

# HMG IA Standard Numbers 1 & 2

## Information Risk Management

# HMG IA Standard Numbers 1 & 2

## Information Risk Management

Issue: 4.0  
April 2012

This document is for the purposes of issuing advice to UK government, public sector organisation and/or related organisations. The copying and use of this document for any other purpose, such as for training purposes, is not permitted without the prior approval of CESG.

The copyright of this document is reserved and vested in the Crown.

### Document History – IS1

Version	Date	Comment
1.0	March 1998	First issue
2.0	April 2003	
2.1	September 2003	
2.2	March 2007	
3.0 Part 2	April 2007	IS1 now divided into two parts; risk assessment and risk treatment
3.0 Part 1	June 2007	IS1 now divided into two parts; risk assessment and risk treatment. Qualitative risk assessment method introduced combining former methodologies from IS1 and IS3
3.1 Part 1	July 2007	
3.1 Part 2	January 2008	
3.2 Part 2	February 2008	
3.2 Part 1	October 2008	
3.3 Part 1	March 2009	
3.4 Part 2	December 2008	
IS1 Parts 1 & 2 3.5	October 2009	IS1 Part 1 & 2 version numbers synchronised
IS1 Parts 1 & 2 3.6	October 2010	
4.0	April 2012	IS1 & IS2 combined into the one Standard. Risk assessment and risk treatment methods combined into the one Supplement

### Document History – IS2

Version	Date	Comment
1.0	April 1999	First issue
2.0	May 2005	
3.0	January 2008	
3.1	October 2008	
3.2	January 2010	
4.0	April 2012	IS1 & IS2 combined into the one Standard

## Intended Readership

This Standard principally addresses two types of audience:

- Those who hold senior Information Assurance (IA) related posts within Her Majesty's Government (HMG), specifically: Senior Information Risk Owners (SIROs), Departmental Security Officers (DSOs), Information Asset Owners (IAOs), Lead Accreditors and others who, in conjunction with the Management Board, are responsible for setting the organisational Information Security Strategy which establishes policies such as Information Risk Management
- Information Risk Managers, Security & Information Risk Advisors (SIRAs), IA Practitioners, Analysts, Accreditors, delivery partners and third party suppliers, who are responsible for identifying, assessing and managing the technical risks to HMG Information and Communication Technology (ICT) systems and services that handle, store or process Government information

Additionally it assists all those who are more widely involved in the information risk management and accreditation of ICT systems or services that handle, store or process Government information.

## Executive Summary

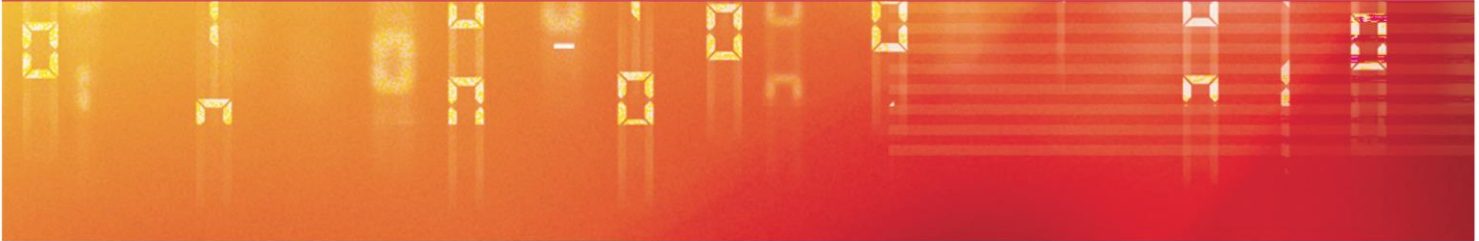
This document is a Tier Four Standard and forms part of the Security Policy Framework (SPF) (reference [a]) and therefore it **must** be used by Central Government Departments and Agencies. It is also recommended for the wider public sector. It directly supports SPF Mandatory Requirements (MRs) 1, 3, 6, 8, 9 and 11.

When setting an organisation's Information Security Strategy, supporting IA structures, policies and processes need to be established. This Standard, its Supplement and the supporting documents published in the CESG IA Policy Portfolio will help Departments and Agencies to achieve this.

Departments and Agencies **must** produce an Information Risk Management Policy; it is a fundamental aspect of an organisation's Information Security Strategy; it not only underpins the corporate approach to information security, but also directs the organisation's wider IA policies, standards, guidance and procedures.

An organisation's Information Risk Management Policy **must** include the following:

- Compliance with all legal and regulatory obligations and requirements
- An IA Governance Framework with IA roles, which define responsibility and accountability for key information risk



management processes. This is equally applicable for shared services

- An information risk appetite statement
- An Accreditation Policy which defines the strategic approach to proportionality of accreditation and re-accreditation within the Department or Agency
- An Education and Training Policy for all mandatory and specialist security roles

A fundamental principle of information risk management is technical risk assessment, and all Departments and Agencies **must** conduct a technical risk assessment for the Confidentiality, Integrity and Availability of their ICT systems or services in line with the stepped methodology presented in the Supplement to this Standard: HMG IA Standard Nos. 1 & 2 – Supplement (Supplement), Technical Risk Assessment and Risk Treatment (reference [b]). Any technical risk assessment **must** include a business impact and threat assessment so that Departments and Agencies can identify and value their information assets and understand the threats that they face.

A technical risk assessment, whilst important, is a precursor to effective information risk management. The management of information risk through treatment, (the selection and implementation of controls), is where organisations should direct their resources, (especially when they are constrained).

Organisations should note that the risks they face are not only technical in nature; they will also have to manage financial, people, and physical risk amongst others. Often risks are interrelated so they should not be assessed or managed in isolation. It is recommended that any technical risk assessments are supported and contextualised by business activities and wider risk management processes such as other corporate risk appetite(s) and Departmental risk registers. Where appropriate the output of wider risk management processes and business context should contribute to the overall understanding of risk amongst the organisation's stakeholders.

The outcome of the technical risk assessment provides organisations with an understanding of the nature and severity of the technical risks that their information assets face, which results in a more informed, and therefore proportionate and appropriate approach to their ongoing management.

Departments and Agencies **must** produce and communicate an Accreditation Policy. By establishing and communicating an Accreditation Policy the SIRO, in conjunction with the Accreditor has the ability to define a strategic approach to accreditation and re-accreditation, which can for example, include the terms for proportionality and the requirements of the document set, (the RMADS); this is critical for cost savings and business objectives to be realised. There is no reason why simple systems cannot have a short and basic RMADS.

It is critical that the Accreditor or their delegated authority is involved at project

# Information Risk Management

start-up meetings so that the requirement for accreditation can be communicated to the ICT project or programme team. These requirements can also be included in the organisation's Accreditation Policy.

Residual risks will remain after treatment activities and any associated information risk management decisions should be taken in the context of the organisation's information risk appetite and tolerance levels, whilst ensuring that business objectives are met and the expectations of risk stakeholders are accommodated. Any management decisions for residual risks that are at variance with the organisation's

information risk appetite **must** be endorsed by the SIRO or their delegated authority.

Information risk management and the processes that support it is a continuous, through life activity. Embedding information risk management into all related processes will help to support this important objective.

## Aims and Purpose

The aim of this Standard is to provide Risk Management Requirements (RMRs) – of which there are twenty, and a number of mandatory preconditions, which Departments and Agencies **must** use as the basis for their Information Risk Management Policy. This Standard supports SPF MR 6 which states that 'Departments and Agencies **must** have an information security policy ...' The RMRs are typically strategic in nature; however the Standard has been written to also support Information Risk Managers, IA Practitioners and Analysts, as well as those in senior IA posts.

Departments and Agencies should note that the purpose of this Standard is not to form the basis for contract creation or legally binding agreements, and it should not be used to do so; its main purpose is to provide national information risk management policy for implementation by Central Government Departments and Agencies through their own Information Risk Management and IA policies.<sup>1</sup>

---

<sup>1</sup> Departments and Agencies may decide that aspects of their own Information Risk Management or IA policies are suitable to be used as the basis for contract creation or legally binding agreements. Where this is the case, business and security requirements need to be clearly communicated to those with contractual responsibility so that they are understood and incorporated into contracts or legally binding agreements. Departments and Agencies should, in the first instance, contact their Commercial and Legal teams.



## Major Changes from IS1 Part 1 v3.6, Part 2 v3.6 & IS2 v3.2

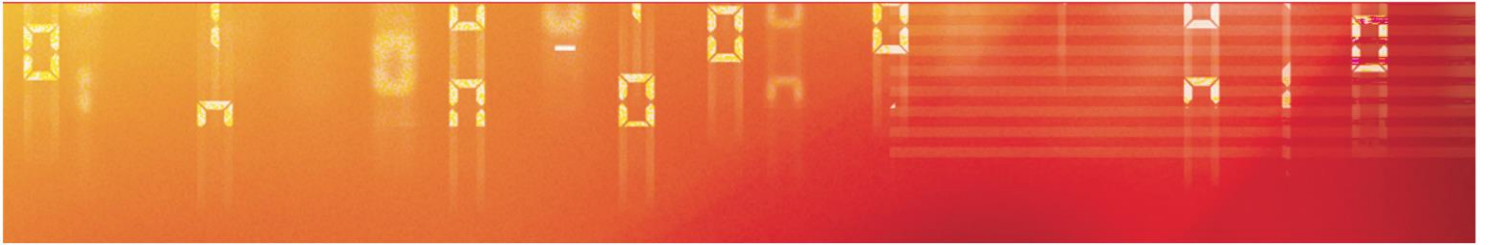
The following changes have been incorporated:

- Alignment with the revised SPF; the style and format of this Standard supports this; policy is clearly identifiable and supported by guidance to assist with its pragmatic interpretation
- The IS1 and IS2 Standards have been incorporated into one document
- The number of policy mandates have been significantly reduced with the focus now being on fundamental information risk management principles which **must** be used as the basis for Departments' and Agencies' Information Risk Management Policy
- The inclusion of information risk management policy in support of shared services
- Departments and Agencies **must** implement the full set of controls as defined in the Baseline Control Set where the Business Impact Level has been assessed as **3** or above for either: Confidentiality, Integrity or Availability
- Departments and Agencies are to establish their own requirements and processes for proportionate accreditation and re-accreditation through the implementation of an Accreditation Policy
- The technical risk assessment and risk treatment methodologies are now found in the accompanying Supplement. This Standard provides formal policy for information risk management; the accompanying Supplement does **not** introduce any additional policy – it supports Departments and Agencies to fulfil their technical risk assessment and risk treatment obligations
- The majority of the information risk management guidance contained in IS2 v3.2 is now located in the supporting Good Practice Guide No. 47, Information Risk Management (reference [c]).

# Information Risk Management

## Contents:

<b>Chapter 1 - Introduction .....</b>	<b>7</b>
Using this Standard .....	7
Status and Applicability.....	8
Pragmatic Information Risk Management – What This Means..	10
<b>Chapter 2 - Policies and the IA Governance Framework.....</b>	<b>13</b>
Information Risk Management Policy .....	13
IA Governance Framework.....	14
Departmental IA Policies .....	18
<b>Chapter 3 - Technical Risk Assessment and Risk Treatment ..</b>	<b>21</b>
Technical Risk Assessment.....	21
Risk Treatment .....	27
<b>Chapter 4 - Accreditation Requirements.....</b>	<b>31</b>
<b>References .....</b>	<b>35</b>
<b>Glossary .....</b>	<b>37</b>
<b>Customer Feedback .....</b>	<b>49</b>



THIS PAGE IS INTENTIONALLY LEFT BLANK

ARCHIVE

## Chapter 1 - Introduction

### Key Principles

- This Standard directly supports SPF MRs 1, 3, 6, 8, 9 and 11; to help Departments and Agencies fulfil their Information Security Policy, technical risk assessment, risk treatment and accreditation obligations
- This Standard is provided with a technical risk assessment and risk treatment Supplement and should be read in conjunction with the supporting GPG 47 (reference [c])
- Departments and Agencies should note that their information risk management processes should be proportionate and appropriate to the system or service under consideration

### Using this Standard

1. This Standard has been formatted to assist Departments and Agencies with clearly identifying what is policy and what is supporting guidance. A policy statement will appear in the body of the text like this: 'the Department or Agency must fulfil this', or in a numbered red text box as shown below:

#### **RISK MANAGEMENT REQUIREMENT #**

This is a mandatory policy statement, the Department or Agency **must** fulfil this.

2. The mandatory policy statement(s) and RMRs are supported by guidance, which will provide the context needed to help Departments and Agencies pragmatically interpret them and fulfil their obligations.
3. This Standard is provided with a technical risk assessment and risk treatment Supplement and a supporting GPG 47 (reference [c]) which will help Departments and Agencies to establish a proportionate and cost effective approach to information risk management within the bounds of national IA Policy.
4. This Standard mandates some fundamental information risk management principles for inclusion in an organisation's Information Risk Management Policy and supporting IA processes.



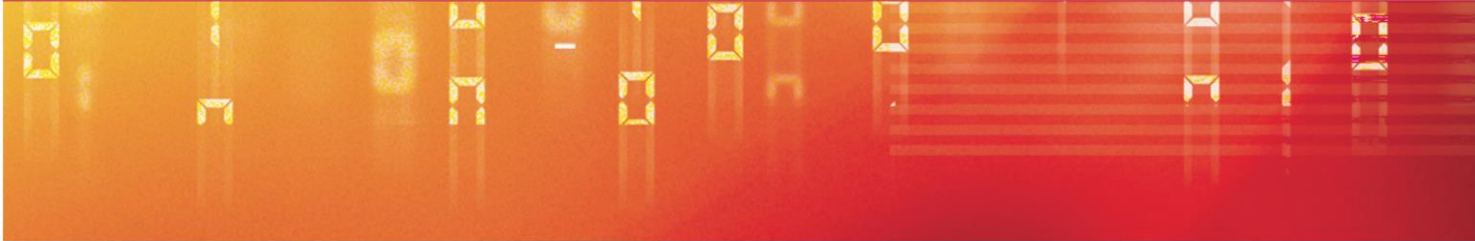
## Status and Applicability

5. This Standard directly supports SPF MRs 1, 3, 6, 8, 9 and 11; to help Departments and Agencies fulfil their Information Security Policy, technical risk assessment, risk treatment and accreditation obligations.
6. The SPF states that 'Departments and Agencies **must** conduct technical risk assessments for all ICT systems or services (using 'HMG IA Standard No. 1 – Technical Risk Assessment')'. This assessment **must** be reviewed annually or wherever there are significant changes to a risk component (threat vulnerability, business use, impact etc).
7. Departments and Agencies should note that where a technical risk assessment has already been conducted for their existing ICT systems or services, then an annual review of the findings will suffice. If there have been no significant changes to the components of risk or the technologies that form the Assessment Scope, then a new technical risk assessment is not required. This decision should be recorded and endorsed by the Accreditor or their delegated authority.
8. It is recommended that any technical risk assessments are supported and contextualised by business activities and wider risk management processes such as other corporate risk appetite(s) and Departmental risk registers. Without this business context organisations will not necessarily consider all the risks that should be captured by the Assessment Scope.
9. SPF MR 8 states that 'All ICT systems that handle, store and process protectively marked information or business critical data, or that are interconnected to cross-government networks or services' ... '**must** undergo a proportionate accreditation process to ensure that the risks to confidentiality, integrity and availability of the data, system and/or service are properly managed'.
10. The accreditation of ICT systems or services handling, storing or processing protectively marked information or business critical data is a formal, independent assessment against its IA requirements, which results in the acceptance of residual risks in the context of business requirements and information risk appetite. Typically this will be a prerequisite for approval to operate.
11. Departments and Agencies should note that the accreditation process **must** be proportionate; where a system is complex then the RMADS will probably contain a lot of information and in particular the risk assessment, risk treatment and assurance activities may be complicated. However, where a system is simple, low risk or follows a standard pattern then the production of an RMADS need not be an overly burdensome activity.

12. The Government Protective Marking System (GPMS) is an administrative system to ensure that access to information assets is correctly managed and safeguarded to an agreed and proportionate level throughout their lifecycle; it is founded upon the 'need to know' principle. Further information on the Government Protective Marking System is available in Security Policy No.2, Security of Information, of the SPF.
13. Information assets are provided with a Protective Marking by the originator or nominated owner based on criteria as defined by the Cabinet Office in Annex One of the SPF. The Protective Marking reflects the need for Confidentiality of the information asset(s) to be maintained and does not relate to Integrity or Availability matters.
14. Organisations should note that HMG information assets do not automatically carry a Protective Marking and that the relationship between Protective Markings and Business Impact Levels (ILs) is **one-way** and it sets the minimum IL for Confidentiality. The Protective Markings of PROTECT, RESTRICTED, CONFIDENTIAL, SECRET and TOP SECRET equate to ILs for Confidentiality of at **least** 1/2, 3, 4, 5 and 6 respectively. However, it is not the case that an information asset that has been assessed, for example as having an IL of 5 for Confidentiality necessitates a Protective Marking of SECRET. Further information on ILs is available in Appendix B of the Supplement to this Standard.
15. Departments and Agencies should note that there may be situations where the assurance gained from accrediting ICT systems or services is required to validate the approach to information risk management even though protectively marked information or business critical data is not being handled, stored or processed. For example, there may be circumstances in which senior risk stakeholders<sup>2</sup> request that the ICT system or service is accredited because of the assessed high level of impact should its Integrity or Availability be compromised, even though the information being processed is not protectively marked.
16. Whilst those organisations that are bound by the SPF are mandated to conduct technical risk assessments, and accredit their ICT systems or services when they are processing protectively marked information or business critical data, they should note that the information risk management processes supporting this should be proportionate and cost effective.
17. CESG support a flexible approach when using the technical risk assessment methodology it provides in the Supplement to this Standard. Whilst it is mandated that organisations produce and communicate an Accreditation Policy, this

---

<sup>2</sup> For the purpose of this Standard, the term senior risk stakeholder refers to any senior member of an organisation who is responsible and accountable for its risk management activities.



Standard does not insist that a specific structure or content is used; instead it provides guidance in GPG 47 (reference [c]) to assist Departments and Agencies with its production. This then allows for the business requirements of the organisation to be included in its information risk management processes.

18. Flexibility can sometimes result in a trade-off with consistency and because of this CESG have provided a stepped methodology in the Supplement to this Standard, which provides Departments and Agencies with a repeatable and consistent approach to technical risk assessment, which follows fundamental principles that **must** be followed. Organisations should note that the mandatory component of the technical risk assessment is the analysis, **not** the generation of forms.
19. A repeatable and consistent approach to technical risk assessment and information risk management processes more generally, is crucial for Pan Government information exchange and shared services<sup>3</sup> so that cost savings are realised. Furthermore, those in specialist security roles, (such as the Lead Accreditor), will be familiar with the methodologies and guidance presented in the supporting Supplement, GPG 47 (reference [c]) and the wider CESG policy portfolio as a whole.
20. This familiarisation can support the decision making process, help gain Management Board approval and establish effective Departmental IA policies, standards, guidance and procedures. For this reason Departments and Agencies may choose to incorporate aspects of CESG's IA guidance in their own Information Risk Management Policy.

### Pragmatic Information Risk Management – What This Means

21. A pragmatic approach to information risk management does **not** mean do nothing or the bare minimum; Departments and Agencies cannot use resource constraints as a means of justifying a lack of information risk management activity. Information risk management and its supporting processes should be proportionate and appropriate to the system or service under consideration, and adapt according to the needs of the business.
22. Information risk management should be viewed as a necessary function of an organisation, enabling Departments and Agencies to successfully conduct business. It should therefore be planned and resourced for appropriately in the

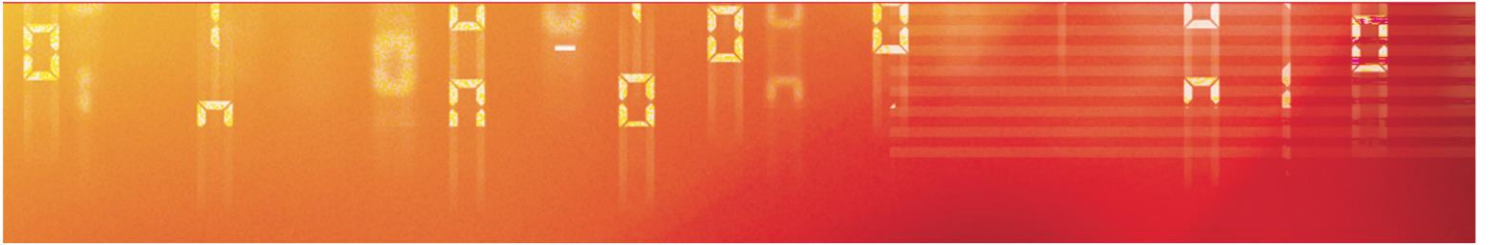
---

<sup>3</sup> For the purpose of this Standard, the term shared service is used to refer to any ICT system or service which is utilised by more than one stakeholder in a combined or collaborative business function. Typical factors identifying a shared service include the sharing of investment between organisations and the re-use and sharing of information assets, including processes and technologies in a combined or collaborative function.

## Information Risk Management

same manner as other professional business functions such as Human Resources (HR) and legal teams.

23. Only when organisations accept that information risk management is an integral aspect of their business activities can the associated costs be managed effectively. If information risk management requirements are 'overlaid' in support of an ICT project or programme, (especially when it has been identified at a late stage in the lifecycle), they are typically more expensive. In this case, information risk management decisions can become influenced by project deliverables and timescales, resulting in related contracts not representing value for money, or worst case, failing to effectively meet the security requirements of the Department or Agency. Organisations should note that Accreditor, (or their delegated authority), involvement at project start-up meetings is essential so that the requirement for accreditation can be communicated to the ICT project or programme team.



THIS PAGE IS INTENTIONALLY LEFT BLANK

ARCHIVE

## Chapter 2 - Policies and the IA Governance Framework

### Key Principles

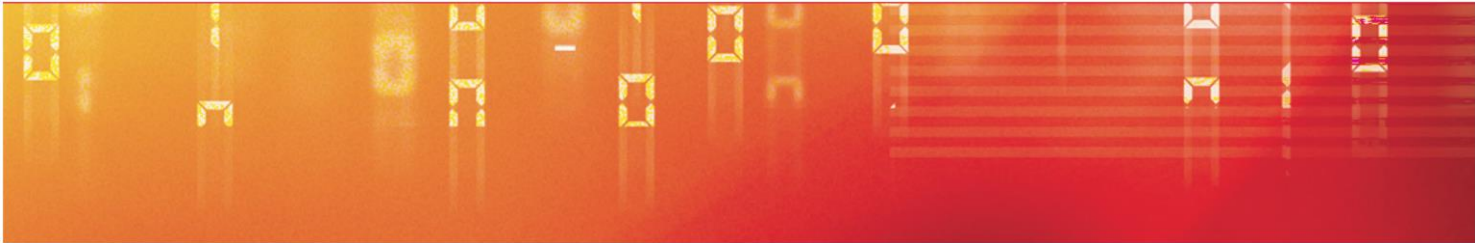
- Ultimate responsibility and accountability for legal and regulatory compliance will always reside with the Accounting Officer/Permanent Secretary of the Department
- In order for an IA Governance Framework to be effective it should be transparent, with IA responsibilities clearly assigned including the remit of delegation
- Having clearly defined roles, responsibilities and functions is a fundamental requirement of an IA Governance Framework and **must** also be established for shared services
- The Management Board's commitment to effective information security is to be communicated; an information risk appetite statement **must** be produced in support of this
- An Accreditation Policy will define the terms for proportionate accreditation and re-accreditation
- An Education and Training Policy will assist those in mandatory and specialist security roles to perform their duties effectively

### Information Risk Management Policy

24. There **must** be a 'through life' approach to information risk management across an organisation. Embedding information risk management into all related processes will help to support this important objective. In order for information risk management to be effective it has to be visibly supported by the Management Board and senior post holders of an organisation. A Management Board statement can clearly communicate their commitment to information risk management and can be included in the Information Risk Management Policy. This will help set the organisation's Information Security Strategy, establish its Information Security Policy and direct the wider Departmental IA policies, standards, guidance and procedures.

#### RISK MANAGEMENT REQUIREMENT 1

Departments and Agencies **must** produce an Information Risk Management Policy which incorporates the Risk Management Requirements (RMRs) of this Standard. The Information Risk Management Policy **must** also include the Mandatory Requirements from the SPF and HMG IA Standards.

- 
25. This RMR supports SPF MR 6. The Information Risk Management Policy will be a component of the overarching Information Security Policy, and **must** be endorsed by the Board. It should set out the IA direction for the Department or Agency as a whole, how this will be achieved and be clearly communicated and made available to all members of the organisation. Aspects of the policy and the supporting Departmental IA policies, standards, guidance and procedures will also be applicable to delivery partners and third party suppliers. A key objective of the Information Risk Management Policy should be the improvement of organisational processes in order to continue to support business objectives and provide assurance that the associated information risks are being managed effectively.
26. Effective information risk management is a continual process, and its main objective is to provide an organisation with the assurance that its ICT systems and services can be trusted to support its business activities. Effective information risk management will support a consistency of approach which is imperative for interoperability and data sharing purposes.
27. Further information on the production of an Information Risk Management Policy is available in Chapter 2 – Departmental IA Policies, Standards, Guidance and Procedures of GPG 47 (reference [c]).
28. In order for information risk management to be effective it should be applied across the entire organisation, further information in support of this is available in CESG Good Practice Guide No. 40 (GPG 40), The Information Assurance Maturity Model and Assessment Framework (reference [d]) and Good Practice Guide No. 28 (GPG 28), Improving Information Assurance at the Enterprise Level (reference [e]).

## **RISK MANAGEMENT REQUIREMENT 2**

The Information Risk Management Policy and its supporting organisational IA policies, standards, guidance and procedures **must** comply with the legal and regulatory obligations and requirements placed upon the Department or Agency.

29. Meeting legal and regulatory obligations and requirements is a significant objective of the corporate governance process and is to be included in all information risk management processes. Ultimate responsibility and accountability for legal and regulatory compliance will reside with the Accounting Officer/Permanent Secretary of the Department.

## **IA Governance Framework**

## RISK MANAGEMENT REQUIREMENT 3

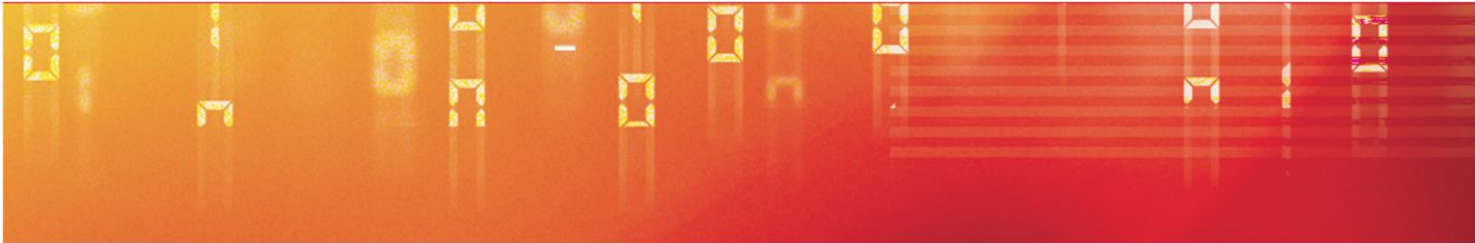
In order to ensure accountability and ownership, Departments and Agencies **must** have an IA Governance Framework in place.

30. This RMR supports SPF MR 1. Whilst it is recognised that the Accounting Officer/Permanent Secretary is ultimately accountable for the information security of the Department, it is the responsibility of every member of staff, and an effective IA Governance Framework helps to reinforce this. In order for an IA Governance Framework to be effective it should be transparent, with IA responsibilities clearly assigned including the remit of delegation. This is an imperative for shared services where common information risk management agreements need to be made.
31. An organisation's IA Governance Framework **must** include the mandatory and specialist security roles as identified in the SPF and HMG IA Standard No. 6 (IS6), Protecting Personal Data and Managing Information Risk (reference [f]). Further information on mandatory and specialist security roles is available in Chapter 5 – Mandatory and Specialist Security Roles, Responsibilities and Functions of GPG 47 (reference [c]).

## RISK MANAGEMENT REQUIREMENT 4

Departments and Agencies **must** establish IA roles which clearly define responsibility and accountability for key information risk management processes including: technical risk assessment, risk treatment, risk ownership and accreditation.

32. Departments and Agencies should manage the succession of those IA roles with responsibility and accountability for key information risk management processes. For example, it is not uncommon for the responsibility and accountability of key information risk management processes to be transferred to different individuals as ICT projects or programmes progress. Equally, succession needs to be managed once an ICT project or programme has been delivered as typically responsibility and accountability are then handed over.
33. If the succession of IA roles is not properly managed then aspects of the information risk management processes or decisions may have to be revisited because there is a lack of supporting rationale, or tangible evaluation and assessment available. This is inefficient as resources and efforts are in effect duplicated potentially leading to increases in cost and project or programme delay.



Inconsistencies of approach will also arise which can result in ineffective information risk management.

### Shared Services

34. Having clearly defined roles, responsibilities and functions is a fundamental requirement of an IA Governance Framework. This is especially important when considering the provision of shared services; a clear definition on how the accreditation and wider risk management processes will be run, and where accountability resides **must** be established. Further information on recommended IA roles, including those for shared services is available in Chapter 5 – Mandatory and Specialist Security Roles, Responsibilities and Functions of GPG 47 (reference [c]).
35. It is crucial that a consistent, common approach to understanding and managing information risk is established in a shared service environment so that consumers can be confident that the provider will securely manage their information in a manner that is mutually acceptable. For shared environments such as the Public Service Network (PSN) where several suppliers may be involved in the provision of similar services, it is important that they have access to consistent and complete information.
36. The responsibility for the accreditation of shared services needs to be defined; there will be situations where a lead organisation or group may accredit a shared service on behalf of others who wish to use it. Accreditation governance for shared services will vary; for example, from a named and recognised Department leading, (with ultimate decision making resting with them), to a Pan Government Accreditor (PGA) making accreditation decisions on behalf of a panel of representative SIROs, both examples are equally suitable, provided that responsibility and accountability are clearly defined.

### Information Risk Appetite Statement

#### **RISK MANAGEMENT REQUIREMENT 5**

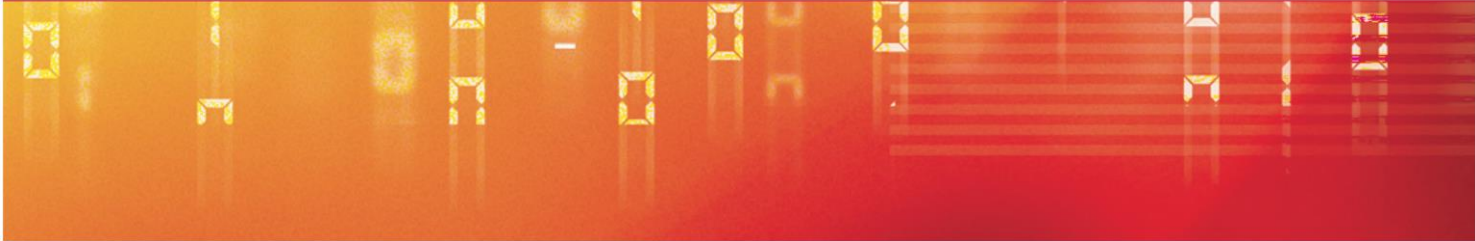
Department and Agency Management Boards, in conjunction with their Senior Information Risk Owner (SIRO), **must** produce and communicate an information risk appetite statement.

37. Good corporate governance requires that organisations identify and manage the risks to their business; this involves senior risk stakeholders in conjunction with the Management Board determining the levels of risk that they are prepared to tolerate in pursuit of their business objectives. This determination, referred to as 'risk appetite', will influence an organisation's business strategy, plans and

## Information Risk Management

policies, which will in turn determine risk tolerance levels for individual business activities and enable the delegation of risk management responsibilities with clear thresholds.

38. This determination is also applicable to information risk. An organisation's information risk appetite statement is the Management Board's primary means of communicating the level of information risk the Department or Agency can accept in balancing the benefits of taking a risk, against the impact of compromise of its information assets. As the Information Security Strategy owner, the SIRO **must** actively demonstrate the Management Board's endorsement of, and commitment to, the information risk appetite statement by signing it on their behalf.
39. Organisations will have a number of, (probably differing), levels of information risk appetite for the strategic, tactical and operational aspects of the business, as well as for the various areas of business activity, its business relationships with other organisations and delivery partners, its short and long term business strategies, and even at different times of the year for seasonal business.
40. Departments or Agencies may also choose to have multiple information risk appetites possibly containing a number of levels within each, as a result of the markedly different business activities and associated technical risks that they face. There is no 'ideal' way for how organisations should choose to communicate information risk; be it through a single appetite statement with one level, through to multiple appetite statements with a number of levels; however it should be clearly understood and reflect the circumstances of the business.
41. Information risk appetite statements are not unchanging; the 'levels' that have been set will need to be revisited by the Board to ensure that they represent manageable risk.
42. When developing or using a shared service, each subscribing organisation will have its own information risk appetite statement so a common 'level' will have to be established. Each subscribing organisation should consider their use of that shared service and the information which is being shared and exchanged. They should use this context to help shape the production of a common information risk appetite statement for the shared service community. An information risk appetite statement **must** be created for the shared service, with input from all involved stakeholders and communicated by the provider. Further detail on information risk appetite including levels and example statements is available in Chapter 2 – Departmental IA Policies, Standards, Guidelines and Procedures and Chapter 3 – Information Risk Management – Shared Services of GPG 47 (reference [c]).
43. Risk tolerance allows for variations in the amount of information risk an organisation is prepared to tolerate for a particular business or project activity. It is



recognised that the amount of risk organisations will tolerate will vary depending on the nature of their business or project activities; however local tolerance decisions should be guided by the overall information risk appetite.

## Departmental IA Policies

### RISK MANAGEMENT REQUIREMENT 6

The SIRO, in conjunction with the Lead Accreditor **must** produce and communicate an Accreditation Policy that defines a proportionate and accountable approach, and includes their requirements of the RMADS, and the conditions for re-accreditation.

44. This RMR supports SPF MR 8. By establishing and communicating an Accreditation Policy the SIRO has the ability to define a strategic approach to accreditation and re-accreditation, which can for example, include the terms for proportionality, and the requirements of the document set; this is critical for cost savings and business objectives to be realised.
45. The Lead Accreditor should use the policy to establish their expectations of the document set so that a balance is agreed between the necessary information for an accreditation decision to be reached and the resources available to achieve this. The scope and complexity of the RMADS should be proportionate and appropriate to the system or service being accredited. There is no reason why simple systems cannot have a short and basic RMADS.
46. The RMADS provides the Accreditor with the basis for judging whether or not the identified risks are being managed appropriately and effectively and is used as the basis for their decision making. Further information on Accreditation Policy is available in Chapter 4 – Accreditation of GPG 47 (reference [c]).

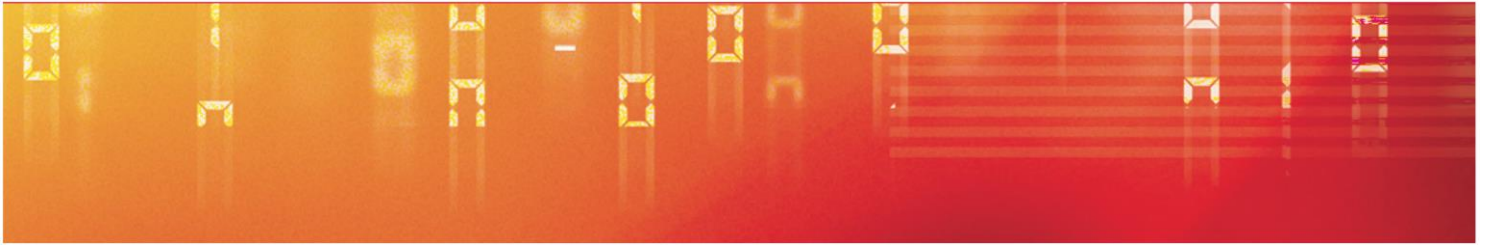
### RISK MANAGEMENT REQUIREMENT 7

Departments and Agencies **must** produce and implement an Education and Training Policy for all mandatory and specialist security roles as defined by the SPF and HMG IA Standards.

47. This RMR supports SPF MR 3. Education and awareness is essential to supporting the effectiveness of information risk management. Increasingly specialised security roles will demand a level of demonstrable professionalism, which can be provided through training and certification; this will assist them with performing their duties effectively.

## Information Risk Management

48. CESA are actively supporting RMR 7 through their IA Professionalisation, Education and Training (PE&T) programme, which aims to raise the level of IA professionalism and skills across HMG, the wider public sector and their suppliers to improve information risk management.
49. Specialist security roles such as Lead Accreditor (LA), Information Technology Security Officer (ITSO) and Security & Information Risk Advisor (SIRA), are professional competencies and are not a function that should be undertaken without training and a proven track record of IA in a business environment. CESA is developing a framework for certifying IA specialists who meet the competency and skills requirement for specialist IA roles. Further information is available via CESA's external website at the following URL: [http://www.cesa.gov.uk/publications/Documents/certification\\_for\\_ia\\_specialists.pdf](http://www.cesa.gov.uk/publications/Documents/certification_for_ia_specialists.pdf).



ARCHIVE

THIS PAGE IS INTENTIONALLY LEFT BLANK

## Chapter 3 - Technical Risk Assessment and Risk Treatment

### Key Principles

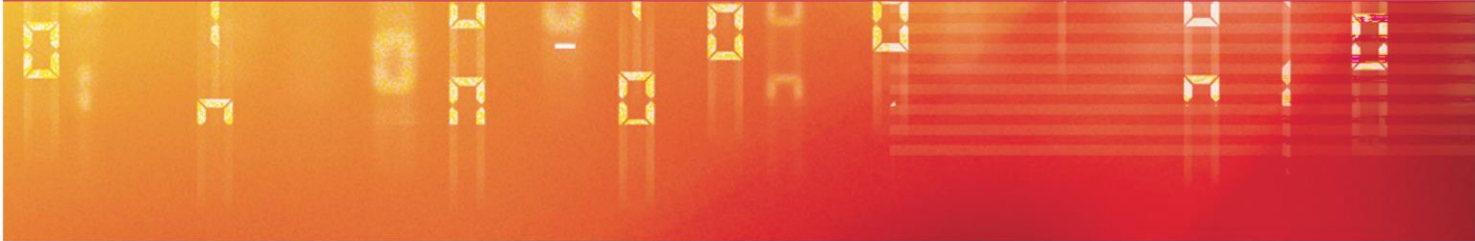
- A repeatable and consistent approach to assessing technical risk **must** be used by Departments and Agencies; it **must** include a business impact and threat assessment
- The output of the technical risk assessment **must** be endorsed by the Accreditor or their delegated authority, and **must** be used as the basis for any information risk management decisions
- Departments and Agencies should treat the technical risks to their information assets in an appropriate and proportionate manner
- The selection of controls and the approach to their implementation **must** be endorsed by the Accreditor or their delegated authority
- Organisations will increasingly rely on service providers for their security requirements, therefore the right to audit these **must** be included in all new ICT contracts

### Technical Risk Assessment

#### RISK MANAGEMENT REQUIREMENT 8

Departments and Agencies **must** assess the technical risks to the Confidentiality, Integrity and Availability of their ICT systems or services. A technical risk assessment **must** be conducted at the start of all HMG ICT projects or programmes, and **must** be refined to reflect any change. The findings of all technical risk assessments **must** be reviewed at least annually to identify any changes to threat, vulnerability or impact.

50. This RMR supports SPF MR 8. A repeatable and consistent approach to technical risk assessment **must** be used; the method **must** incorporate a business impact and threat assessment. A stepped technical risk assessment methodology is presented in the Supplement to this Standard, which **must** be used; it provides a repeatable and consistent approach for Departments and Agencies to follow.
51. As discussed any technical risk assessments should be supported and contextualised by business activities and wider risk management processes such as corporate risk appetite and Departmental risk registers. Without this business context organisations will not necessarily consider all the risks that should be captured by the Assessment Scope. For example, the technical risk assessment



methodology presented in this Supplement to this Standard does not support the consideration of risk from a stakeholder's (the citizen's) perspective. However, this is still an important consideration for organisations to make and should contextualise the overall technical risk assessment. Extensive work has already been conducted with regards to identifying and understanding stakeholder risk, and guidance on this is available in CESG Good Practice Guide No. 43 (GPG 43), Requirement for Secure Delivery of Online Public Services (RSDOPS) (reference [g]).

52. CESG support a flexible approach when using the technical risk assessment methodology it provides in the Supplement; whilst the stepped process is mandated, the way in which organisations work with each stage should be proportionate and cost effective and reflect the needs of the business. In particular the mandatory component of the technical risk assessment is the analysis, **not** the generation of forms. Whilst the use of forms provided in the Supplement is recommended, it is not mandatory; as long as the relevant information is captured and analysed the policy requirements can be considered met; organisations may choose to achieve this through the use of software tools.
53. There may be situations where organisations choose to conduct a snapshot technical risk assessment as a precursor to the detailed analysis that Steps 1 – 6 of the Supplement provides, this can assist with the following:
  - In support of change management processes for dynamic systems or services where components are being regularly upgraded or replaced
  - The technical risk assessment of simple or less complex systems, such as standalone laptops or small office networks with no interconnections
  - In support of Urgent Operational Requirements (UOR) where a more detailed risk assessment cannot be conducted because of time constraints
  - At the start of ICT projects or programmes in order to establish the information security context for the proposed business activities
  - To assist in outline project plans and budgetary estimates for providing controls
54. The purpose of the snapshot technical risk assessment is to produce a general understanding of technical risk. A snapshot technical risk assessment can be used to help the Accreditor decide how much more detailed analysis is needed.
55. Organisations that face resource constraints may decide that a less detailed approach to technical risk assessment is more proportionate and cost effective. The decision to conduct a snapshot technical risk assessment in lieu of a more detailed technical risk assessment **must** be endorsed by the Accreditor or their delegated authority. An organisation's Accreditation Policy should include the

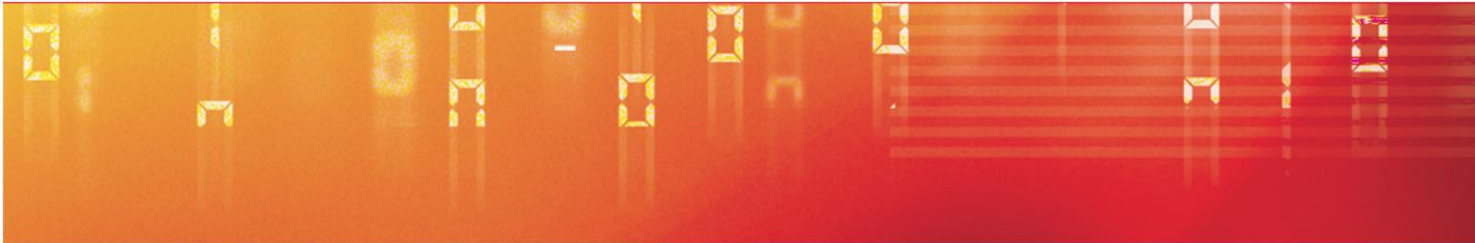
circumstances for when a snapshot technical risk assessment is to be used; further information is available in Chapter 4 – Accreditation of GPG 47 (reference [c]). The Accreditor or their delegated authority may require that a more detailed technical risk assessment is conducted after a snapshot technical risk assessment has been completed. Further information on snapshot technical risk assessment is provided in the Supplement to this Standard.

56. A technical risk assessment, whilst important, is a precursor to effective information risk management. The management of information risk through treatment, (the selection and implementation of controls), is where organisations should direct their resources, (especially when they are constrained).
57. Departments and Agencies should note that an annual review of technical risk is unlikely to require a completely new assessment. If there have been no significant changes to the components of risk or the technologies that form the Assessment Scope, then a review can be conducted that simply provides confirmation of this. A series of review points have been added to the technical risk assessment methodology to assist with this.
58. An example of a significant change to a component of risk could be an increase to the Threat Level. For example, a new Threat Source has been identified as actively targeting the HMG ICT system or service under consideration and it has been assessed that they possess an increased capability and priority over those that form part of the existing Assessment Scope.
59. Departments and Agencies should conduct their technical risk assessment whilst taking into account wider corporate risk management activities. It is recommended that any technical risk assessments are supported and contextualised by corporate risk appetite and Departmental risk registers, and that, where appropriate, the output contributes to the overall understanding of risk amongst the organisation's risk stakeholders. Further information is available in Chapter 2 – Departmental IA Policies, Standards, Guidance and Procedures of GPG 47 (reference [c]) in support of this.

### RISK MANAGEMENT REQUIREMENT 9

A business impact assessment, using Business Impact Levels (ILs), **must** be conducted against the Accreditation Scope; its findings **must** be endorsed by the Information Asset Owner (IAO) or their delegated authority, in conjunction with the Accreditor and inform the technical risk assessment.

60. This RMR supports the SPF which states that 'Departments and Agencies **must** use 'Business Impact Levels', also known simply as Impact Levels (ILs), to assess



the level of impact from a compromise of Confidentiality, Integrity and Availability'. ILs, in conjunction with the GPMS is to be used by Departments and Agencies to provide them with the means to consistently identify and assess the impacts to the business through a loss of Confidentiality, Integrity or Availability of data and ICT systems or services, should the risks be realised. Further information on business impact is available in the Supplement to this Standard.

61. It is highly probable that a number of different stakeholders from across the organisation, led by the IAO, will need to contribute to the information asset identification and valuation process, and thus any associated IL marking. It is believed that such an approach will help Departments and Agencies to produce a more rounded and realistic business impact assessment should the risks be realised.
62. Business impact assessments should be made in terms of the likelihood of compromise in a typical business context in which the organisation uses the information asset(s); this should be based upon a reasonable, informed assessment of actions by Threat Sources or Actors in the typical course of events.

#### **RISK MANAGEMENT REQUIREMENT 10**

A technical threat assessment **must** be conducted against the Accreditation Scope; its findings **must** be endorsed by the Accreditor or their delegated authority, and inform the threat levels of the technical risk assessment.

63. A technical threat assessment can be conducted in-house or be obtained from relevant authorities: CESG, the Centre for the Protection of National Infrastructure (CPNI), or the Ministry of Defence (MoD) can request threat information from Defence Intelligence (DI). When organisations are conducting an in-house technical threat assessment they **must** use the components of technical threat: priority or motivation and capability, as presented in the Supplement to this Standard, as the basis for their assessment.
64. In most instances an in-house technical threat assessment will be more appropriate; as it will probably encompass a more specific appreciation of the technical threats the Department or Agency faces, and this will be contextualised by an understanding of the business activities. A number of different areas of the business can contribute to the technical threat assessment through supporting processes such as accounting, audit, monitoring and security incident reviews. Further information on technical threat is available in CESG Technical Threat Briefing No. 1, Assessment of Technical Threat (reference [h]).

## Information Risk Management

65. There will be situations where it is advisable for organisations to obtain an external technical threat assessment from the authorities because of the scale or nature of their business activities. For example, national or Pan Government ICT programmes.
66. To request technical threat information from CESG, organisations can contact their CESG Customer Account Manager (CAM), or the Threat Assessment team: at [threat@cesg.gsi.gov.uk](mailto:threat@cesg.gsi.gov.uk), or by telephoning 01242 221491 ext 30165. Please note that CESG's capacity for producing technical threat assessments is limited and subject to a prioritisation process.
67. To request non-technical threat information from CPNI, organisations can contact: [enquiries@cpni.gov.uk](mailto:enquiries@cpni.gov.uk) or telephone 020 7233 8181.
68. Vulnerability is another significant component of technical risk and should be used to further contextualise the technical threat assessment. The methodology presented in the Supplement to this Standard depicts vulnerability as an abstraction which should be considered as part of the compromise methods and attacks associated with threat. The assessment of vulnerability and associated compromise methods should be conducted in the context of the system or service under consideration.

### RISK MANAGEMENT REQUIREMENT 11

The findings of the technical risk assessment **must** be endorsed by the Accreditor or their delegated authority.

69. The findings of the technical risk assessment **must** be used as the basis for any information risk management decisions and should be presented to the Accreditor in a format that has been agreed with them. Areas of concern, (such as high risk levels), should be brought to the Accreditor's attention. This is easier to achieve if areas of concern are not concealed amongst the details of hundreds of 'Very Low' or 'Low' risks.



## Shared Services

### RISK MANAGEMENT REQUIREMENT 12

Providers of shared services to HMG **must** supply Departments and Agencies with a residual risk statement and the corresponding Assessment Scope so that they can understand and review the risks to their own information assets. The SIRO of the subscribing organisation is ultimately responsible for the risk associated with any Departmental information being handled, stored or processed by the shared service.

70. Commercial shared service providers to Government, **must** conduct a technical risk assessment in line with the methodology presented in the Supplement to this Standard, where it is proposed that they will handle, store or process information with an IL of 3 or above for Confidentiality, Integrity or Availability. This will provide assurance to the users of the shared service that a consistent and proven technical risk assessment methodology has been followed.
71. Where it is proposed that a commercial provider of a shared service to Government will handle, store or process information with an IL of 2 or below they will not be expected to conduct a technical risk assessment in line with the methodology presented in the Supplement to this Standard. Instead assurance will be achieved by them gaining ISO27001 certification to a scope agreed with the Accreditor.
72. A mutual approach to trust will need to be adopted amongst the users of a shared service so that the benefits of collaboration, efficiencies and cost savings can be fully realised; however this does **not** mean that the responsibility for information risk has been transferred to the provider. Where appropriate, provisioned shared services should form part of an organisation's Reliance or Assessment Scope when conducting a technical risk assessment for their own information assets.
73. It is important to note that the organisation's Management Board will still own the risks to their information even where their services have been outsourced or are part of a multi-organisation shared service. Further information is available in Chapter 3 – Information Risk Management – Shared Services of GPG 47 (reference [c]) in support of this.

## Risk Treatment

### RISK MANAGEMENT REQUIREMENT 13

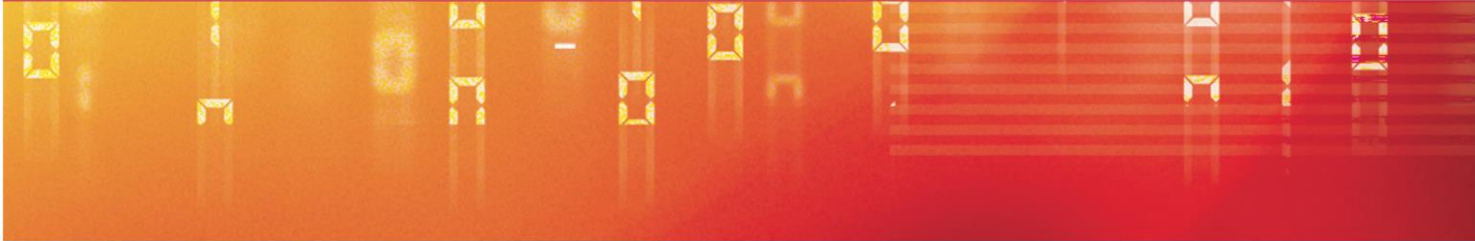
The findings of the technical risk assessment **must** inform and substantiate the selection, and implementation approach of the controls used to treat the identified technical risks. The approach to selection and implementation **must** be endorsed by the Accreditor or their delegated authority.

74. The output of the technical risk assessment will typically be a consolidated and prioritised list of risks, (a risk register), and this **must** be used as the basis for any information risk management decisions that are to be taken by organisations. A mapping should be established between the risks that are to be treated and the type of control, (this can be physical, personnel or procedural as well as technical), and the expected implementation of that control. If this mapping does not take place then not only is there a likelihood that some of the controls will be unsuitable, but that resources and funding will be misapplied.
75. The Supplement to this Standard presents the concept of the Segmentation Model, which aims to segment responses to information risk at the various levels in both an appropriate and proportionate manner. It is believed that this approach will promote the implementation of controls in a pragmatic, appropriate and cost effective way and that the risks will be managed in a manner that supports the organisation's objectives. Any information risk management activities should be proportionate, align with the organisation's information risk appetite and tolerance levels and be able to adapt to meet changing business requirements. Further information on the selection and implementation of controls and the Segmentation Model is available in the Supplement to this Standard.
76. The selected controls should form the basis of a risk treatment plan which can underpin the more specific functional security requirements of the system or service under consideration.

### RISK MANAGEMENT REQUIREMENT 14

The risk treatment plan **must** include as a minimum the mandatory protective controls from the SPF, HMG IA Standards and other relevant Tier 4 policy documents.

77. The risk treatment plan will typically form part of the RMADS and support the security case. Any risk treatment plan will have to define how it meets the relevant Mandatory Requirements in the SPF and HMG IA Standards as well as the



Information Risk Management Policy. For example, if the risk treatment plan includes the use of cryptographic controls to manage the risk of interception of protectively marked information as it traverses an untrusted network it would have to detail how it complied with HMG IA Standard No. 4 (IS4), Management of Cryptographic Systems (reference [i]).

### **RISK MANAGEMENT REQUIREMENT 15**

By default every HMG information system or service with a Business Impact Level (IL) of 3 or above, for either: Confidentiality, Integrity or Availability, **must** implement the full set of controls as defined in the Baseline Control Set of the Supplement to this Standard.

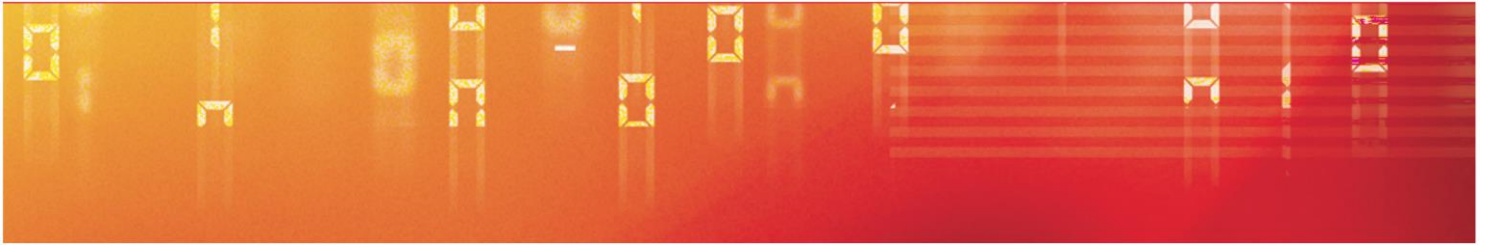
78. Where it is proposed that a commercial provider of a shared service to Government will handle, store or process information with an IL of 2 or below they are not expected to implement the full set of controls as defined in the Baseline Control Set of the Supplement to this Standard. Instead assurance will be achieved by them gaining ISO27001 certification to a scope agreed with the Accreditor.
79. For information systems or services with an IL of no more than 2, for each of Confidentiality, Integrity or Availability, the Baseline Control Set (BCS) should be consulted to help determine appropriate controls. Application of these controls is left to the Accreditor's discretion or their delegated authority.
80. Situations may occur where stakeholders from the business have taken the decision not to apply a particular control because it is demonstrably not appropriate or reasonable to do so. Where this is the case this **must** first be endorsed by the Accreditor or their delegated authority, and it should be captured in the risk treatment plan. For example, there may be a situation where an organisation is processing IL3 information on a standalone system, which is physically separate from the rest of the organisation's ICT, which is processing IL1 information. The Accreditor or their delegated authority is responsible for deciding whether the application of the full set of baseline controls to the standalone system is appropriate and proportionate or not.
81. There are large economies of scale when controls are designed, deployed and operated across the whole organisation instead of system by system or service by service. Designing, deploying and operating controls across the whole organisation promotes consistency and standards that can support and facilitate the accreditation process. Controls can be provided by enterprise wide management processes and common infrastructure services/components; therefore only a subset of the controls presented in the Baseline Control Set need

be implemented or augmented in respect of an individual system or service. Controls can be selected from enterprise standards or from other control sets or new controls can be designed to meet specific needs as appropriate. Further information is available in GPG 28 (reference [e]).

### RISK MANAGEMENT REQUIREMENT 16

All new ICT contracts **must** include the right for Departments and Agencies to audit the services and security requirements being provided to them.

82. This RMR supports SPF MR 11. Increasingly Departments and Agencies are relying on contractual agreements with service providers to deliver their security requirements. In order for this to be effective, business and security requirements need to be clearly communicated to those with contractual responsibility so that they are understood and incorporated into contracts and service agreements.
83. Departments and Agencies will have established processes, (such as an audit function), that they currently use internally as a means of providing implementation and operational assurance; these can be adapted for use with service providers. Departments and Agencies should define what is required as evidence of compliance from the service provider; for example, this can be based on key controls from the Baseline Control Set.
84. Departments and Agencies should take a risk based approach to identify those service providers they decide to undertake auditable activity on. Obtaining evidence of compliance can be achieved in a number of ways:
  - Receiving evidence of compliance from an independent audit function such as the PGA
  - Receiving evidence of compliance from the service provider's audit function
  - Requesting the service provider conducts an independent audit against the security requirements using their own resources to provide evidence of compliance, (this may need to be expressly stated in the contract)
  - Conducting a site visit and requesting to see evidence of compliance



THIS PAGE IS INTENTIONALLY LEFT BLANK

ARCHIVE

## Chapter 4 - Accreditation Requirements

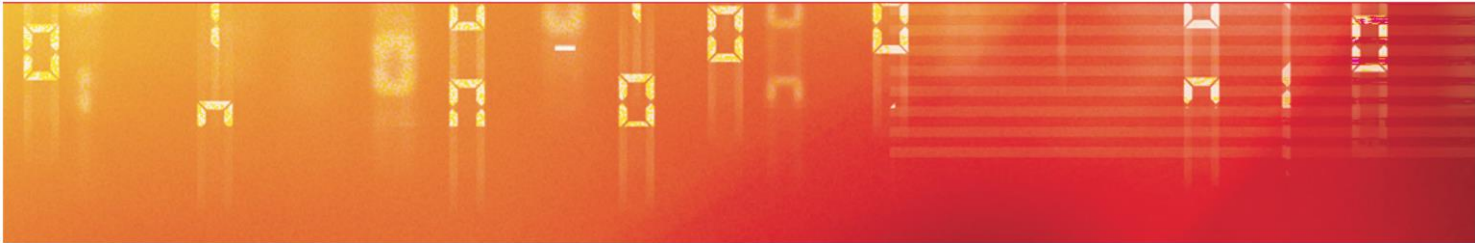
### Key Principles

- Engaging with the Accreditor or their delegated authority, will provide ICT projects and programmes with the requirements for an accreditation decision. Any deliverables should be proportionate and appropriate to the level of complexity and risk to the system or service being accredited
- Assurance activities are used to ascertain and support the effectiveness of the selected controls
- Residual risks will remain after treatment and any management decisions should be taken in the context of the organisation's information risk appetite and tolerance levels
- Any management decisions for residual risks that are at variance with the organisation's information risk appetite **must** be endorsed by the SIRO or their delegated authority

### RISK MANAGEMENT REQUIREMENT 17

The Accreditor or their delegated authority **must** be involved at the start of all ICT projects or programmes so that the requirements for accreditation can be agreed and are clearly understood.

85. Organisations should use their Accreditation Policy as a means of delegating authority and communicating the requirements for accreditation. By engaging with the Accreditor or their delegated authority at the earliest opportunity, ICT projects and programmes will be provided with the requirements for an effective accreditation decision; this allows for project and programme managers to plan and resource for this accordingly. Accreditor oversight should be provided throughout the ICT project or programme with, for example, representation at the following:
- Risk Working Groups
  - Threat Assessment Workshops
  - Security Working Groups
  - Change Advisory Boards
86. Any deliverables should be proportionate and appropriate to the level of complexity and risk to the system or service being accredited. The Accreditor may insist that a snapshot technical risk assessment is conducted in support of the ICT project or programme start-up.

- 
87. A security case will be used by the Accreditor as a basis for deciding whether the risks have been appropriately managed or not. An important aspect of this will be the residual risk assessment which will demonstrate to the Accreditor that the risks have been managed effectively, (or not as the case may be), through treatment and accreditation activities.
88. Any accreditation decisions should be taken within the context of the organisation's information risk appetite and tolerance levels, whilst ensuring that business objectives are met and the expectations of risk stakeholders are accommodated. The Accreditor will be better placed to achieve this on behalf of the risk owners if the evidence presented to them is concise, pertinent and comprehensible.

#### **RISK MANAGEMENT REQUIREMENT 18**

Security Operating Procedures (SyOPs) **must** be produced for all users or providers of HMG ICT systems or services. Users or providers **must** sign to acknowledge that they understand the content of the SyOPs, and that they will follow its procedures.

89. The SyOPs should identify the procedures to be carried out by the users or providers of HMG ICT systems or services in order to reduce the likelihood of compromise and to support the implemented controls. SyOPs should be concise and where possible role based, this ensures that the individual understands only those procedures that are needed for them to perform their duties. Departments and Agencies should note that SyOPs are applicable to all members of an organisation who use or provide that given ICT system or service, and are a useful means of providing traceability and accountability. Senior management participation provides visible endorsement and support to the organisational information risk management processes in place.
90. SyOPs should not be produced in isolation of wider System Operating Procedures (SOPs); SOPs should include the requisite security procedures where appropriate. A benefit of issuing the users or providers of an ICT system or service with the necessary operating procedures will be a reduction of accidental compromise.

#### **RISK MANAGEMENT REQUIREMENT 19**

Assurance activities **must** be implemented which ascertain and support the ongoing effectiveness of the controls selected to treat the identified technical risks. These assurance activities **must** be endorsed by the Accreditor or their delegated authority.

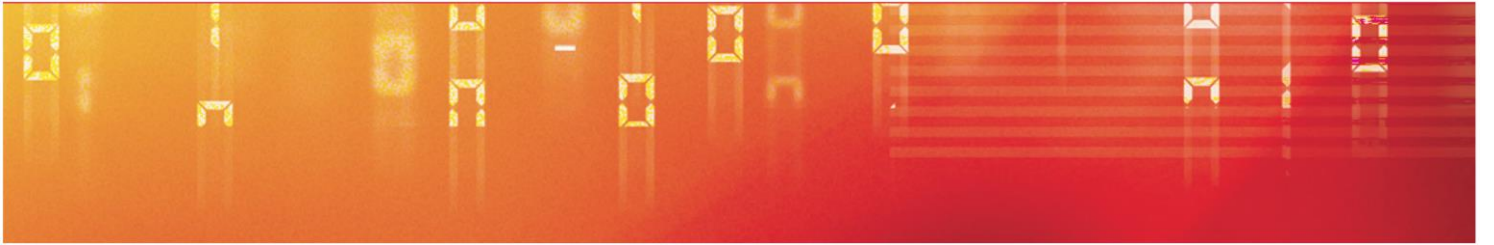
provides a snapshot of the effectiveness of a control, therefore assurance should be sought from all key security enforcing controls: physical, personnel or procedural as well as technical, and continue throughout the lifecycle of the ICT system or service; this approach is as important as the activities themselves. Assurance is equally applicable to services and systems as well as products.

92. Assurance activities should be proportionate and appropriate to the risks that Departments and Agencies face. Formal sources of assurance may be costly and time consuming, (and so where possible), should be pragmatic, appropriate and cost effective so that the maximum benefit is realised. Any solution or assurance gaps should also be included in the RMADS. Further information on assurance is available in CESG Good Practice Guide No. 30 (GPG 30), Assurance of ICT Systems and Services (reference [jj]).

### **RISK MANAGEMENT REQUIREMENT 20**

If the residual risks are at variance with the information risk appetite they **must** be escalated within the IA Governance Framework, any ensuing management decisions **must** be endorsed by the SIRO or their delegated authority.

93. Departments and Agencies should note that residual risks will remain after treatment activities. Any residual risk management decisions should be taken in the context of the organisation's information risk appetite and tolerance levels, whilst ensuring that business objectives are met and the expectations of risk stakeholders are accommodated. The approach to the treatment of risk may even need to be reviewed where necessary to address any functional shortcomings or assurance gaps. Guidance on residual risk assessment can be found in the Supplement to this Standard.
94. An organisation's corporate risk register should include those residual risks that have been escalated within the IA Governance Framework to the SIRO or their delegated authority and subsequently accepted by them.

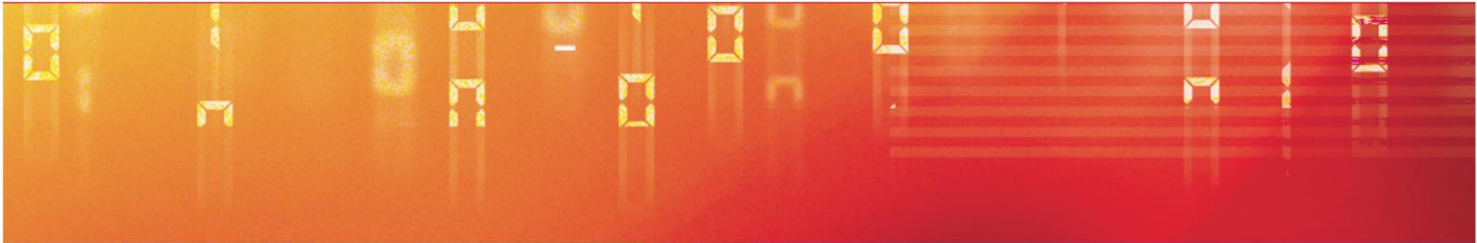


ARCHIVE

THIS PAGE IS INTENTIONALLY LEFT BLANK

## References

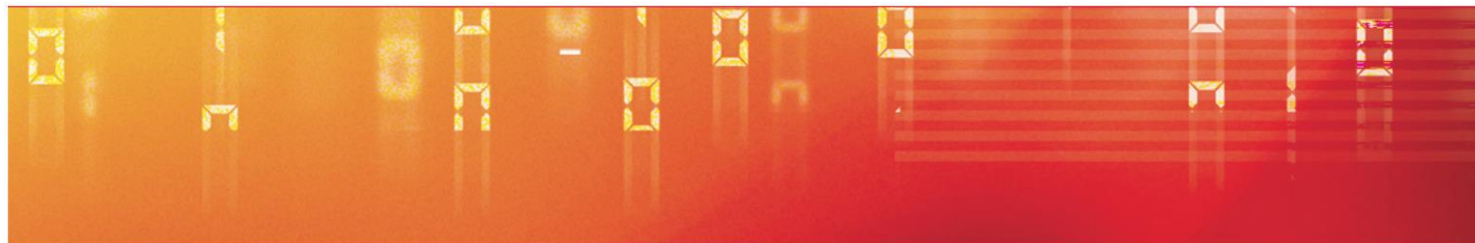
- [a] HMG Security Policy Framework. Tiers 1-3 (Not Protectively Marked). Available at <http://www.cabinetoffice.gov.uk/resource-library/security-policy-framework>
- [b] HMG IA Standard Nos. 1 & 2 – Supplement Technical Risk Assessment and Risk Treatment Issue 1.0, April 2012 (UNCLASSIFIED). Available from the CESG IA Policy Portfolio.
- [c] CESG Good Practice Guide No. 47, Information Risk Management, Issue 1.0, April 2012 (UNCLASSIFIED). Available from the CESG IA Policy Portfolio.
- [d] CESG Good Practice Guide No. 40, The Information Assurance Maturity Model and Assessment Framework, Issue 1.0, May 2011. Available from the CESG IA Policy Portfolio.
- [e] CESG Good Practice Guide No. 28, Improving Information Assurance at the Enterprise Level, Issue 1.1, September 2010 (UNCLASSIFIED). Available from the CESG IA Policy Portfolio.
- [f] HMG IA Standard No. 6, Protecting Personal Data and Managing Information Risk, Issue 2.0, October 2011 (UNCLASSIFIED). Available from the CESG IA Policy Portfolio.
- [g] CESG Good Practice Guide No. 43, Requirements for the Secure Delivery of Online Public Services (RSDOPS), Issue 1.0, (UNCLASSIFIED). In production, available soon.
- [h] CESG Technical Threat Briefing No. 1, Assessment of Technical Threat, Issue 1.1, October 2011 (UK RESTRICTED). Available from the CESG IA Policy Portfolio.
- [i] HMG IA Standard No. 4, Management of Cryptographic Systems, Issue 5.1, April 2012 (UNCLASSIFIED). Available from the CESG IA Policy Portfolio.
- [j] CESG Good Practice Guide No. 30, Assurance of ICT Systems and Services, Issue 1.0, April 2011 (UNCLASSIFIED). Available from the CESG IA Policy Portfolio.



ARCHIVE

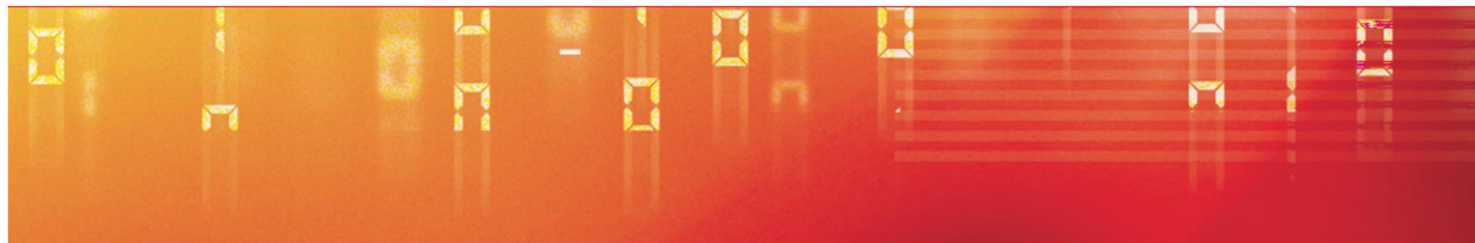
## Glossary

<b>Accreditation</b>	Accreditation is the formal, independent assessment of an ICT system or service against its IA requirements, resulting in the acceptance of residual risk in the context of the business requirement and information risk appetite. This will be a prerequisite for approval to operate.
<b>Accreditation Scope</b>	The Accreditation Scope includes all of the capability and services for which the project is responsible for delivering and accrediting. This will typically be the same as the scope of the project.
<b>Agreed Information Threshold</b>	The Agreed Information Threshold (AIT) is a means by which the stakeholders of a shared service can agree a common and consistent approach to the risk management of data aggregation.
<b>Aggregation</b>	Aggregation is where the business impact of compromise of a set of assets is greater than the impact of an individual compromise. This could be due to accumulation of information or because of association of assets with each other.
<b>Analysis Scope</b>	The Analysis Scope includes everything that is part of the risk assessment. This includes everything that is part of the Accreditation and Reliance Scope as well as considering business information exchange requirements and system connections.
<b>Analyst</b>	The Analyst is the person(s) who are conducting the technical risk assessment and risk treatment activities; the person following the technical risk assessment and risk treatment methodologies presented in the Supplement to this Standard. These activities are typically managed by the Security and Information Risk Advisor (SIRA).
<b>Asset</b>	Anything that has value to the organisation, its business operations and its continuity.
<b>Assurance</b>	Assurance is the confidence that controls perform the functions expected of them. Assurance can come from many different sources such as trust of the manufacturer (Intrinsic Assurance) or through testing and evaluation (Extrinsic assurance).



<b>Assurance Framework</b>	The Assurance Framework is a conceptual model that considers assurance throughout the lifecycle of an ICT system or service. The framework presents four elements of assurance: Intrinsic, Extrinsic, Implementation and Operational.
<b>Assurance Plan</b>	The assurance plan describes how appropriate assurance will be gained in all controls applied to manage information risk. Additionally the plan describes any assurance gaps and forms part of the security case.
<b>Assured Products</b>	IT products that have a formally recognised level of security efficiency.
<b>Availability</b>	The property of being accessible and usable upon demand by an authorised entity.
<b>Business Continuity</b>	Strategic and tactical capability of the organisation to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable pre-defined level (BS 25999-1)
<b>Business Continuity Plan</b>	The Business Continuity Plan (BCP) is a documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident to enable an organisation to continue to deliver its critical activities at an acceptable pre-defined level [BS 25999-1).
<b>Baseline Control Set</b>	The Baseline Control Set (BCS) contains a single set of protective controls that should be considered as the HMG baseline for managing information risk.
<b>Business Impact</b>	The result of an information security incident on business functions and the effect that a business interruption may have upon them.
<b>Business Impact Level</b>	A Business Impact Level (IL) is a numeric indicator of the level of impact likely to result from the compromise of Confidentiality, Integrity or Availability of an asset. It is a seven point scale ranging from IL0, (no impact), to IL6 (maximum impact).
<b>Capability</b>	Capability is the component of threat and a characteristic of a Threat Actor or Threat Source. It defines a level, which indicates the types and technical sophistication of the threat.

<b>Code of Connection</b>	A Code of Connection (CoCo) is an agreement on the policy and rules for the connection of internal or external ICT systems or services, which are subject to different management or accreditation domains.
<b>Confidentiality</b>	The property that information is not made available or disclosed to unauthorised individuals, entities, or processes.
<b>Control Measure</b>	Control measures are determined from control objectives to describe controls that are appropriate for the system or service under consideration. These measures should be at a level of detail consistent with how much is known about the system architecture at that point.
<b>Control Objectives</b>	A Control Objective describes functionally and the purpose of a control, but may not define how that control will be achieved or implemented.
<b>Compromise Method</b>	A compromise method is the broad type of attack by which a Threat Actor type may attempt to compromise the Confidentiality, Integrity or Availability of an asset.
<b>Critical National Infrastructure</b>	The Critical National Infrastructure (CNI) is those infrastructure assets that are vital to the continued delivery and integrity of the essential services upon which the UK relies.
<b>DEFEND</b>	DEFEND is a conceptual level of the Segmentation Model which presents a bespoke implementation approach to the controls presented in the Baseline Control Set to protect against the most sophisticated and highly capable Threat Actors (Formidable capability), such as those enhanced by Foreign Intelligence Services.
<b>DETECT &amp; RESIST</b>	DETECT & RESIST is a conceptual level of the Segmentation Model which presents a robust implementation approach to the controls presented in the Baseline Control Set to protect against targeted attacks from skilled Threat Actors (Significant capability) using bespoke tools that exploit known vulnerabilities.
<b>DETER</b>	DETER level is a conceptual level of the Segmentation Model aims which presents a Government good practice implementation approach to the controls presented in the Baseline Control Set to protect against targeted attacks from



the Internet by skilled Threat Actors (Limited capability) using freely available tools with bespoke modification.

<b>Disaster Recovery</b>	The process of recovering from an emergency, including the immediate aftermath and priorities for the critical business functions which need to be resumed.
<b>Extrinsic Assurance</b>	Extrinsic assurance is the actions and activities that are undertaken independently of the development environment, and that seek to find vulnerabilities through the response of the ICT system or service to context, threat and risk informed stimuli through independent testing.
<b>Focus of Interest</b>	A Focus of Interest (Fol) is a collection of assets, with associated features that are the subject of a given risk assessment. In essence, a Fol simply acts to conveniently group assets so that a risk assessment can be conducted for the group, rather than requiring an assessment of each individual component.
<b>Forensic Readiness</b>	The achievement of an appropriate level of capability by an organisation in order for it to be able to collect, preserve, protect and analyse digital evidence so that this evidence can be effectively used in any legal or disciplinary matters, in an employment tribunal or in a court of law.
<b>IA Governance Framework</b>	An organisational structure which defines individuals with responsibility and accountability for key information risk management processes including: technical risk assessment, risk treatment, risk ownership, accreditation and the remit of delegation.
<b>Impact</b>	The result of an information security incident, caused by a threat, which affects assets.
<b>Implementation Assurance</b>	Implementation Assurance is the actions and activities necessary to combine one or more components and so establish and verify the properties of an ICT system or service

# Information Risk Management

such that they meet the needs of the business at an acceptable level of risk.

## **Information Assurance**

Information Assurance (IA) is the confidence that information systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users.

## **Integrity**

The property of safeguarding the accuracy and completeness of assets - this may include the ability to prove an action or event has taken place, such that it cannot be repudiated later

## **Intrinsic Assurance**

Intrinsic assurance is the actions and activities necessary to understand the risks associated with the origin of an ICT system, service or solution.

## **Information Security**

Preservation of Confidentiality, Integrity and Availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved [ISO/IEC 27001]

## **Information Security Management System (ISMS)**

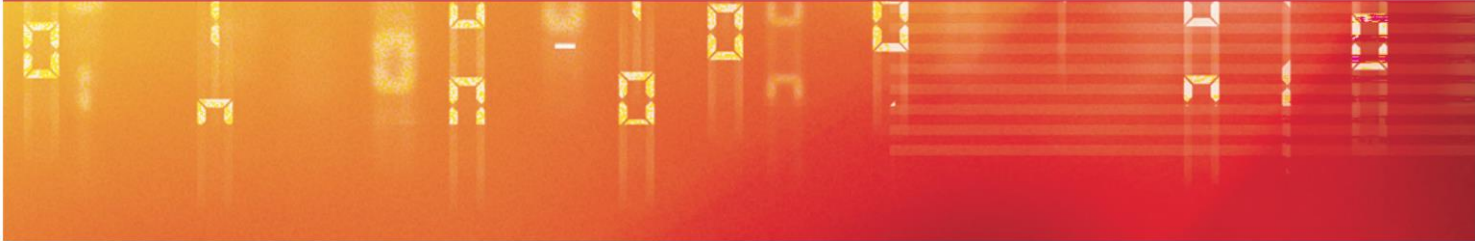
That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security (within the defined ISO/IEC 27002 scope). Note: The management system includes organisational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

## **ISO/IEC 27001**

International Standard that specifies requirements for establishing, implementing and documenting Information Security Management Systems (ISMS).

## **ISO/IEC 27002**

International Standard that defines a Code of Practice for information security management. It establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organisation. It specifies control objectives and controls that can be



implemented to meet the requirements identified by a risk assessment.

**IT Health Check**

A technical analysis of a system or service to ensure correct implementation of security functions and the identification of vulnerabilities which may compromise the Confidentiality, Integrity or Availability of information.

**Likelihood**

The probability of an attack being successfully realised (i.e. an asset being compromised).

**Memorandum of Understanding**

Memorandum of Understanding (MoU) is a mutual agreement between parties; however it is not legally binding and more akin to a gentlemen's agreement.

**Motivation**

Motivation is a measure of how much a Threat Actor is induced or encouraged to compromise an asset or group of assets.

**Operational Assurance**

The actions and activities necessary to maintain the risk assessed baseline once the ICT system or service has entered use, including provision for activities to monitor changes in vulnerability and threat.

**Plan-Do-Check-Act**

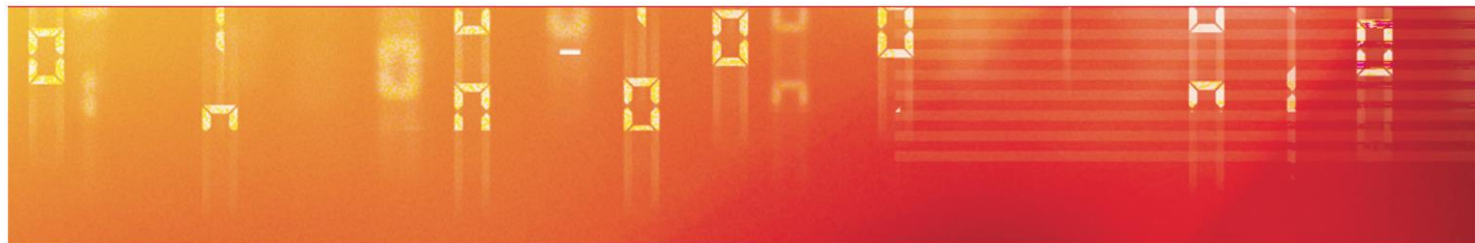
Plan-Do-Check-Act (PDCA) is the ISO/IEC 27001 "virtuous circle" model.

**Privacy Impact Assessment**

A Privacy Impact Assessment (PIA) is a structured assessment, adopting a risk management approach, of a project's potential impact on privacy, enabling Departments to anticipate and address the likely impacts of new initiatives, foresee problems and negotiate solutions.

# Information Risk Management

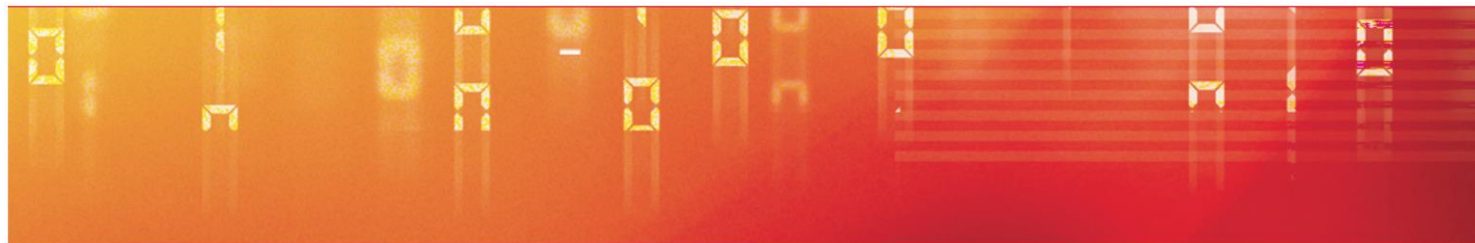
<b>Priority</b>	Priority is a measure of how much a Threat Source desires to compromise an asset or group of assets.
<b>Reliance Scope</b>	The Reliance Scope identifies capability and services that the Accreditation Scope relies upon, but is not directly supplied by the project. A trusted risk assessment and accreditation of these components is required in order to rely upon them without further analysis.
<b>Reputation</b>	The trust and value placed upon an organisation or programme by both internal and external stakeholders and/or customers. A valued asset to be protected.
<b>Residual Risk</b>	A native risk as identified by the risk assessment that has been managed through treatment and/or assurance activities.
<b>Residual Risk Indicator</b>	Residual Risk Indicator (RRI) is a qualitative gauge for the effectiveness of risk treatment and assurance activities; it can be used as an indication of confidence to build a case that demonstrates to the Accreditor that the risks have been managed effectively, (or not as the case may be).
<b>Risk</b>	The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation.
<b>Residual Risk Acceptance</b>	The decision to accept a residual risk.
<b>Risk Acceptance</b>	The decision to accept a risk.



<b>Risk Analysis</b>	The systematic use of information to identify sources and to estimate the risk.
<b>Risk Appetite</b>	Risk appetite is logically a function of the organisation's capacity to bear risk, which should not be exceeded.
<b>Risk Assessment</b>	The overall process of risk analysis and risk evaluation.
<b>Residual Risk Avoidance</b>	The decision not to be involved in, or action to withdraw from, a residual risk situation.
<b>Risk Avoidance</b>	The decision not to be involved in, or action to withdraw from, a risk situation.
<b>Risk Evaluation</b>	Process of comparing the estimated risk against given risk criteria to determine the significance of risk
<b>Risk Identification</b>	Process to find, list and characterise elements of risk.
<b>Risk Management</b>	Process of coordinating activities to direct and control an organisation with regard to risk. Defined approaches to risk management are: acceptance, avoidance, transfer or treatment.

# Information Risk Management

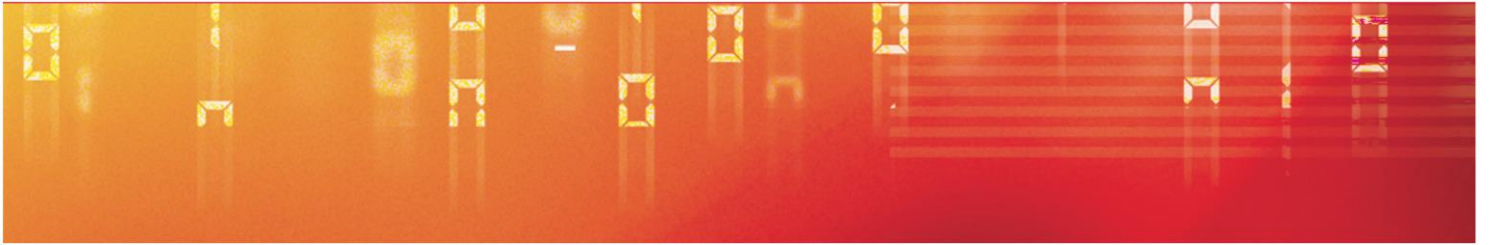
<b>Risk Management &amp; Accreditation Document Set</b>	The Risk Management & Accreditation Document Set (RMADS) is often a portfolio, which specifies the risk management measures, Accreditation Policy, and accreditation status of an ICT system or service.
<b>Risk Reduction</b>	Action taken to lessen the probability, negative consequences, or both, associated with risk
<b>Risk Register</b>	A detailed record of the risks as identified by a risk assessment methodology. An owner should be identified for each risk. Where a risk is to be reduced there should be a cross reference to the Risk Treatment Plan.
<b>Risk Tolerance</b>	Risk tolerance is closely related to risk appetite, whereas appetite refers to risk at the corporate level, risk tolerance allows for variations in the amount of risk an organisation is prepared to tolerate for a particular project or business activity.
<b>Residual Risk Transfer</b>	Sharing with another party the burden of loss or benefit of gain for a residual risk.
<b>Risk Transfer</b>	Sharing with another party the burden of loss or benefit of gain for a risk.
<b>Risk Treatment</b>	A series of mitigation activities to manage risk through the implementation of controls.
<b>Risk Treatment Plan</b>	The plan should contain detail the approach to manage risk through mitigation activities. It provides details on the controls that are being applied and the ownership of them. It will also record the implementation approach and status of each control.



<b>Security Case</b>	The security case describes how all of the identified risks have been satisfactorily treated. It includes the list of risks, a description of application of all controls, the assurance plan and any functional or assurance gaps that may be present.
<b>Segmentation Model</b>	The Segmentation Model provides a framework that ensures that the approach to the implementation of controls are both appropriate and proportionate to manage the identified risks, at a given level of impact or threat to an ICT system or service. The Segmentation Model presents three conceptual levels: DETER, DETECT & RESIST and DEFEND.
<b>Senior Information Risk Owner</b>	The Senior Information Risk Owner (SIRO) is a member of the senior management board with responsibility for IA governance and risk ownership in the organisation on behalf of the board.
<b>Shared Services</b>	Any ICT system or service which is utilised by more than one stakeholder in a combined or collaborative business function.
<b>Service Level Agreement</b>	A Service Level Agreement (SLA) is a negotiated agreement between two or more parties, (typically a customer and service provider). These are typically contracts and can be legally binding, formal or informal in nature.
<b>Snapshot Risk Assessment</b>	A snapshot risk assessment follows the technical risk assessment methodology as depicted in the Supplement to this Standard; however it recognises the limitations of understanding of risk components at the early stages of a project or programme. This risk assessment is therefore intended to inform the organisation of the types and magnitudes of risk that will require management in order to, for example, help make a decision about whether or not to proceed.
<b>Statement of Applicability</b>	(ISO/IEC 27001) Documented statement describing the control objectives and controls that are relevant and applicable to the organisation's ISMS. Note: control objectives and controls are based on the results and conclusions of the risk assessment and risk treatment processes, legal or regulatory requirements, contractual obligations and the organisation's business requirements for information security.

# Information Risk Management

<b>Threat</b>	A potential cause of an incident that may result in harm to a system or organisation.
<b>Threat Actor</b>	A Threat Actor is a person who actually performs an attack or, in the case of accidents, will cause the accident.
<b>Threat Actor Group</b>	A Threat Actor group is a group of people who can reasonably be considered to have the same characteristics in terms of capability, motivation and opportunity to perform an attack.
<b>Threat Level</b>	The threat level is a value attributed to the combination of the capability and motivation/priority of a Threat Actor or Threat Source to attack an asset.
<b>Threat Source</b>	A Threat Source is a person or organisation that desires to breach security and ultimately will benefit from a compromise in some way.
<b>Vulnerability</b>	A weakness of an asset or group of assets that can be exploited by one or more threats.



THIS PAGE IS INTENTIONALLY LEFT BLANK

ARCHIVE

# Information Risk Management

## Customer Feedback

CESG Information Assurance Guidance and Standards welcomes feedback and encourage readers to inform CESG of their experiences, good or bad in this document. We would especially like to know about any inconsistencies and ambiguities. Please use this page to send your comments to:

Customer Support  
CESG  
A2b  
Hubble Road  
Cheltenham GL51 0EX  
(for the attention of IA Policy Development Team)

Fax: (01242) 709193 (for UNCLASSIFIED FAXES ONLY)

Email: [enquiries@cesg.gsi.gov.uk](mailto:enquiries@cesg.gsi.gov.uk)

For additional hard copies of this document and general queries please contact CESG enquiries at the address above

PLEASE PRINT

Your Name:

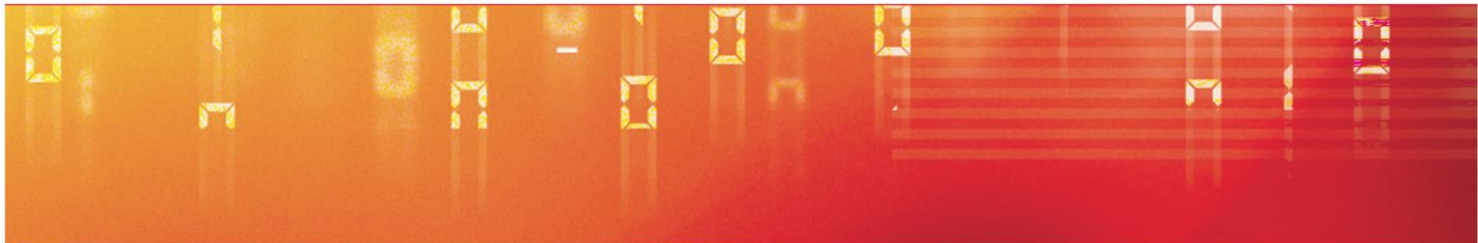
Department/Company Name and Address:

Phone number:

Email address:

Comments:

---



ARCHIVE

---

HMG IA Standards are issued jointly by Cabinet Office and CESG, the UK National Technical Authority for Information Assurance, in support of Mandatory Requirements specified in the HMG Security Policy Framework (SPF). The standards outline minimum measures that must be implemented by Departments and Agencies bound by the SPF, and compliance with SPF Mandatory Requirements cannot be claimed unless adherence to the Standards can be demonstrated. They do not provide tailored technical or legal advice on specific ICT systems or IA issues. Cabinet Office and GCHQ/CESG and its advisers accept no liability whatsoever for any expense, liability, loss, claim or proceedings arising from reliance placed upon this Standard.

ARCHIVE

CESG Enquiries  
Hubble Road  
Cheltenham  
Gloucestershire  
GL51 0EX

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

© Crown Copyright 2012.