
• When was the last independent IA Benchmarking Review, or similar review,	• IA Benchmark Review Report, or the report of similar review together with follow-		4.2.4 8

conducted? [IAMM Tool Evidence Reference: 4 (v3.5/v4.0); Importance: M] • Have the recommendations from that Review been acted upon? [IAMM Tool Evidence Reference: 5 (v3.5/v4.0); Importance: M]	up action plan		A.6.1.8

2.2.2 Required Outcome: The SIRO has gained independent assurance of the effective operation of the information risk management compliance regime operating within the organisation, its Delivery Partners and its 3rd party suppliers. Plans are in place to address identified weaknesses that impact on the core business of the organisation
[Links from 1.2.2 and to 3.1.2; IAMM Tool Question Reference: 06.02.05 (v3.5), 06.02.07 (v4.0), QUES1677559938180 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Has the process put in place by the SIRO (or their equivalent) to validate the effectiveness of the compliance regime reported? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H] • Has action been taken to rectify the weaknesses identified? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H] • In addition, has the SIRO gained independent assurance of the effective operation of the information risk management compliance regime operating within the delivery chain? [IAMM Tool Evidence Reference: 3 (v3.5/v4.0); Importance: M]	• Details of the Report. • Details of any resultant action. • Details of any independent assessment.	IS1&2 & IS6. GPGs 6, 13, 19, 28 & 30	5.1 g) 5.2.1 e) A.6.1.8

2.3 Assuring the Compliance Regime [Cyber Category Type: Peripheral]

2.3.1 Required Outcome: The Audit Committee actively engages with those responsible for IRM within the organisation to ensure that the control measures being taken are proportionate and are matched to the needs of the business
[Links from 1.3.1 and to 3.2.1; IAMM Tool Question Reference: 06.03.02 (v3.5/v4.0), QUES1677559938185 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Do members of the Audit Committee, and particularly the NEDs, have appropriate engagement with those responsible for IRM? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: M] • Are they conversant with the control measures being implemented to limit the information risks and the potential adverse effect these can have on the conduct of the business? [IAMM Tool Evidence Reference: 2 & 3 (v3.5/v4.0); Importance: 2-M, 3-H]	• It is apparent by the way the Audit Committee members engage that they understand the risk balance issues. • Members of the Audit Committee are able to make informed judgements as to whether the controls being implemented are matched to the needs of the business?	IS1&2 & IS6. GPGs 19, 28 & 30	5.2.1 7

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

3.1 Assurance Activities [Cyber Category Type: Supporting]

3.1.1 Required Outcome: Internal and external audits have been conducted to gain assurance of the efficacy of the IRM regime pertaining to Business Critical ICT systems and their related business processes throughout the delivery chain
[Links from 2.2.1 and to 4.1.1; IAMM Tool Question Reference: 06.02.03 (v3.5/v4.0), QUES1677559938176 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Are plans in place to action all of the recommendations made in all reviews and audits of the organisation's IA posture relating to business critical IS and related processes? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H] • Has the IA risk management process, particularly as it applies to business critical IS and processes, been subject to independent assurance? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: M]	• Plans and details of progress checking mechanisms. • Audit report or an independent compliance assessment report.	IS1&2 & IS6. GPGs 6, 13, 19, 28 & 30	8.2 6 A.6.1.8

3.1.2 Required Outcome: The SIRO is content that appropriate action has been taken to address the recommendations made in all reviews and audits of IA that adversely impact Business Critical ICT systems and their related business processes
[Links from 2.2.2 and to 4.1.2; IAMM Tool Question Reference: 06.02.06 (v3.5), 06.02.08 (v4.0), QUES1677559938181 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Is progress against any improvement plans relating to business critical IS and related processes tracked and managed by the SIRO (or his/her equivalent)? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H]	• Evidence of SIRO's engagement.	IS1&2 & IS6. GPGs 6, 13, 19, 28 & 30	5.1 h) 8.2

3.2 Assuring the Compliance Regime [Cyber Category Type: Peripheral]

3.2.1 Required Outcome: The Audit Committee is content that the IRM regime, pertaining to Business Critical ICT systems and their related business processes, is proportionate and is matched to the needs of the business, and is also communicated appropriately down the organisation
[Links from 2.3.1 and to 4.2.1; IAMM Tool Question Reference: 06.03.03 (v3.5/v4.0), QUES1677559938186 (v5.0); Recipient Type: Organisation]
[Modified in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does the Audit Committee have sufficient evidence to assure itself that the IRM control measures in place within the organisation are proportionate to the risks, are supported, and are sufficiently robust to protect the critical aspects of the business? [IAMM Tool Evidence Reference: 1 (v3.5/v4.0); Importance: H] • Have the audit committee findings, for critical systems, been cascaded appropriately down the organisation? [IAMM Tool Evidence Reference: 2 (v3.5/v4.0); Importance: H]	• The Audit Committee gives unqualified assessments to critical systems. • Relevant personnel support the risk appetite statement (e.g. IAO's). • Evidence that the "Head's of Business Units", or the organisational equivalent, have seen the relevant documents for critical systems (e.g. SRMO submission, and/or relevant audit findings).	IS1&2 & IS6. GPGs 6, 13, 19, 28 & 30	7.3

LEVEL 4 – Quantitatively Managed – The board has established its broader IA Road Map for all its information, systems and processes

4.1 Assurance Activities [Cyber Category Type: Supporting]

4.1.1 Required Outcome: The organisation understands and is aware of non-compliances with policy and has taken a business decision to accept the associated business risk across the delivery chain
[Links from 3.1.1 and to 5.1.1; IAMM Tool Question Reference: 06.02.04 (v4.0), QUES1677559938177 (v5.0);
Recipient Type: Organisation, Delivery Partners, and Third Parties][Modified in GPG 40 Version 2.0]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Has the SIRO conducted an assessment of exceptions to policy and standards to include mitigation as necessary? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: H] • Are mitigations to deficiencies having the desired result? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: M] • 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? [IAMM Tool Evidence Reference: 3 (v4.0); Importance: H] • Does a plan exist to address the areas of non-compliance? [IAMM Tool Evidence Reference: 4 (v4.0); Importance: M]	• Details of the assessment. • Feedback into the business is showing benefits. • Main Board papers. • Details of the plan and activity, and evidence that the plan is supported at the appropriate management, and operational, levels.	IS1&2 & IS6. GPGs 6, 13, 19, 28 & 30	7.2 8.2
4.1.2 Required Outcome: The Main Board can show evidence that the consolidated view of the IRM regime is effectively managing the organisations risks [Links from 3.1.2 and to 5.1.2; IAMM Tool Question Reference: 06.02.09 (v4.0), QUES1677559938182 (v5.0); Recipient Type: Organisation, Delivery Partners, and Third Parties][Modified in GPG 40 Version 2.0]			
Areas to Probe	**Evidence Expected**	**Policy Reference**	**ISO27001 Reference**
• 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? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: H]	• Robust and accurate evidence in audit reports, as the Main Board believe that this quality of data is required to drive improvement.	IS1&2 & IS6. GPGs 6, 13, 19, 28 & 30	7.2 A.6.1.8
4.2 Assuring the Compliance Regime [Cyber Category Type: Peripheral]			
4.2.1 Required Outcome: The Audit Committee is content that the IRM regime, pertaining to all relevant systems and their related business processes, is proportionate and is matched to the needs of the business, and is also communicated appropriately down the organisation [Links from 3.2.1; IAMM Tool Question Reference: 06.03.04 (v4.0), QUES1677559938187 (v5.0); Recipient Type: Organisation][New in GPG 40 Version 2.0]			
Areas to Probe	**Evidence Expected**	**Policy Reference**	**ISO27001 Reference**
• Does the Audit Committee have sufficient evidence to assure itself that the IRM control measures in place within the organisation are proportionate to the risks, are supported, and are sufficiently robust to protect all relevant aspects of the business? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: H] • Have the audit committee findings, for all relevant systems, been cascaded appropriately down the organisation? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: H]	• The Audit Committee gives unqualified assessments on all relevant systems. • Evidence that the “Head’s of Business Units”, or the organisational equivalent, have seen the documents for all relevant systems (e.g. SRMO submission, and/or relevant audit findings).	IS1&2 & IS6. GPGs 6, 13, 19, 28 & 30	7.3

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

5.1 Assurance Activities [Cyber Category Type: Supporting]

5.1.1 Required Outcome: The organisation is cited as an exemplar of IRM best practice amongst its peers
[Links from 4.1.1; IAMM Tool Question Reference: 06.02.05 (v4.0), QUES1677559938178 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Does the organisation seek to share its knowledge, experience and expertise with organisations who are struggling to achieve an equivalent standard? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: L]	• Details of knowledge sharing.	IS1&2 & IS6. GPGs 6, 13, 19, 28 & 30	A.6.1.6 A.6.1.7

5.1.2 Required Outcome: The organisation has assurance that its IRM regime is appropriate to the needs of the business and no outstanding issues remain unresolved
[Links from 4.1.2; IAMM Tool Question Reference: 06.02.10 (v4.0), QUES1677559938183 (v5.0); Recipient Type: Organisation]

Areas to Probe	Evidence Expected	Policy Reference	ISO27001 Reference
• Has an independent evaluation of the entire organisation IA control measures been undertaken? [IAMM Tool Evidence Reference: 1 (v4.0); Importance: H] • Is there evidence to confirm that there are no significant remaining areas of weakness to be addressed? [IAMM Tool Evidence Reference: 2 (v4.0); Importance: M]	• Evaluation report. • Independent audit report.	IS1&2 & IS6. GPGs 6, 13, 19, 28 & 30	A.6.1.8 8.2

Annex C: ISO/IEC27001:2005 Correlation with IAAF

Serial	ISO27001 Reference	Description	HMG IA Maturity Model – IAAF Reference					
			L&G	TEA	IRM	TLIA	AIS	C
Main Body of Standard								
1	**4**	**Information Security Management System**						
2	**4.1**	**General Requirements**	4.2.1					
3	**4.2**	**Establishing and Managing the ISMS**						
4	4.2.1	Establish the ISMS	1.3.1, 1.3.2, 2.1.2, 3.1.1, 4.1.1	1.3.1, 3.1.3	1.1.1, 1.2.1, 1.3.1, 1.3.3, 1.4.1, 1.5.1, 1.7.1, 2.3.1, 2.4.1, 2.5.1, 2.6.1, 2.7.1, 3.1.1, 3.3.1, 3.3.2, 3.4.1, 3.5.1, 3.6.1, 3.7.1, 4.1.1, 4.2.1, 4.4.1, 4.5.1, 4.7.1	1.1.2, 1.9.1, 2.1.1, 2.1.2, 2.4.1, 2.9.1, , 3.1.2, 3.6.1, 4.5.1, 5.3.1,	1.1.1, 1.2.1, 1.5.1, 2.1.1, 2.3.1, 3.1.1	1.3.1
5	4.2.2	Implement and Operate the ISMS	2.1.3, 2.3.1, 3.1.1, 3.1.3, 3.2.1	2.3.1	1.7.1, 2.4.1	1.1.2, 1.7.1, 2.1.1, 2.7.1, 3.1.2, 3.6.1, 4.5.1, 5.3.1	1.5.1, 1.7.1, 2.3.1	
6	4.2.3	Monitor and Review the ISMS	1.2.1, 1.6.1, 2.1.2, 2.1.3, 2.3.1, 3.1.1, 3.1.2, 3.3.1, 4.1.1, 4.1.2, 4.2.1	2.3.1, 3.3.1, 4.1.1, 4.3.1, 5.1.1	1.3.1, 1.3.2, 1.6.1, 1.7.1, 2.1.1, 2.2.1, 2.3.2, 2.4.1, 2.6.1, 2.7.1, 3.2.1, 3.3.2, 3.4.1, 3.6.1, 4.2.1, 4.4.1, 5.2.1	1.1.1, 1.1.2, 2.1.1, 2.1.2, 2.9.1, 3.1.2, 3.6.1, 4.3.1, 4.5.1, 5.3.1	1.3.1, 3.2.1	1.1.1, 1.1.2, 1.1.3, 1.2.1, 1.3.1, 2.1.1, 2.2.1
7	4.2.4	Maintain and Improve ISMS	3.1.1, 3.3.1, 4.1.1, 4.2.1	3.3.1, 4.1.1, 4.3.1, 5.1.1	1.1.1	1.12.1		2.2.1
8	**4.3**	**Documentation Requirements**	1.3.1					1.2.1
9	4.3.1	General	3.1.1	3.1.1	1.7.1		3.3.1	
10	4.3.2	Control of Documents						
11	4.3.3	Control of Records		3.1.3	1.3.2			
12	**5**	**Management Responsibility**						
13	**5.1**	**Management Commitment**	1.1.1, 1.3.1, 2.3.1, 3.1.1, 3.3.1, 4.1.1, 4.1.3	3.1.2	4.2.1	3.4.1, 4.3.1	2.2.1	1.2.1, 1.3.1, 2.1.2, 3.1.2
14	**5.2**	**Resource Management**	4.1.1					
15	5.2.1	Provision of Resources	2.1.3, 2.3.1, 4.1.1			2.7.1, 2.11.1	1.7.1	2.2.2, 2.3.1
16	5.2.2	Training, Awareness and Competence		1.1.3, 2.1.3, 2.2.1, 3.1.3, 3.2.1	1.7.1, 2.6.1, 2.7.1, 3.7.1	2.1.1, 2.11.1, 3.1.1	1.3.1, 2.5.1	2.2.1

Serial	ISO27001 Reference	Description	HMG IA Maturity Model – IAAF Reference					
			L&G	TEA	IRM	TLIA	AIS	C
17	**6**	**Internal ISMS Audits**			1.7.1	1.6.1, 2.7.1, 2.15.1, 4.1.1	1.3.1, 2.2.1	1.2.1, 2.2.1, 3.1.1
18	**7**	**Management Review of the ISMS**			2.4.1, 3.4.1	5.4.1	2.4.1, 4.2.1	2.2.1, 2.2.2
19	**7.1**	**General**			4.4.1, 5.2.1	2.1.1, 3.1.1, 4.1,1 4.10.1	4.3.1	
20	**7.2**	**Review Input**			4.2.1	2.1.1, 3.1.1	2.5.1, 4.3.1	4.1.1, 4.1.2
21	**7.3**	**Review Output**	1.3.1		4.2.1, 5.1.1	2.1.1, 3.1.1, 4.1.1, 4.10.1	4.3.1	3.2.1, 4.2.1
22	**8**	**ISMS Improvement**		2.3.1	2.4.1	5.4.1		2.2.1
23	**8.1**	**Continual Improvement**				1.12.1, 5.7.1	1.7.1, 2.5.1, 3.3.1, 4.3.1, 5.1.1	
24	**8.2**	**Corrective Action**				1.11.1, 2.1.1, 2.6.1, 3.1.1	1.7.1, 2.3.1, 2.5.1, 3.5.1, 4.3.1, 5.1.1	1.2.2, 3.1.1, 3.2.2, 4.1.1
25	**8.3**	**Preventative Action**				1.11.1, 2.7.1, 5.1.1, 5.8.1	1.7.1, 2.5.1, 3.5.1, 4.3.1, 5.1.1	

Serial	ISO27001 Reference	Description	HMG IA Maturity Model – IAAF Reference					
			L&G	TEA	IRM	TLIA	AIS	C
Annex A Control Objectives and Controls								
1	**A.5**	**Security Policy**						
2	**A.5.1**	**Information Security Policy**						
3	A.5.1.1	Information Security Policy Document	1.1, 1.6.1				3.4.1	
4	A.5.1.2	Review of the Information Security Policy	2.5.1, 3.1.2					
5	**A.6**	**Organisation of Information Security**						
6	**A.6.1**	**Internal Organisation**						
7	A.6.1.1	Management Commitment to Information Security	1.1.1, 2.1.1, 2.1.2, 3.1.1, 5.1.1			3.4.1, 5.2.1, 5.4.1		
8	A.6.1.2	Information Security Co-ordination	1.1.1, 1.3.1, 1,4.1, 2.1.1		1.4.1	1.7.1, 2.7.1	2.4.1, 3.1.1	
9	A.6.1.3	Allocation of Information Security Responsibilities	1.1.1, 1.3.1, 1.3.2, 1.4.1, 1.5.1, 2.1.1, 2.3.1, 3.1.1			1.6.1, 3.4.1	1.2.1, 2.4.1	

Serial	ISO27001 Reference	Description	HMG IA Maturity Model – IAAF Reference					
			L&G	TEA	IRM	TLIA	AIS	C
10	A.6.1.4	Authorisation Process for Information Processing Facilities			1.6.1, 2.6.1, 3.6.1		2.2.1, 2.3.1	
11	A.6.1.5	Confidentiality Agreements	1.6.1			1.3.1		
12	A.6.1.6	Contact with Authorities	1.3.1, 2.1.2, 2.3.1		1.1.1, 1.2.1, 2.3.1, 2.6.1, 3.6.1	1.3.1, 1.12.1, 2.13.1, 3.6.1, 3.9.1, 3.10.1, 3.11.1, 4.8.1, 4.10.1, 5.1.1, 5.3.1	2.2.1, 2.5.1, 3.3.1, 3.5.1, 4.3.1	5.1.1
13	A.6.1.7	Contact with Special Interest Groups	1.3.1, 2.1.2, 2.3.1		1.1.1, 2.3.1, 2.6.1, 3.6.1	1.1.1, 2.11.1, 5.1.1, 5.3.1	2.2.1, 2.3.1, 2.5.1, 3.3.1, 3.5.1, 4.3.1	5.1.1
14	A.6.1.8	Independent Review of Information Security	2.1.2, 4.1.1		1.7.1			1.2.1, 1.2.2, 2.2.1, 2.2.2, 3.1.1, 4.1.2, 5.1.2
15	**A.6.2**	**External Parties**	1.1.1, 1.1.2, 1.3.1, 2.1.1, 2.3.2, 3.3.2		1.1.1, 4.6.1		4.1.1	
16	A.6.2.1	Identification of Risks Related to External Parties	1.1.1		1.1.1, 1.3.3, 2.3.2		1.1.1, 2.2.1	
17	A.6.2.2	Addressing Security when Dealing with Customers	1.2.1		1.1.1, 2.3.2, 5.2.1			
18	A.6.2.3	Addressing Security in 3rd Party Agreements	1.1.1, 2.5.1	1.1,1, 3.1.2	1.1.1, 1.3.3, 1.6.1, 2.3.2, 2.6.1	1.7.1, 1.12.1, 2.2.1, 2.7.1, 2.9.1, 3.4.1, 4.3.1		
19	**A.7**	**Asset Management**						
20	**A.7.1**	**Responsibility for Assets**	2.3.1, 2.4.1					
21	A.7.1.1	Inventory of Assets			1.5.1, 2.5.1, 2.7.1	1.7.1, 2.7.1		
22	A.7.1.2	Ownership of Assets	1.4.1		1.5.1	1.7.1, 2.7.1		
23	A.7.1.3	Acceptable Use of Assets	1.4.2		1.5.1	1.4.1, 2.4.1		
24	**A.7.2**	**Information Classification**						
25	A.7.2.1	Classification Guidelines	1.6.1		1.5.1			
26	A.7.2.2	Information Labelling and handling	1.6.1		1.5.1	1.1.1, 1.15.1, 2.1.1, 3.1.1		
27	**A.8**	**Human Resources Security**	1.3.1, 2.5.1				1.6.1	
28	**A.8.1**	**Prior to Employment**						
29	A.8.1.1	Roles and Responsibilities	1.3.1, 1.3.2, 1.4.1, 1.5.1	4.2.1		2.3.1	1.2.1	
30	A.8.1.2	Screening				1.1.1, 1.3.1, 2.3.1		

Serial	ISO27001 Reference	Description	HMG IA Maturity Model – IAAF Reference					
			L&G	TEA	IRM	TLIA	AIS	C
31	A.8.1.3	Terms and Conditions of Employment				1.3.1		
32	**A.8.2**	**During Employment**						
33	A.8.2.1	Management Responsibilities	1.1.1, 1.3.1, 2.5.1	1.3.1, 2.3.1			1.3.1,	
34	A.8.2.2	Information Security Awareness, Education and Training	1.2.1, 2.2.1, 2.3.1	1.1.1, 1.1.3, 2.1.1, 2.1.2, 2.1.3, 2.2.1, 2.3.1, 3.1.2, 3.1.3, 3.2.1, 4.1.1	1.2.1, 1.7.1, 3.7.1	1.6.1, 2.1.1, 2.6.1, 3.1.1	1.3.1, 2.5.1	
35	A.8.2.3	Disciplinary Process		1.3.1		2.6.1		
36	**A.8.3**	**Termination or Change in Employment**						
37	A.8.3.1	Termination of Responsibilities	1.6.1			1.3.1		
38	A.8.3.2	Return of Assets				1.3.1		
39	A.8.3.3	Removal of Access Rights				1.3.1, 1.10.1		
40	**A.9**	**Physical and Environmental Security**	2.5.1				1.6.1	
41	**A.9.1**	**Secure Areas**				1.2.1, 2.2.1		
42	A.9.1.1	Physical security Perimeter						
43	A.9.1.2	Physical Entry Controls						
44	A.9.1.3	Securing Offices Rooms and Facilities						
45	A.9.1.4	Protecting Against External and Environmental Threats						
46	A.9.1.5	Working in Secure Areas						
47	A.9.1.6	Public Access, Delivery and Loading Areas						
48	**A.9.2**	**Equipment Security**				1.2.1, 2.2.1		
49	A.9.2.1	Equipment Siting and Protection						
50	A.9.2.2	Supporting Utilities						
51	A.9.2.3	Cabling Security						
52	A.9.2.4	Equipment Maintenance					2.2.1	
53	A.9.2.5	Security of Equipment off Premises				1.5.1, 2.5.1, 3.2.1		
54	A.9.2.6	Secure Disposal or re-use of Equipment	2.1.2			1.15.1		
55	A.9.2.7	Removal of Property						
56	**A.10**	**Communications and Operations Management**						
57	**A.10.1**	**Operational Procedures and Responsibilities**						

Serial	ISO27001 Reference	Description	HMG IA Maturity Model – IAAF Reference					
			L&G	TEA	IRM	TLIA	AIS	C
58	A.10.1.1	Documented Operating Procedures				1.12.1, 2.10.1, 2.12.1, 3.4.1, 3.9.1, 4.3.1, 4.8.1, 5.2.1, 5.6.1	3.4.1	
59	A.10.1.2	Change Management				1.7.1, 1.12.1, 1.13.1, 2.7.1, 2.12.1, 3.4.1, 4.3.1, 5.2.1, 5.6.1	3.4.1	
60	A.10.1.3	Segregation of Duties						
61	A.10.1.4	Separation of Development, Test and Operational Facilities						
62	**A.10.2**	**3rd Party Service Delivery**	1.1.2, 2.3.2, 3.3.2		1.1.1, 2.6.1, 3.6.1, 4.6.1	2.9.1		
63	A.10.2.1	Service Delivery	1.1.1			1.12.1, 2.12.1		2.2.1
64	A.10.2.2	Monitoring and Review of 3rd Party Services	1.1.1	1.1,1	1.6.1	2.12.1, 3.4.1, 3.9.1, 4.3.1, 4.5.1, 4.8.1		2.2.1
65	A.10.2.3	Managing Changes to 3rd Party Services			1.6.1	3.6.1, 4.3.1, 4.5.1		
66	**A.10.3**	**System Planning and Acceptance**						
67	A.10.3.1	Capacity Management				4.3.1	3.1.1	
68	A.10.3.2	System Acceptance						
69	**A.10.4**	**Protection Against Malicious and Mobile Code**				1.14.1, 3.11.1, 4.10.1	1.7.1	
70	A.10.4.1	Controls against Malicious Code				1.14.1, 2.14.1, 3.11.1, 4.10.1, 5.8.1	1.6.1,	
71	A.10.4.2	Controls against Mobile Code				1.14.1, 2.14.1, 3.11.1, 4.10.1, 5.8.1	1.6.1,	
72	**A.10.5**	**Back-up**						
73	A.10.5.1	Information Back-up				1.8.1, 2.8.1, 3.5.1, 4.4.1		
74	**A.10.6**	**Network Security Management**					1.6.1, 2.2.1, 3.1.1, 3.4.1	
75	A.10.6.1	Network Controls					1.6.1, 2.5.1, 3.5.1	
76	A.10.6.2	Security of Network Services					3.4.1, 3.5.1	
77	**A.10.7**	**Media Handling**				1.9.1, 2.9.1		

Serial	ISO27001 Reference	Description	HMG IA Maturity Model – IAAF Reference					
			L&G	TEA	IRM	TLIA	AIS	C
78	A.10.7.1	Management of Removable Media				1.5.1, 1.8.1,1.15.1, 2.5.1, 3.2.1	1.3.1	
79	A.10.7.2	Disposal of Media				1.8.1, 1.15.1		
80	A.10.7.3	Information Handling Procedures				1.1.1, 1.5.1, 1.8.1, 1.15.1, 2.1.1, 2.5.1, 3.1.1, 3.2.1	1.1.1, 1.2.1, 1.3.1, 1.4.1	
81	A.10.7.4	Security of System Documentation						
82	**A.10.8**	**Exchange of Information**						
83	A.10.8.1	Information Exchange Policy and Procedures				1.7.1	1.1.1, 1.2.1, 1.4.1, 2.2.1	
84	A.10.8.2	Exchange Agreements	1.2.1				1.2.1, 1.4.1, 2.2.1, 3.5.1	
85	A.10.8.3	Physical Media in Transit					1.3.1, 1.4.1	
86	A.10.8.4	Electronic Messaging					1.3.1, 1.4.1	
87	A.10.8.5	Business Information Systems					1.6.1, 2.2.1, 3.1.1	
88	**A.10.9**	**Electronic Commerce Services**					1.4.1	
89	A.10.9.1	Electronic Commerce					1.1.1, 1.2.1, 1.4.1	
90	A.10.9.2	On-Line Transactions					1.4.1	
91	A.10.9.3	Publically Available Information					1.4.1	
92	**A.10.10**	**Monitoring**					1.6.1, 1.7.1	
93	A.10.10.1	Audit Logging	1.4.1			1.10.1, 2.10.1, 5.6.1	2.2.1, 3.5.1	
94	A.10.10.2	Monitoring System Use	1.4.1			1.10.1	2.2.1, 2.5.1	
95	A.10.10.3	Protection of Log Information					2.2.1	
96	A.10.10.4	Administrator and Operator Logs				1.10.1		
97	A.10.10.5	Fault Logging						
98	A.10.10.6	Clock Synchronisation						
99	**A.11**	**Access Control**				2.10.1, 3.7.1, 4.6.1, 5.7.1		
100	A.11.1	Access Control Policy	1.4.2			1.10.1, 1.11.1, 5.4.1		
101	**A.11.2**	**User Access Management**				1.10.1		
102	A.11.2.1	User Registration	1.4.1, 1.4.2					
103	A.11.2.2	Privilege Management	1.4.2			1.13.1	2.2.1	

Serial	ISO27001 Reference	Description	HMG IA Maturity Model – IAAF Reference					
			L&G	TEA	IRM	TLIA	AIS	C
104	A.11.2.3	User Password Management						
105	A.11.2.4	Review of User Access Rights	1.4.2			1.10.1, 2.10.1		
106	**A.11.3**	**User Responsibilities**						
107	A.11.3.1	Password Use				1.10.1		
108	A.11.3.2	Unattended User Equipment						
109	A.11.3.3	Clear Desk and Clear Screen Policy						
110	**A.11.4**	**Network Access Control**					1.6.1, 1.7.1	
111	A.11.4.1	Policy Use of Network Services					2.4.1	
112	A.11.4.2	User Authentication for External Connections				1.10.1, 1.13.1	1.3.1	
113	A.11.4.3	Equipment Identification in Networks						
114	A.11.4.4	Remote Diagnostic and Configuration Port Protection				1.13.1		
115	A.11.4.5	Segregation in Networks						
116	A.11.4.6	Network Connection Control					1.6.1, 2.2.1, 2.4.1, 3.4.1	
117	A.11.4.7	Network Routing Control					3.1.1	
118	**A.11.5**	**Operating System Access Control**					1.3.1, 1.7.1	
119	A.11.5.1	Secure Log-on Procedures				1.10.1		
120	A.11.5.2	User Identification and Authentication				1.10.1		
121	A.11.5.3	Password Management System						
122	A.11.5.4	Use of System Utilities						
123	A.11.5.5	Session Time-Out						
124	A.11.5.6	Limitation of Connection Time						
125	**A.11.6**	**Application and Information Access Control**					1.7.1	
126	A.11.6.1	Information Access Restriction					2.2.1	
127	A.11.6.2	Sensitive System Isolation						
128	**A.11.7**	**Mobile Computing and Teleworking**						
129	A.11.7.1	Mobile Computing and Communications	2.1.2					
130	A.11.7.2	Teleworking	2.1.2					
131	**A.12**	**Information System Acquisition, Development and Maintenance**						

Serial	ISO27001 Reference	Description	HMG IA Maturity Model – IAAF Reference					
			L&G	TEA	IRM	TLIA	AIS	C
132	**A.12.1**	**Security Requirements of Information Systems**						
133	A.12.1.1	Security Requirements Analysis and Specification	1.3.1, 2.1.2, 2.3.1		1.6.1		1.5.1, 2.3.1, 3.1.1	
134	**A.12.2**	**Correct Processing in Applications**						
135	A.12.2.1	Input Data Validation						
136	A.12.2.2	Control of Internal Processing						
137	A.12.2.3	Message Integrity						
138	A.12.2.4	Output Data Validation						
139	**A.12.3**	**Cryptographic Controls**						
140	A.12.3.1	Policy on the use of Cryptographic Controls				1.1.1		
141	A.12.3.2	Key Management				1.1.1		
142	**A.12.4**	**Security of System Files**						
143	A.12.4.1	Control of Operational Software						
144	A.12.4.2	Protection of System Test data						
145	A.12.4.3	Access Control to Programme Source Code						
146	**A.12.5**	**Security in Development and Support Processes**						
147	A.12.5.1	Change Control Procedures				1.7.1, 1.12.1, 2.7.1		
148	A.12.5.2	Technical Review of Applications After Operating System Changes				3.8.1		
149	A.12.5.3	Restrictions on Changes to Software Packages						
150	A.12.5.4	Information Leakage						
151	A.12.5.5	Outsourced Software Development				1.7.1		
152	**A.12.6**	**Technical Vulnerability Management**						
153	A.12.6.1	Control of Technical Vulnerabilities				1.11.1, 1.12.1, 2.11.1, 3.8.1, 4.7.1, 5.5.1	1.6.1, 3.1.1, 3.4.1, 3.5.1	
154	**A.13**	**Information Security Incident Management**						
155	**A.13.1**	**Reporting Information Security Events and Weaknesses**				1.6.1, 5.1.1	2.2.1	
156	A.13.1.1	Reporting Information Security Events				1.6.1, 4.5.1		
157	A.13.1.2	Reporting Security Weaknesses		1.3.1, 2.3.1				

Serial	ISO27001 Reference	Description	HMG IA Maturity Model – IAAF Reference					
			L&G	TEA	IRM	TLIA	AIS	C
158	**A.13.2**	**Management of Information Security Incidents and Improvements**				1.6.1	4.3.1	
159	A.13.2.1	Responsibilities and Procedures				2.6.1, 4.2.1	2.5.1	
160	A.13.2.2	Learning From Information Security Incidents				2.6.1, 3.3.1, 4.2.1, 4.5.1, 5.1.1	1.7.1, 3.5.1, 4.3.1, 5.1.1	
161	A.13.2.3	Collection of Evidence				1.6.1, 2.6.1		
162	**A.14**	**Business Continuity Management**						
163	**A.14.1**	**Information Security Aspects of Business Continuity Management**	2.3,1		3.5.1	1.8.1, 2.8.1, 3.5.1, 4.4.1		
164	A.14.1.1	Including Information Security in the Business Continuity Management Process				5.3.1		
165	A.14.1.2	Business Continuity and Risk Assessment				5.3.1	3.1.1	
166	A.14.1.3	Developing and Implementing Continuity Plans Including Information Security						
167	A.14.1.4	Business Continuity Planning Framework						
168	A.14.1.5	Testing, Maintaining and Re-Assessing Business Continuity Plans				1.8.1, 2.8.1, 3.5.1, 4.4.1		
169	**A.15**	**Compliance**						1.1.3
170	**A.15.1**	**Compliance with Legal Requirements**						1.1.1, 1.2.2, 2.1.1
171	A.15.1.1	Identification of Applicable Legislation	1.1.1, 1.2.1		1.1.1, 1.7.1	1.2.1, 1.5.1, 1.6.1, 1.7.1, 1.11.1, 2.11.1, 3.8.1, 4.7.1, 5.3.1	1.3.1	1.2.2, 1.3.1, 2.2.1
172	A.15.1.2	Intellectual Property Rights (IPR)						1.1.2
173	A.15.1.3	Protection of Organisational Records						
174	A.15.1.4	Data Protection and Privacy of Personal Information	1.1.1, 2.2.1		1.7.1	1.1.1, 1.7.1, 1.10.1	1.4.1	1.2.2
175	A.15.1.5	Prevention of Misuse of Information Processing Facilities				1.4.1, 2.4.1		
176	A.15.1.6	Regulation of Cryptographic Controls	1.5.1		1.6.1, 2.7.1	1.1		
177	**A.15.2**	**Compliance with Security Policies and Standards, and Technical Compliance**				2.12.1, 2.14.1, 2.15.1, 3.8.1, 4.8.1	1.6.1, 2.4.1	1.1.2, 1.1.3
178	A.15.2.1	Compliance with Security Policies and Standards	1.4.1, 1.4.2, 4.1.1	2.1.4, 3.1.1, 5.1.1	1.1.1, 1.7.1	1.6.1, 1.10.1, 1.12.1, 2.2.1, 2.4.1, 2.5.1, 2.10.1,	1.3.1, 1.6.1, 1.7.1, 2.2.1, 2.5.1, 3.3.1	1.2.1, 2.2.1

Serial	ISO27001 Reference	Description	HMG IA Maturity Model – IAAF Reference					
			L&G	TEA	IRM	TLIA	AIS	C
						2.13.1, 3.1.1, 3.2.1, 3.7.1, 3.8.1, 3.10.1, 4.1.1, 4.5.1, 4.6.1, 4.8.1, 4.9.1		
179	A.15.2.2	Technical Compliance Checking	2.3,.1	1.1.4	1.3.2, 1.7.1	1.12.1, 1.13.1, 3.11.1, 4.10.1	1.6.1, 3.3.1	
180	**A.15.3**	**Information Systems Audit Considerations**						
1	A.15.3.1	Information Systems Audit Controls			1.7.1			
1	A.15.3.2	Protection of Information Systems Audit Tools						

References

Unless stated otherwise, these documents are available from the CESG website. Users who do not have access should contact CESG Enquiries to enquire about obtaining documents.

[a] Government ICT Strategy, March 2011. (Not Protectively Marked). Available at http://www.cabinetoffice.gov.uk .

[b] HMG Security Policy Framework (SPF), Tiers 1-3 (Not Protectively Marked). Available at http://www.cabinetoffice.gov.uk.

[c] HMG IA Standard No. 6, Protecting Personal Data and Managing Information Risk (UNCLASSIFIED) – latest issue available from the CESG website

[d] ISO/IEC 27001:2005 Information Security Management Systems – Requirements

[e] National Security Strategy, October 2010. (Not Protectively Marked). Available at http://www.direct.gov.uk. Available at http://www.cabinetoffice.gov.uk.

[f] Cyber Security Strategy, November 2011. (Not Protectively Marked). Available at http://www.cabinetoffice.gov.uk.

[g] Civil Service Reform Plan, June 2012. (Not Protectively Marked). Available at http://www.civilservice.gov.uk . [Note: This document indicates that the Government Digital Service will publish the Government Digital Strategy. This GPG has not referenced that strategy as it was not available during this GPG drafting process.]

[h] CESG Good Practice Guide No. 28, Improving IA at the Enterprise Level (UNCLASSIFIED) – latest issue available from the CESG website.

[i] The Government Digital Service (GDS) will publish the Government Digital Strategy, although it is planned to be available in December 2012. This GPG has not referenced that strategy as it was not available during this GPG drafting process.

[j] Supplier Information Assurance Assessment Framework and Guidance, Issue 1.0, January 2011. Available from the CESG website.

[k] The National Archives' Managing Information Risk – A Guide for Accounting Officers, Board Members and SIROs, March 2008 (Not Protectively Marked). Available at http://www.nationalarchives.gov.uk.

[l] HMT Risk Management Assessment Framework, July 2009. (Not Protectively Marked). Available at http://www.hm-treasury.gov.uk.

[m] Cabinet Office (Efficiency and Reform Group [ERG]) OGC Gateway Review Process available at http://www.cabinetoffice.gov.uk (which after transition did have a link to the appropriate National Archives location, as the OGC became part of the ERG on 15 June 2010).

[n] HMG IA Standard No 1 & 2, Information Risk Management (UNCLASSIFIED) – latest issue available from the CESG website.

[o] CESG Good Practice Guide No. 6, Outsourcing and Offshoring: Managing the Security Risks (UNCLASSIFIED) – latest issue available from the CESG website.

[p] HMG IA Standard No. 5, Secure Sanitisation (UNCLASSIFIED) – latest issue available from the CESG website.

[q] HMG IA Standard No. 4, Protective Security Controls for the Handling and Management of Cryptographic Items (OFFICIAL SENSITIVE) – latest issue available from the CESG website.

[r] CESG Good Practice Guide No. 8, Protecting External Connections to the Internet (Not Protectively Marked) – latest issue available from the CESG website.

[s] CESG Good Practice Guide No. 13, Protective Monitoring for HMG ICT Systems (UNCLASSIFIED) – latest issue available from the CESG website.

CESG Enquiries
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX

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