

HMG IA Standard No. 1 Technical Risk Assessment



NATIONAL TECHNICAL AUTHORITY
FOR INFORMATION ASSURANCE

CabinetOffice



UNCLASSIFIED

**HMG IA Standard No. 1,
Technical Risk Assessment**

Issue: 3.51
October 2009

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

UNCLASSIFIED

Technical Risk Assessment

Intended Readership

This Standard is intended for Risk Managers and IA Practitioners who are responsible for identifying, assessing and treating the technical risks to Information and Communication Technology (ICT) systems and services that handle, store and process government information.

This Standard is not intended to be an introduction to the principles of information risk management. Appropriate application of the methodology it contains will require a high level of skill, judgement and experience in the field of Information Assurance.

This Standard is aligned and supports the overarching information risk management policy for HMG ICT systems provided by HMG IA Standard No.2, Risk Management and Accreditation of ICT Systems and Services (IS2) (Reference [a])

A CESG Busy Reader Guide, Risk Management and Accreditation, has been produced that provides a high level summary.

Executive Summary

This Standard is a component of the HMG Security Policy Framework (SPF) (Reference [b]) therefore it is mandatory policy for all HMG Departments and Agencies. It is also recommended for the wider Public Sector.

This Standard provides the IA practitioner with a methodology for

identifying, assessing and determining the level of risk to an ICT system and a framework for the selection of appropriate risk treatments.

This Standard includes definitions of the Business Impact Levels (BIL). The use of these levels is mandatory for HMG (SPF MR 33) and they are recommended for other organisations. The BIL's are aligned with a number of UK sectors, such as the military, the economy and the Critical National Infrastructure (CNI). An understanding of Business Impact Levels is critical to understanding the impact of a compromised information asset.

Risk assessment (evaluation) and risk treatment forms part of the overarching process of risk management.

The components of risk will change over time and those changes **must** be factored into the risk assessment to ensure the risk treatment controls are appropriate.

Risk Management is therefore an activity that **must** take place throughout the lifecycle of an ICT system or service. IS2 describes the risk management lifecycle.

A key component of a risk assessment is threat. IS1 differentiates between threat sources (those who wish a compromise to occur) and threat actors (those who actually carry out the attack). A method is provided that allows the Analyst to assess the level of threat from threat sources and threat actors including the case where a source may influence or coerce an

actor to mount an attack on their behalf. The output of the risk assessment is a set of risks.

Aims and Purpose

The aim and purpose of the Standard is to provide a risk assessment and risk treatment process that allows Analysts, Accreditors, SIROs and other interested parties to:

- Analyse a proposed or existing system to identify risks and estimate the levels of those risks;
- Select appropriate controls to manage the treatable risks.

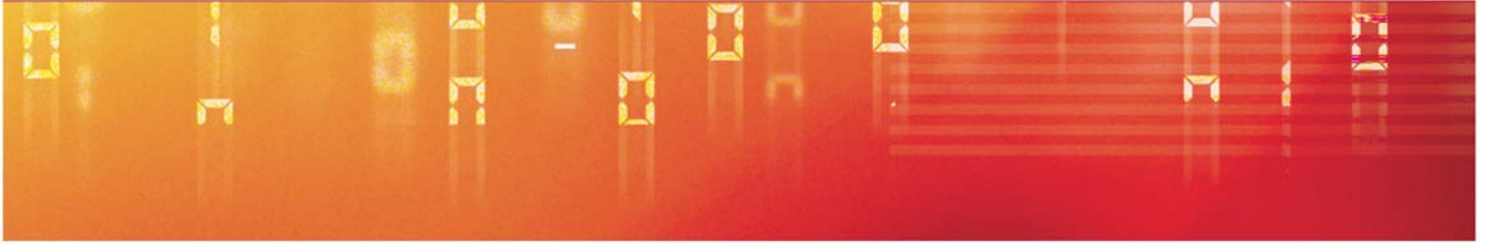
By providing a common method for estimating risk levels the Standard enables meaningful comparisons between different organisations, which is especially important if they wish to interconnect, interact or rely on shared services for protection. This supports one of the key principles of the National IA Strategy (Reference [c]).

Technical Risk Assessment

Major Changes from the Previous Issue

The following changes have been incorporated:

- The assessment process has been clarified;
- The set of minimum assumptions have been dropped to avoid confusion with the Baseline Control Set;
- Minor changes have been made to the business impact statement tables and a new table that considers impacts to the citizen has been provided;
- Guidance has been produced about using IS1 throughout the risk management and accreditation lifecycle. This new guidance is consistent with IS2;
- The treatment of threat has been modified, to make it simpler, clearer and easier to apply. Threat actor clearance and deterrence has moved into the threat level assessment, with some consequential changes such as the disappearance of likelihood as an explicit parameter. The process for assessing coercion of threat actors by threat sources has been clarified. This has resulted in a number of changes to Form 4;
- A new guided worked example has been developed to reflect these changes.



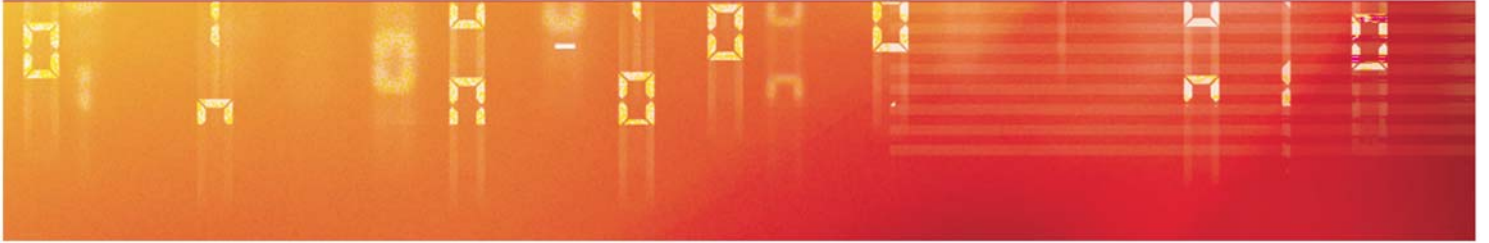
THIS PAGE IS INTENTIONALLY LEFT BLANK

Technical Risk Assessment

Contents:

Chapter 1 - Introduction	7	Outline of the Step-By-Step Method	21
Structure of this Standard and How to Use it	7	Appendix A: Business Impact Level Tables	45
Status and Applicability	8	Introduction	45
Using this Standard	8	Using the tables	45
Chapter 2 - Risk Management Lifecycle	9	Appendix B: Modelling Technique	55
Introduction.....	9	Introduction	55
Risk Appetite and Risk Tolerance....	9	Risk Analysis and Analysis Scope	55
Project Lifecycle	10	Model Concepts.....	56
Chapter 3 - Concepts used in the method	15	Modelling Reference Guide	57
Risk Assessment Scope	15	Appendix C: Threat Actor Type and Compromise Methods	63
Assets, Focus of Interest and Modelling	16	Definitions of Threat Actor Types..	63
Business Impact Level.....	16	Description of Threat Actor Types	65
Threat Sources and Threat Actors.	17	Compromise Methods Available to Threat Actors	67
Threat Levels.....	18	Appendix D: Worked Example	73
Compromise Methods	18	Introduction	73
Risk	19	Scenario	73
Risk Level.....	19	Appendix E: Blank Forms	97
Chapter 4 - The Risk Assessment Method	21	References	103
		Glossary	104
		Customer Feedback	109

UNCLASSIFIED



THIS PAGE IS INTENTIONALLY LEFT BLANK

UNCLASSIFIED

Technical Risk Assessment

Chapter 1 - Introduction

Key Principles

- It is a mandatory requirement that HMG Departments and Agencies bound by the SPF carry out risk assessments for their ICT systems using this Standard.
- IS1 is intended to be used by an IA practitioner. A lot of analysis and professional judgement is required throughout application of this Standard.

Structure of this Standard and How to Use it

1. IS1 provides a method to identify and assess the technical risks that an ICT system is exposed to. The key output is a list of prioritised risks that can be used as a basis for risk treatment requirements and options for managing the risks, such as the set of controls provided in ISO 27001, *Information Security Management Systems* (reference [d]). ISO 27001 provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management Systems (ISMS). There may be significant alignment for organisations using both IS1 and ISO 27001.
2. Risk assessment is an ongoing process that **must** be carried out within the broader context of the risk management and accreditation process, as described in IS2.
3. Understanding that the risk components¹ will change throughout the lifecycle of an ICT system (such as during development, in service and end of life) is a key aspect of information risk management. Technical risk **must** be reviewed at least annually or when there are significant changes to the risk components as required by the SPF, MR 32. For ICT systems handling personal or sensitive information, the risk assessment **must** be reviewed quarterly. Further detail on alignment of IS1 to the risk management and accreditation lifecycle is contained in Chapter 2, *Risk Management Lifecycle*.
4. For every HMG ICT system IS2 requires a Privacy Impact Assessment (PIA) to be conducted. The first element of that assessment is a screening process to determine if personal or sensitive information is included within the scope of the ICT system. IS1 supports the PIA process, which is described in further detail in IS2.
5. IS1 provides a method to assess technical information risk. It does not provide guidance on the assessment of non-technical risk, such as fire or flood. These risks should be assessed using an appropriate method and included within the overall Risk Management and Accreditation Documentation Set (RMADS).

¹ Risk Components are, Assets (Impact), Threat, Vulnerability, Likelihood.

6. Throughout the IS1 method, significant decisions have to be made on risk components such as threat. It is essential that the Accreditor is involved throughout the whole risk assessment process, influencing and agreeing assumptions and decisions. IS1 supports the risk management and accreditation process described in IS2. This Standard requires formal Accreditor sign off of deliverables at various stages, including those delivered by application of IS1. For further information refer to Chapter 2, *Risk Management Lifecycle*.
7. Within this Standard the **must** imperative is used to describe a mandatory requirement. The **should** imperative is used where the application of the measure is recommended but not mandatory.

Status and Applicability

8. The SPF MR 32 requires that all Government Departments and Agencies apply this Standard to assess and treat the technical risks to all HMG ICT systems.
9. This Standard is designed to be applicable to a broad range of customers across the public and private sectors. Where this Standard is used by organisations not bound by the SPF (such as Local Authorities), the mandatory requirements should be taken as strong recommendations. This Standard is strongly recommended for e-Government related risk assessments, and is endorsed by the e-Government Security Framework (reference [e]).
10. This Standard has been produced to be consistent with and support the application of the ISO 27000 series, as good practice for the risk management of information systems.

Using this Standard

11. IS1 is not prescriptive about how a risk should be treated. As the risk appetite of the organisation and the business context will differ for each. Therefore significant judgements will have to be made and, ideally, the analyst should have a solid understanding of the principles of risk management and practical experience of applying them. Technical skills are not critical to using the Standard.
12. The assessment and treatment of technical risk is complex and to achieve accurate outcomes requires a skilled practitioner. Whilst not essential, it is recommended that before using this Standard, practitioners attend a formal training course.
13. Government Departments who require advice on the application of this Standard should approach CESG (via their Customer Account Manager) or consider engaging a member of the CESG Listed Advisors Scheme (CLAS) to support them.

Technical Risk Assessment

Chapter 2 - Risk Management Lifecycle

Key Principles

- Risk Management is an activity that must take place throughout the lifecycle of an ICT system, from inception, design, in-service delivery and finally decommissioning.
- IS1 can and should be used in conjunction with the risk management and accreditation process described in IS2.
- Early project risk assessments may have to make a number of assumptions or generalisations. As more information becomes known about the project and associated components of risk, the risk assessment **must** be refined and updated.

Introduction

14. The risk management and accreditation process is established and fully described in IS2. Risk management is an iterative process that must be carried out throughout the lifecycle of an ICT system, from early planning, system development, in-service and eventually decommissioning and disposal. Effective risk management provides an organisation with confidence that risks to the ICT system and its information are effectively managed whilst allowing business opportunities to be realised.
15. Risk management requires a thorough understanding of business requirements, potential threats and vulnerabilities that may be exploited and an evaluation of the likelihood and impact of a risk being realised. IS1 provides a method to evaluate these factors and risk. This chapter describes how IS1 can, and should, be used throughout the risk management lifecycle. Activities described are aligned to the IS2 stage process.

Risk Appetite and Risk Tolerance

16. A Risk appetite statement allows an organisation to communicate the overall level of risk that they are prepared to tolerate in order to achieve their business aims. This statement sets the context for decisions about the acceptable level of risk for particular business activities or projects, known as risk tolerance. Risk tolerance is not a fixed level. An organisation may set an initial risk tolerance for an ICT system, taking into account the organisation's risk appetite, then reconsider that tolerance in the light of new understanding or circumstances.

17. When considering the application of controls to manage information risk, the Analyst should take account of the risk appetite and risk tolerance statements in deciding how robust controls need to be and determining an appropriate assurance plan. Further guidance on risk appetite and risk tolerance is provided in IS2.

Project Lifecycle

18. A typical project will begin with a business requirement to be achieved. There may be some organisational statements (such as the risk appetite) and policies; the Analyst and Accreditor may know something about applicable threat sources. At this stage of the project very little is typically known about the design or architecture of the eventual solution and thus little is known about specific vulnerabilities. A risk assessment will provide quite generic outputs and significant assumptions may need to be made.

19. As more is known about the project, and business requirements are refined, the risk assessment can be refined. Generic categories of vulnerability may be able to be deduced, leading to a set of risks and associated security requirements to manage those risks. Typically these security requirements could be used to inform and influence an Invitation To Tender (ITT) and then be used as a basis for tender evaluation.

20. As a system is designed and implemented, knowledge about specific functionality and architecture becomes known. This allows a more refined assessment of vulnerability, controls and assurance in place. Vulnerabilities are never static and thus the risk assessment **must** regularly and continually take into account these changes as well as changes in the threat environment and business use. Finally, when an ICT system is decommissioned the risk assessment **must** be updated to evaluate and manage risks associated with decommissioning, such as disposal of equipment.

21. The lifecycle described follows the IS2 staged risk management process. At a number of stages the risk assessment **must** be refined and updated to reflect improvements in or new knowledge of the components of risk. The following sections describe IS1 activities and outputs required for each IS2 stage.

Stage 0 – Early Planning and Feasibility

22. The purpose of Stage 0 is to assess and provide early identification of the high-level IA risks associated with the business requirement. At this stage an IS1 'snapshot' risk assessment should take place.

Technical Risk Assessment

Snapshot Risk Assessment

23. A snapshot risk assessment follows the IS1 method; however, it recognises the limitations of the level of understanding and detail of risk components. This risk assessment is therefore intended to inform the organisation of the types and magnitudes of risk that will require management in order to help make a decision about whether to proceed. A broad understanding of the business requirement is required for this stage. The normal IS1 method should be followed with the following guidance:

- Assets at risk of compromise should be understood at a broad and high-level. The maximum business impacts of compromise of confidentiality integrity and availability should be assessed.
- Categories of threat sources should be assessed and understood at this stage. Corporate threat information may exist. At this stage of the project there may be little refined understanding of threat actors, however broad categories should be understood and assessed. For example, it will be known whether there will be system users or not.
- A snapshot of risk level can be evaluated. This will provide an indication of the level and types of risk that will need to be managed. In addition, at this stage the Analyst and Accreditor should be able to assess which Segmentation Model levels will be applicable.

24. Where the proposed system includes interconnections to or dependencies on other systems, then a similar snapshot assessment should be carried out for that system.

Stage 1 – Accreditation Strategy

25. The aim of Stage 1 is to define and develop an accreditation strategy. This strategy should include definition of how the risk assessment and risk treatment method (as described in this Standard) will influence and be incorporated into the RMADS.

26. As more becomes known about the components of risk, the snapshot assessment can be refined and developed. In particular, more will be known about the application of the baseline controls and which risks will require controls at higher levels of the Segmentation Model. At this stage, controls will be defined in terms of 'control objectives' set out in a security case. That is, they will describe functionally the purpose of the control but may not define how that control will be achieved. For example, a control objective to stop malware executing could be achieved by stopping the malware at a boundary or by using an executable 'white list'. The security case will begin to define how assurance might be achieved, recognising that there is still a lot of uncertainty of the final solution.

27. The draft security case supports the risk treatment plan that is required to be produced for the RMADS at this stage.

Stage 2 – IA Requirements

28. Stage 2 aims to develop a set of IA requirements that are of sufficient quality to be included in an ITT process. The requirements should give adequate guidance to potential suppliers and be able to provide a basis for discrimination between different bids.

29. This stage is at the core of IS1. The risk assessment method should be carried out in full, with a more developed analysis of the business requirements, threat sources and threat actors (including threat sources influencing threat actors).

30. All HMG systems are expected to apply a full set of baseline controls, with any exceptions justified and agreed with the Accreditor. For risks that require treatment at a higher level of the Segmentation Model, control objectives should be developed. These objectives **must** be of sufficient quality that they can be used as a basis for supplier discrimination, contract negotiation and that once a solution is developed against those requirements, it will provide the overall required levels of risk management. Assurance requirements **must** also be defined at this stage, as the assurance activities required will need to be built into the ITT and therefore the suppliers cost model. Both the control objectives and assurance requirements **must** be built into the security case and RMADS

31. It is critical that this stage is carefully and completely followed. Once a set of security requirements have been agreed contractually, it may be extremely difficult and expensive to later request changes or debate ambiguity.

Stage 3 – Options Assessment and Selection

32. The purpose of Stage 3 is to assess the supplier's ability to deliver a solution that meets the IA and business requirements. The bids provided should be assessed against the security requirements defined in Stage 2. Security requirements contained within the ITT will typically take the form of control objectives. The suppliers will propose a solution that aims to meet those objectives with associated assurance.

Stage 4 – Accreditation in Development and Acceptance

33. The aim of Stage 4 is to confirm that the delivered solution is fit for purpose, meets the security requirements and can be accredited. It is at this stage where considerably more information about the system risks becomes known. IS1 uses the concept of compromise methods. These can be thought of as a generalisation of possible vulnerabilities that a threat actor could exploit. As more information is

Technical Risk Assessment

known these compromise methods can be developed by the Analyst to deliver a greater level of granularity to the risk assessment.

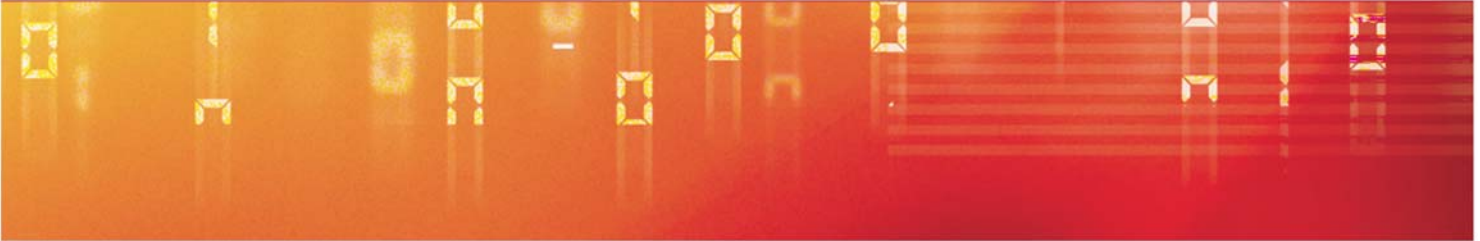
34. As more is known about the architecture and design of the solution, more will be known about how threat actors might be able to exercise particular compromise methods, what controls are in place and what vulnerabilities remain. The strength of a set of controls that manage risks from a given set of threats **must** take account of the risk tolerance statement. This statement will provide a qualitative measure of how robust the controls need to be and what residual vulnerability may be acceptable. For example if the risk was related to malware exercising a known vulnerability²:

- If the risk tolerance level is stated as Very Low this may mean that all system components require immediate patching all of the time.
- If the risk tolerance level is stated as Medium this may mean that patches can be grouped and applied as a batch.

35. The Analyst should ensure that the solution effectively delivers all of the baseline controls and that appropriate assurance is in place or planned. Similarly the Analyst should ensure that all control objectives at higher Segmentation Model levels are sufficiently implemented and assured. The Analyst should:

- In light of the design or solution, for each risk (or set of similar risks) deduce how the compromise method relates to different ways of compromising the system. For example, a system has email and web browsing to the Internet. One risk will be that an Internet connected threat agent performs a network attack. In this case network attack may compromise:
 - Abuse of email protocol (such as SMTP);
 - Abuse of web protocols (such as HTTP);
 - Abuse of any other protocol, which is disallowed in the policy.
- The Analyst can then deduce whether the solution effectively manages these decomposed risks and any gaps. These solution gaps **must** be recorded in the updated security case and included in the RMADS. Similarly, any assurance gaps **must** be recorded in the updated security case and included in the RMADS.

² Note that these statements are just examples of how the risk tolerance level may influence controls; they are not necessarily appropriate responses.



Stage 5 – Risk Management In-Service & Accreditation Maintenance

36. Stage 5 aims to ensure that the ICT system is and remains compliant with the corporate security policy and the agreed IA requirements (including assurance) as documented in the RMADS.
37. As a system is used, the specific business uses may vary, threats may change and new vulnerabilities will be discovered. The risk assessment **must** reflect the current prevailing risk components. It is therefore essential to regularly review and update the risk assessment.
38. The SPF (MR 32) requires that all ICT systems are subject to an annual risk assessment or an updated assessment when there is significant change to any of the risk components. The latest threat and vulnerability assessments should be reviewed (at least annually) and the risk assessment correspondingly updated. In particular when system profile changes (such as a new interconnection) then the risk assessment **must** be revisited and updated.
39. Assurance activities **must** continue throughout the lifecycle of the ICT system. Accreditors and IA Practitioners should consider the CESG Assurance Framework to ensure that assurance has been considered in the round.

Stage 6 – Secure Decommissioning and Disposal

40. The final stage (6) aims to ensure that an ICT system is decommissioned and disposed of in a secure way. There are likely to be specific risks associated with this final stage that should be assessed using IS1. The disposal or reuse of equipment or media that has not been securely erased may compromise the confidentiality of any data on media left on the system.

Technical Risk Assessment

Chapter 3 - Concepts used in the method

Key Principles

- The scope of a risk assessment can be defined to include services delivered by the project, other components such as external connections that require analysis as well as components that are provided and accredited by others and can be trusted.
- IS1 differentiates between a threat source and a threat actor. A threat source is somebody who wishes a compromise to occur, or would benefit from a compromise occurring. A threat actor is somebody who would actually mount the attack. A threat source can influence or coerce a threat actor to mount an attack on their behalf.
- The IS1 risk assessment method takes the concept of a threat actor, using a compromise method to compromise the confidentiality, integrity or availability of information or an ICT system.

Risk Assessment Scope

41. ICT systems are typically not developed in isolation and either rely upon, or deliver controls for, other systems outside of the scope of the project. A risk assessment may therefore involve consideration of facilities and services that have been, or need to be, accredited by another organisation. To accommodate these situations this Standard introduces the concepts of Accreditation Scope, Reliance Scope and Analysis Scope.
42. The **Accreditation Scope** includes all of the capability and services for which the project is responsible for delivering. This will typically be the same as the scope of the project.
43. 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. For example a project may decide to rely upon services provided by the Government Secure Intranet (GSI), without having to accredit those services themselves. The use of shared services should come within the reliance scope.
44. The **Analysis Scope** includes everything that is part of the risk assessment. This includes everything that is part of the project and reliance scope as well as considering business information exchange requirements and system connections.

45. Where a project team is responsible for all the defences to protect its assets, the project and reliance scopes will be the same. However, often projects provide services to other projects and/or rely on other projects to provide security services. This Standard requires that you explicitly identify these dependencies.

Assets, Focus of Interest and Modelling

46. An asset is broadly defined in IS2 as 'anything, which has value to an organisation, its business operations and its continuity'. If the confidentiality, integrity or availability of an asset is compromised then there will be an impact felt by the business or other stakeholders.

47. 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.

48. The IS1 method contains a modelling technique, that allows the Analyst to model assets under consideration to help them gain a greater understanding of the system. Use of the modelling technique is recommended but not mandatory. If the user prefers a different method of modelling the system they are free to use that method, so long as the Accreditor is content with the approach.

49. The core of the modelling technique is based around model objects. These include assets but the term also includes things that would not normally be considered explicitly as assets, such as support objects or connection objects. The detail of the model objects and modelling technique is contained within Appendix B.

Business Impact Level

50. The successful exploitation of a compromise method by a threat actor will result in compromise of Confidentiality, Integrity or Availability (C, I or A) of an asset. This compromise will have a business impact. The SPF and this Standard ranks business impact on a seven-point (0 to 6) numerical scale. Appendix A lists a series of criteria, grouped according to UK sectors, by which to judge the appropriate Business Impact Level (BIL).

51. Business impact is by definition the impact that a compromise has on the operations or efficiency of the organisation or on customers or citizens. It is for the organisation to make a business led decision on the appropriate BIL to assign to an asset.

52. The business impact level tables presented in Appendix A, describe impacts from the common perspective of UK Society. For example the impact of a given financial loss to a small company, large company or HMG is taken from the

Technical Risk Assessment

perspective of damage to the UK economy, rather than the perspective of the individual organisation.

53. Where the business impact of compromise of a set of assets is greater than the impact of an individual compromise, aggregation applies. Care should be taken when considering aggregation. Where a set of information has a higher BIL because of aggregation it does not necessarily follow that the applicable threats have increased. This means that it is not always appropriate to increase the Protective Marking of information (for confidentiality) when the BIL rises due to aggregation. For example a database of many IL3 (for confidentiality) records may aggregate to IL5. It does not follow that this database should be marked SECRET, as this would lead to disproportionate and inappropriate controls being required. CESG GPG 9, *Taking Account of the Aggregation of information* (reference [f]) provides further detail.

Threat Sources and Threat Actors

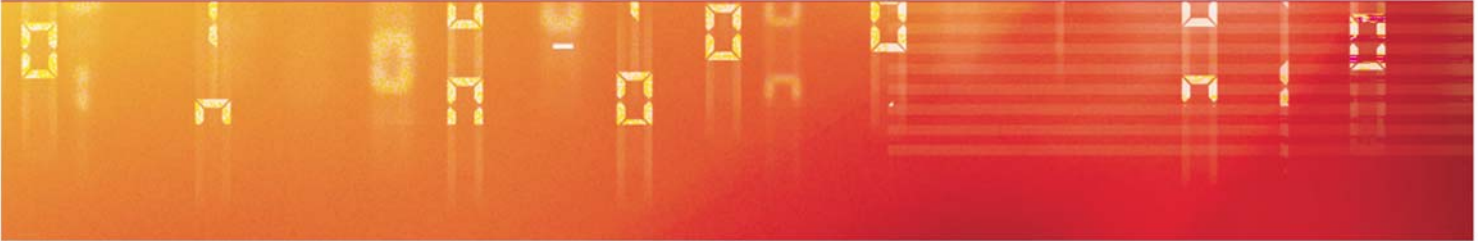
54. This Standard distinguishes between threat sources and threat actors, although one person or organisation may be both a source and an actor.

55. A threat source is a person or organisation that desires to breach security and ultimately will benefit from the breach in some way. A threat actor is a person who actually performs the attack or, in the case of accidents, will cause the accident. For example a criminal may wish to breach the confidentiality of some HMG data. The criminal wishes the breach of security to happen and thus is the threat source. If the criminal persuades a system user to release the desired information to them then the user is actually carrying out the attack. They are the threat actor.

56. Every system will have 'authorised users', who are threat actors for some compromise methods. Occasionally, it may be desirable to split authorised users into groups if their capability, motivation or security clearance varies considerably. For example it may be useful to consider DV and BS cleared authorised users of the same system as two different groups of threat actors.

57. 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. For example a Department's set of cleaners may be grouped together as one threat actor group, rather than conducting a risk assessment for each individual cleaner.

58. The threat actor type is a key concept in this Standard because it defines the types of attack that a threat actor can mount. Each threat actor belongs to one or more threat actor types according to the degree and type of access to an asset. These threat actor types are:



Bystander (BY)	Physical Intruder (PI)
Handler (HAN)	Privileged User (PU)
Indirectly Connected (IC)	Service Consumer (SC)
Information Exchange Partner (IEP)	Service Provider (SP)
Normal User (NU)	Shared Service Subscriber (SSS)
Person Within Range (PWR)	Supplier (SUP)

These threat actor types are described more fully in Appendix C.

59. The list of threat actor types is intended to be exhaustive in that any threat actor will fit into one or more threat actor types. If a situation arises where a threat actor group cannot fit into any of the types then discretion may be used to create and use a new type.

Threat Levels

60. The threat level is a value attributed to the combination of the capability and motivation of a threat actor or threat source to attack an asset. It takes into account any clearances that may apply to the threat actors and whether they are considered Deterrable.

Compromise Methods

61. A compromise method is the broad type of attack by which a threat actor may attempt to compromise the C, I or A of an asset. Once the threat actors' types have been determined it is straightforward to identify from Appendix C, the compromise methods they might use, and then consider which of those are actually plausible.

62. The compromise methods are stated at a very high level (such as Deliberately Disrupts) and could include several detailed types of attack. As such the compromise methods can be thought of as a generalisation of vulnerability. When the Analyst has more detailed information about the system and understands elements of the architecture and deployed controls they can deconstruct the compromise methods to provide more detail in their specific risk assessment. For example the compromise method *Misuses Business or Network Connections* could be decomposed into specific vulnerabilities that arise because of the business requirements and the designed architecture.

Technical Risk Assessment

Risk

63. In general terms an information risk can be thought of as the likelihood that a threat will exploit a vulnerability leading to a business impact. IS1 aims to define all risks and estimate a risk level for each.

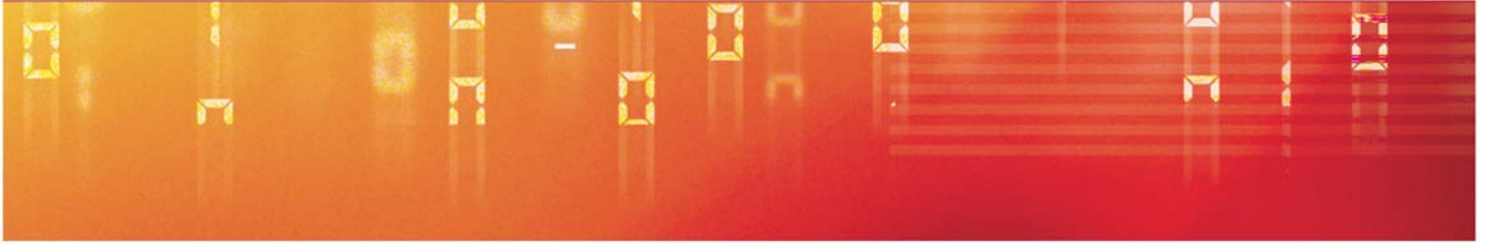
64. Within IS1 a risk can be thought of as consisting of a number of components:

- Threat actor and threat actor type;
- Threat source;
- Compromise method;
- Property (C, I or A) of an asset or FoI and business impact level associated with the compromise of that property.

Risk Level

65. The risk level for an IS1 risk is a combination of threat level and business impact level. The elements of likelihood and vulnerability cannot be assessed in a generic sense and in the early stages of a risk assessment may not be known. A risk level is therefore an indicative assessment of risk.

66. For the purposes of this Standard, risk level is defined on a six-point scale: Very Low; Low; Medium; Medium-High; High; Very High. The step-by-step process in Chapter 4 indicates how to estimate risk levels.



THIS PAGE IS INTENTIONALLY LEFT BLANK

Technical Risk Assessment

Chapter 4 - The Risk Assessment Method

Key Principles

- The IS1 risk assessment method is a 6 step process. The process aims to develop an understanding of the system under consideration, the applicable threats (and associated compromise methods) and determine risks and risk levels.
- The output of IS1 is a prioritised list of risks.

Outline of the Step-By-Step Method

67. The IS1 risk assessment method follows six defined steps. These steps allow the Analyst to understand the system under consideration, define applicable threats and determine risks to the system with associated risk levels.
68. The risk assessment method supports the overall risk management and accreditation process as described in IS2. For further detail about using IS1 in the risk management and accreditation lifecycle see Chapter 2, *Risk Management Lifecycle*.
69. The six steps are:
- Step 1: Catalogue the system;
 - Step 2: Define the threat sources;
 - Step 3: Define the focus of interest;
 - Step 4: Define the threat actors and estimate threat level;
 - Step 5: Identify the risks and estimate risk levels;
 - Step 6: Prioritise risks in terms of risk level.
70. The risk assessment process described is intended to stimulate thought about risk. It is not intended to simply generate paperwork. The forms provided are for recording and presenting the results of analysis for review. Production of a paper form is not the primary objective.
71. Risk assessment is a complex activity that requires skill and experience. The process involves making decisions based on professional judgement and the Analyst should agree and record rationale and assumptions with the Accreditor.

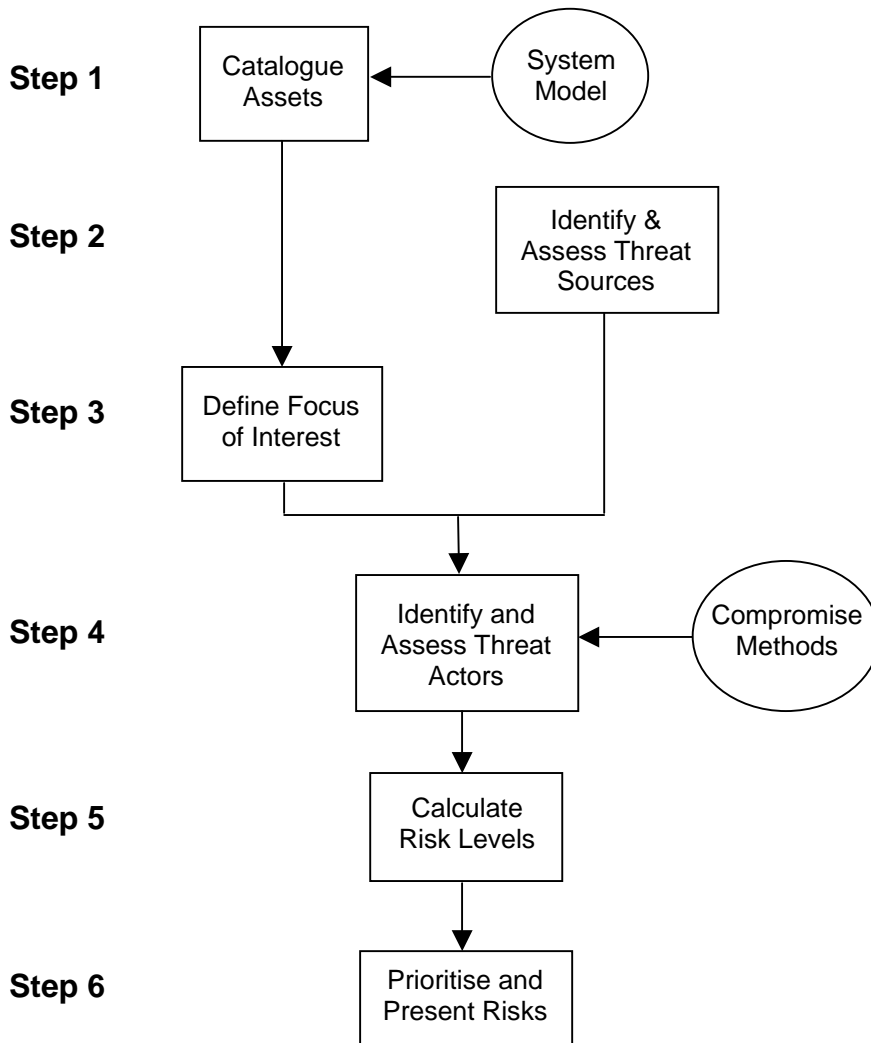


Figure 1: Risk Assessment Method

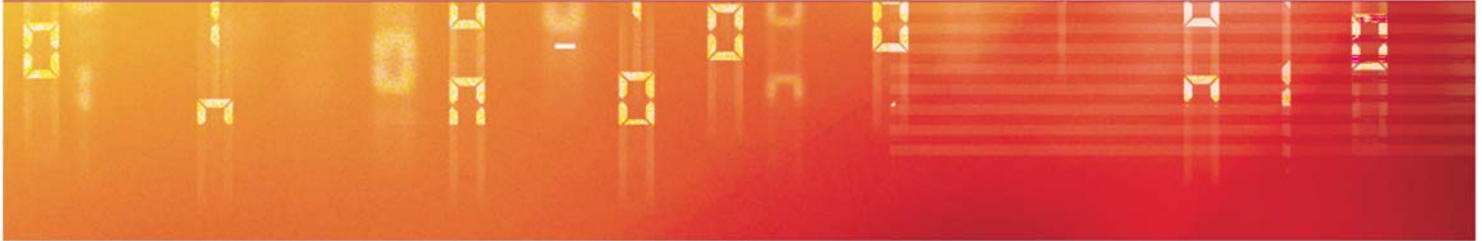
Technical Risk Assessment

Use of Forms

72. The method uses a number of forms to record the information at each step. Each step is associated with a form with the same number, thus Step 3 uses Form 3. Each form is shown with an example entry provided to allow demonstration of how the form may be used. This entry is provided in *italics*. Forms 1-5 are mainly for use by the Analysts and other ICT security professionals, Forms 4 and 5 are key forms as they contain detailed information about threats and risk. Form 6 is intended to present the summarised results in a way that is easily assimilated by non-specialists.
73. The forms may be altered (with Accreditor agreement) by adding elements to suit local requirements. In particular readers may wish to develop their own softcopy versions of the forms for ease of completion and reproduction.
74. The Accreditor is highly likely to require some explanation of the reasoning behind decisions. This can be recorded in the comments boxes on the forms or, if preferred, in a separate free-format 'rationale log'.

Step 1: Analyse and catalogue the system

75. The objective of Step 1 is to describe the system and agree with all interested parties what the system consists of, what the high-level business information exchange requirements are and the scope of the project's responsibility. It may be useful for the Analyst to identify threat actor groups in this step but this is optional and may be deferred until later.
76. The system should be described and a list of assets produced. The description of the system typically will include:
- Business assets and information exchange requirements;
 - Systems that directly or indirectly support the implementation of the above;
 - Places where people work and/or that contain assets.
77. Production of a model is recommended, but it is subject to agreement between the Analyst and the Accreditor, taking into account factors such as:
- The complexity and connectivity of the system;
 - The ability to complete further risk assessment steps without a diagram;
 - The possible usefulness of a diagram when identifying risk treatment requirements and options for managing the risks, such as a set of controls;
 - The accreditation stage of the project or programme.



78. Additionally a diagram may be a very succinct way of assimilating and communicating information about the system under consideration. It is frequently a valuable exercise to develop a diagram for the benefits of understanding the system in addition to the finished output.

79. The suggested modelling technique is described in Appendix B, however, any technique that achieves the same objectives may be used with the agreement of the Accreditor.

80. Irrespective of whether a diagram is produced or not, a Form 1 **must** be produced and completed.

81. A sample Form 1 is shown below. To complete Form 1:

- Create a row in Form 1 for every named asset;
- Generate an Identifier and enter it in column 1.1;
- Generate descriptive text to explain what each asset comprises and enter it in column 1.2. This should include factors such as whether aggregation applies;
- For each asset, assess the highest business impact level for a compromise for each of the properties C, I and A according to the business impact level tables in Appendix A and enter the value in column 1.3. A description of the business impact can be entered in column 1.2.

82. The business impact levels represent business impacts and therefore should be determined by the organisation. In the first instance the Accreditor should provide guidance, referring to the relevant Information Asset Owner (IAO) for further guidance as required.

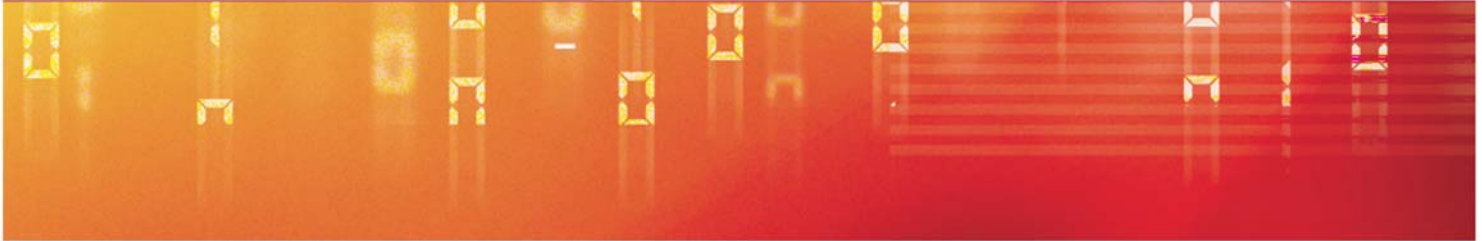
Technical Risk Assessment

Form 1 – Asset List				
1.1 Asset Identifier	1.2 Description/Notes	1.3 Impact Levels		
		C	I	A
Each asset is provided with an identifier. This can simply be a name such as: <i>Secret Database</i>	Describe the asset and explain the business impact: <i>This includes all information provided in the Secret Database</i>	5	3	3

Form 1 - Asset List

Step 2: Define and Assess Threat Sources

83. Identifying threat sources is a matter of exercising professional judgment to decide who might deliberately attack the system and should be agreed with the Accreditor. With regard to threat levels for some threat sources (particularly the major threat sources relating to national security) the most authoritative source of technical threat information may be a specific threat assessment from CESG, CPNI or for the MOD the Defence Intelligence Staff (DIS). Their advice should help to identify key threat sources and aid the production of an in-house threat assessment.



84. A suggested overall approach is to:

- Consult the Departmental Security Officer or IT Security Officer, who will have access to relevant threat information, including advice from CPNI.
- Perform an initial in-house threat assessment as described below and submit it to the Accreditor.
- Then, if the Accreditor requires, obtain a specific threat assessment and revise the threat levels accordingly.

85. If the threat levels from an in-house assessment are markedly different from one from the Security Authorities then it is a matter for professional judgement and agreement with the Accreditor which to use, but in general those from the Security Authorities should be regarded as the more authoritative.

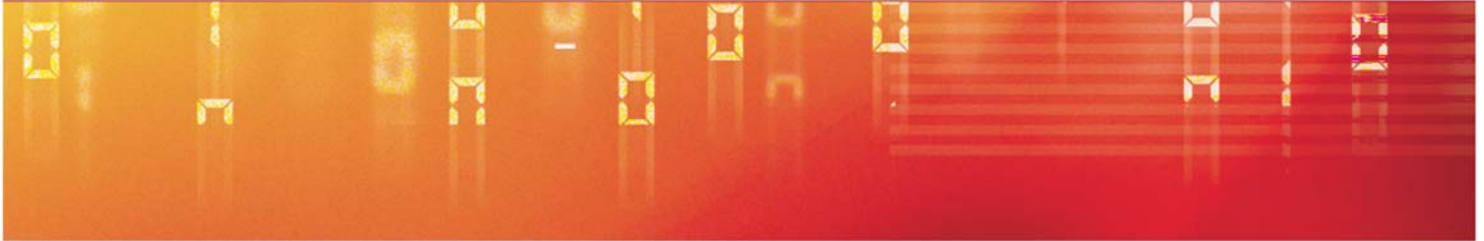
86. Threat sources should be identified whether they can act as threat actors carrying out their own attacks or would have to coerce or subvert another threat actor to act on their behalf.

87. A sample Form 2 is shown below, but there are a number of sub-steps involved in its production. The method is:

- Identify each threat source that is applicable to the analysis. Create a row in Form 2 for each, providing a unique identifier and a description. Threat sources may include, but are not limited to:
 - Disaffected or dishonest employees;
 - Foreign Intelligence Services;
 - Amateur or professional hackers;
 - Virus and other malware writers;
 - Terrorists;
 - Investigative journalists;
 - Commercial competitors (i.e. industrial espionage);
 - Political pressure groups/activists;
 - Organised criminal groups.
- If an external threat assessment is used simply record the threat level value from that assessment directly in Form 2 column 2.5. Columns 2.3 and 2.4 for capability and priority are not required. Identify the external source of the threat assessment in column 2.6.
- Where the Analyst is using the IS1 in-house threat assessment method, the threat sources capability and priority **must** be assessed.

Technical Risk Assessment

- Table 1, *Threat Source Capability* should be used to assess capability and Table 2, *Threat Source Priority* should be used to assess priority. Insert these values into column 2.3 and 2.4 respectively. Assessment of these factors requires considerable judgement and should be agreed with the Accreditor.
- Threat level can then be simply determined by using the evaluated capability and priority in Table 3, *Threat Level*. This threat level should be recorded in column 2.5 and 'in-house' should be recorded in column 2.6 as the source of the threat assessment.
- An assessment should be made as to whether it is believed that the threat source will attempt to influence threat actors (such as Normal Users) through coercion or bribery. A simple Yes or No should be recorded in column 2.7.
- A threat source can also be a threat actor. The Analyst should make a judgement as to whether they believe this to be the case and enter a Yes or No in column 2.8.



Form 2 – Threat Sources								
			2.3	2.4	2.5	2.6	2.7	2.8
2.1 Source Name	2.2 Description (and Rationale)	Property	Capability (Table 1)	Priority (Table 2)	Threat Level (Table 3)	Source of Threat Assessment	Influencer Y/N	Threat Actor Y/N
Provide a sensible name for the source such as: <i>Country X Foreign Intelligence Service</i>	Describe the threat source and provide rationale why they are relevant: <i>Country X is known to be interested in finding out about the Secret Database.</i>	C	4	4	Severe	<i>In-house</i>	Y	Y
		I						
		A						
		C						
		I						
		A						
		C						
		I						
		A						
Notes/Rationale: <i>Country X are known to be interested in compromising the Confidentiality of the Secret Database and believe that they would try to attack the system frequently and persistently. We know that they are capable and have significant resources.</i>								

Form 2 - Threat Sources

Technical Risk Assessment

Capability	Description
5 – FORMIDABLE	<p>Where the threat source is extremely capable and well-resourced, i.e. can:</p> <ul style="list-style-type: none"> • Devote several man-years to penetrating a system • Develop bespoke attacks • Coordinate information about targeted systems from several sources • Cultivate insiders for long-term attacks • Deploy large amounts of equipment • Coordinate attacks using several threat actors <p>Typically a well-resourced Foreign Intelligence Service</p>
4 – SIGNIFICANT	<p>Where the threat source is capable and has significant resources, i.e. can:</p> <ul style="list-style-type: none"> • Devote several man-weeks to penetrating a system • Use all publicly available attack tools • Influence insiders for specific attacks • Deploy modest amounts of equipment <p>Typically a moderately well-resourced Foreign Intelligence Service or well organised terrorist or criminal group</p>
3 – LIMITED	<p>Where the threat source has modest capabilities and resources, i.e. can:</p> <ul style="list-style-type: none"> • Devote a few man-days to penetrating a system • Use well-known publicly available attack tools • Deploy small amounts of equipment <p>Typically a small organised terrorist or criminal group, or a competent individual hacker</p>
2 – LITTLE	<p>Where the threat source has very modest capabilities and resources, i.e. can:</p> <ul style="list-style-type: none"> • Devote a few man-days to penetrating a system • Deploy a very small amount of equipment <p>Typically an average internet user.</p>
1 – VERY LITTLE	<p>Where the threat source has almost no capabilities or resources, i.e. can:</p> <ul style="list-style-type: none"> • Use simple "plug-and-play" plug-in devices and removable media • Devote a few man-hours to penetrating a system <p>Typically a computer or internet novice.</p>

Table 1 - Threat Source Capability

Priority	Description
5 – VERY HIGH (FOCUSED)	<p>The threat source has a primary aim to attack the system.</p> <p>Typically the threat source will undertake detailed research on the target system and generate bespoke attacks, including attacks, which are engineered to appeal to, or take advantage of, specific user behaviour (such as opening what appears to be a work relevant email attachment). The threat source is very likely to attempt to use direct persuasion, bribery and coercion of the user community, to inform and facilitate their attacks.</p> <p>The threat source is likely to be prepared to wait to exploit an attack opportunity that only rarely occurs and then surge resources in the form of several coordinated threat actors in order to mount the attack.</p> <p>Typically known hostile, major Foreign Intelligence Services.</p>
4 – HIGH (COMMITTED)	<p>The threat source will attempt to attack the system on a persistent and frequent basis, and is willing to devote several people to the attack(s), including development of attacks that aim to specifically take advantage of user behaviour. The threat source may attempt to use direct persuasion, bribery and coercion of the user community, to inform and facilitate their attacks.</p> <p>Typically most Foreign Intelligence Services and major criminal organisations.</p>
3 – MEDIUM (INTERESTED)	<p>The threat source will attempt to attack the system on a frequent basis, and is willing to devote a few people to the attack(s). The threat source is unlikely to attempt to use direct persuasion, bribery and coercion of the user community.</p> <p>Typically minor terrorist organisations, organised crime where the system is of particular interest to the criminal organisation.</p>
2 – LOW (CURIOUS)	<p>The threat source will attempt to attack the system on an occasional or fortuitous basis, and is willing to devote very few people to the attack(s). The threat source is very unlikely to attempt to use direct persuasion, and coercion of the user community.</p> <p>Typically single-issue political pressure groups, amateur hackers, investigative journalists and academics, commercial rivals.</p>
1 – VERY LOW (INDIFFERENT)	<p>The threat source is very unlikely to attempt any attack on the system.</p> <p>Typically business partner organisations, organisations with a good reputation that would be damaged if it became known they were attacking the system.</p>

Table 2 - Threat Source Priority

Technical Risk Assessment

		Capability Level				
		1 VERY LITTLE	2 LITTLE	3 LIMITED	4 SIGNIFICANT	5 FORMIDABLE
Priority	1 INDIFFERENT	Negligible	Negligible	Low	Low	Moderate
	2 CURIOUS	Negligible	Negligible	Low	Moderate	Substantial
	3 INTERESTED	Negligible	Low	Moderate	Substantial	Severe
	4 COMMITTED	Low	Low	Moderate	Severe	Severe
	5 FOCUSED	Low	Moderate	Substantial	Severe	Critical

Table 3 - Threat Levels

Obtaining Threat Information from the Security Authorities

88. To request Threat information from CESG contact either your CESG Customer Account Manager, or the Threat Assessment team: threat@cesg.gsi.gov.uk, phone 01242 221491 ext 30165. Note that CESG's capacity for producing threat assessments is limited and subject to a prioritisation process, and in many instances an Accreditor will prefer an in-house assessment on the basis that it will be adequate and more quickly available.

89. To request threat information from CPNI contact enquiries@cpni.gov.uk or phone 020 7233 8181.

90. To request threat information from DIS contact, via the MOD email and telephone networks:

- SITCEN DIRM: e-mail DI OPS-SITCEN DIRM, telephone 9621 87215
- SITCEN DTR: e-mail DI OPS-SITCEN DTR, telephone 9621 82700

Step 3: Define the Focus of Interest (Fol)

91. The purpose of Step 3 is to define the specific groups of assets, features and facilities that will be the focus of a particular risk assessment. This is known as the focus of interest.

92. To some extent it is for the Analyst to decide what is included in a Fol. If assets are not grouped into a Fol each asset should be considered individually. This will mean more work for the Analyst than is required. If too many assets are grouped together then there are a number of dangers:

- That risks within a Fol will be missed in the analysis
- That more controls than are appropriate will be required, as the risk assessment will focus on the worst case (highest) BILs. Experience and judgement will help determine the optimum grouping.
- That pragmatic, appropriate and cost effective controls will not be applied at the right point in the system.

93. Complete Form 3 (shown below), grouping assets features and facilities where they can sensibly be considered together. The method is:

- Create a row for each identified Fol and enter a Fol name in column 3.1 for each;
- List all assets contained within the Fol in column 3.2 (These should be taken from Form 1)
- Describe the rationale for the grouping of those assets in column 3.3.
- Determine from Form 1 the highest business impact level of any asset within the Fol for each property of C, I and A and enter those values in column 3.4.

Technical Risk Assessment

Form 3 – Focus of Interest					
3.1 Fol Name	3.2 Assets	3.3 Rationale	3.4 Max Impacts		
			C	I	A
Create a name for the focus of interest: <i>The Secret ICT System</i>	List all assets that fall within that Fol (your model should help): <i>The Secret Database</i>	Why have you chosen this collection of assets as an Fol? <i>All assets that are Secret are grouped together for the purposes of a risk assessment</i>	5	3	3

Form 3 - Focus of Interest

Step 4: Define Threat Actors

94. The purpose of Step 4 is to define the threat actor groups and assess the threat level they pose. Threat actors are specific to each Fol, so a Form 4 **must** be generated for each Fol.

95. A threat actor is someone who can actually carry out an attack on the Fol, so they must have an opportunity to do so. That opportunity may be very brief, but as attack can be planned and prepared in advance even a brief opportunity may be adequate.

96. If a Threat Assessment is available from the Security Authorities for a threat actor group then this assessment should be used directly. In this case, simply mark the Form 4 columns 4.4 - 4.10 'N/A', with the source of the threat assessment and enter the threat level in column 4.11.

97. Identifying the threat actor groups is a matter of judgement. The Analyst should consider the question "which groups could plausibly attack the system?" Each group may contain a number of threat actor types. A threat actor type falls into a

particular group if it is reasonably likely that the threat actor type would be able and willing to use the compromise methods appropriate to that type.

98. The process for completing Form 4 is:

- The identified threat actor group should be entered in column 4.1 with a description of that group.
- Each threat actor group will include one or more threat actor types (for example Organised Crime may be both Persons Within Range and Physical Intruders). Applicable threat actor types should be entered in Column 4.2
- Any clearances held by the threat actor group should be entered in column 4.3. If the group contain a mix of clearances then the worst case (lowest) clearance should be used. Where the threat actor group holds a non-UK clearance, then judgement should be used to determine whether that clearance is acceptable and applicable for the system under consideration. There are no specific rules and each case must be considered on its own merits.
- For each property assess the threat actors' 'Native' (unenhanced by another threat source) capability using Table 4, enter the value in column 4.4. You may enter N/K (Not Known) if the threat actor's capability is not known and is likely to be dominated by another threat source.
- For each property assess the threat actors' 'Native' (unenhanced by a another threat source) motivation using Table 5, enter the value in column 4.5. Note that this table has some limits based on the threat actor's formal clearance and their 'deterability'. You may enter N/K (Not Known) if the threat actor's motivation is not known and is likely to be increased by another threat source.
- Use Table 6 to determine the threat actors' native threat level, enter the value in column 4.6.
- Assess, using professional judgement and if necessary consulting others such as the Accreditor, whether any threat actors are likely to be influenced by any of the threat sources identified in Step 2.
 - If the answer is no enter 'None' in column 4.7 and enter 'N/A' in columns 4.8, 4.9 and 4.10.
 - If the answer is yes then assess which threat source will be dominant, replicate the name or identifier into column 4.7. Note that there can be different dominant threat sources for different properties, e.g., a Foreign Intelligence Service for confidentiality and a Terrorist Group for availability.

Technical Risk Assessment

- Assess the threat actor's enhanced capability using Table 4. (Assess to what level the threat source will raise the threat actor's capability by supplying tools and techniques.) The value must not be lower than the native capability, nor higher than the threat source's capability. Enter the value in column 4.8.
- Assess the threat actor's enhanced motivation using Table 5. (Assess to what level the threat source will increase the threat actor's motivation.) The value must not be lower than the native motivation, nor higher than the threat source's priority. Also note that threat actors with formal clearances have maximum motivations, as stated in Table 5. Enter the value in Form 4 column 4.9.
- Determine the threat actor's enhanced threat level from Table 6, enter the value in Form 4 column 4.10.
- Select the final threat level, which is either the native threat level (from column 4.6), or the enhanced threat level (from column 4.10). Enter the value in Form 4 column 4.11.
- If there is a plausible risk that the threat actor group could accidentally cause a security breach assess the threat level using Table 7 and enter the estimated level in Form 4 column 4.11 in the appropriate row; if there is no such plausible risk enter N/A.

99. Assessing which threat sources will influence threat actors is a matter for significant professional judgement, possibly involving discussion with the Accreditor and Security Authorities. There are no firm rules and the simplistic option of always assuming worst-case can very heavily overestimate risk levels and lead to impossibly onerous controls being imposed.

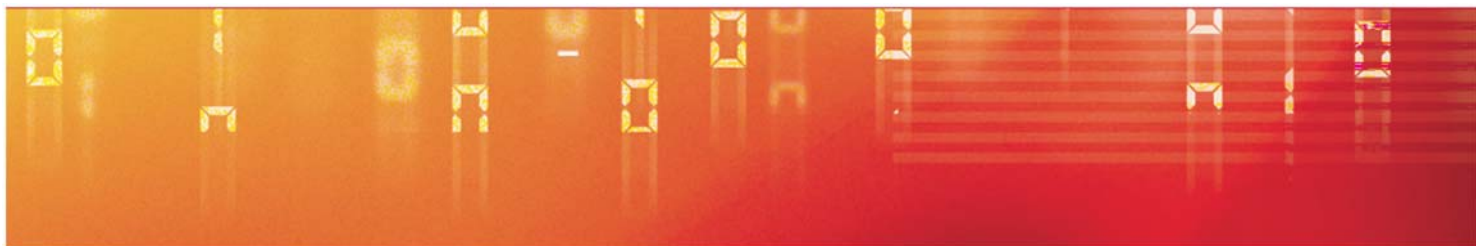
Fol		There will be one Form 4 for each Fol. Identify the Fol here.		Form 4 – Threat Actors								
4.1 Threat Actor Group Name	4.2 TA Types	4.3 Clearance	Property	4.4 Native Capability	4.5 Native Motivation	4.6 Native Threat Level	4.7 Dominant Influencing Threat Source	4.8 Enhanced Capability	4.9 Enhanced Motivation	4.10 Enhanced Threat Level	4.11 Final Threat Level	
			C	Refer to Table 4	Refer to Table 5	Refer to Table 6	Record if any	Refer to Form 2 and Table 4	Refer to Form 2 and Table 5	Refer to Table 6	Either of 4.6 or 4.10	
			I									
			A									
			Accidental Compromise								Refer to Table 7	
Users of the Secret Database	NU	SC	C	2	2	Negligible	FIS of Country X	3	3	Moderate	Moderate	
			I									
			A									
			Accidental Compromise									
			C									
			I									
			A									
			Accidental Compromise									

Form 4 -Threat Actors

Technical Risk Assessment

Capability	Description
5 – FORMIDABLE	<p>Where the threat actors are resourced by a threat source with Formidable capability, i.e. in addition to lower capabilities can:</p> <ul style="list-style-type: none"> • Devote a several man-months or even years to penetrating a system • Use specially developed bespoke attacks • Deploy a large amount of equipment • Deploy physical attacks to facilitate further technical compromise <p>Typically a full-time well-educated computer expert</p>
4 – SIGNIFICANT	<p>Where the threat actors, can</p> <ul style="list-style-type: none"> • Devote between a few man-months or a few man-weeks to penetrating a system • Adapt publicly available attack tools for specific targets • Deploy a large amount of equipment • Deploy physical attacks to facilitate further technical compromise <p>Typically a full-time well-educated computer expert</p>
3 – LIMITED	<p>Where the threat actors, can:</p> <ul style="list-style-type: none"> • Devote a few man-weeks or days to penetrating a system • Use well-known publicly available attack tools • Deploy a small amount of equipment <p>Typically a trained computer user</p>
2 – LITTLE	<p>Where the threat actors can:</p> <ul style="list-style-type: none"> • Devote a few man-hours or days to penetrating a system • Deploy a small amount of equipment <p>Typically an average untrained computer user</p>
1 – VERY LITTLE	<p>Where the threat actor has almost no capabilities or resources, i.e. can:</p> <ul style="list-style-type: none"> • Devote a few hours to penetrating a system using only the equipment already connected to the system. • Use simple plug and play devices and removable media

Table 4 - Threat Actor Capability



Motivation	Description
<p>5 – VERY HIGH (FOCUSED)</p>	<p>It is assessed that the threat actor’s prime aim is to attack the system.</p> <p>With a very substantial (>~1000) Uncleared threat actor group normally it should be assumed that some will fall into this category</p>
<p>4 – HIGH (COMMITTED) (Maximum for BS cleared threat actors) (Maximum for deterrable uncleared threat actors)</p>	<p>It is assessed, taking any formal clearances into account and whether they could be deterred, that the threat actor will attempt to attack the system on a frequent or constant basis</p> <p>With a substantial (>~100) Uncleared threat actor group normally it should be assumed that some will fall into this category</p>
<p>3 – MEDIUM (INTERESTED) (Maximum for SC cleared threat actors) (Maximum for deterrable BS cleared threat actors)</p>	<p>It is assessed, taking any formal clearances into account and whether they could be deterred, that the threat actor will attempt to attack the system if the opportunity arises fortuitously or the attack takes minimal effort.</p> <p>With a substantial (>~100) BS threat actor group it should be assumed that some will fall into this category</p>
<p>2 – LOW (CURIOUS) (Maximum for DV cleared Threat Actors) (Maximum for deterrable SC cleared threat actors)</p>	<p>It is assessed, taking any formal clearances into account and whether they could be deterred, that the threat actor may casually investigate or attack the system if exposed to it, but will not seek the system out to attack it.</p> <p>With a substantial (>~100) SC threat actor group it should be assumed that some will fall into this category</p>
<p>1 – VERY LOW (INDIFFERENT) (Maximum for deterrable DV cleared threat actors)</p>	<p>It is assessed, taking any formal clearances into account and whether they could be deterred, that the threat actors will not attack the system.</p> <p>SC and DV threat actors normally fall into his category unless there is reason to think they fall into a higher category</p>

Table 5 - Threat Actor Motivation

Technical Risk Assessment

		Capability Level				
		1 VERY LITTLE	2 LITTLE	3 LIMITED	4 SIGNIFICANT	5 FORMIDABLE
Motivation	1 INDIFFERENT	Negligible	Negligible	Low	Low	Moderate
	2 CURIOUS	Negligible	Negligible	Low	Moderate	Substantial
	3 INTERESTED	Negligible	Low	Moderate	Substantial	Severe
	4 COMMITTED	Low	Low	Moderate	Severe	Severe
	5 FOCUSED	Low	Moderate	Substantial	Severe	Critical

Table 6 - Threat Levels

Threat Level	Threat Actor Group Characteristic
SEVERE	<p>Where the threat actor group is demonstrably very poorly behaved, very often ignores security advice, is frequently erratic and unreliable.</p> <p>The group may be under enormous pressure to deliver and a lack of training and awareness leads them to carry out un-safe actions for business expediency.</p> <p>Past history demonstrates a significant number of accidental breaches on a frequent basis.</p> <p>Typically where the organisation fails to meet IA Maturity Model Level 1.</p>
SUBSTANTIAL	<p>Where the threat actor group is not well-behaved, occasionally ignores security advice, is occasionally erratic and unreliable.</p> <p>The group may be under pressure to deliver business results and may not follow rules or procedures in order to deliver business.</p> <p>Past history shows a significant number of accidental breaches.</p> <p>Typically where the organisation meets Level 1 on the IA Maturity Model.</p>
MODERATE	<p>Where the threat actor group is reasonably well behaved and reliable, and accepts the need for security controls.</p> <p>The group has been well trained in the need to follow procedures and rules and typically will not seek to bypass controls in the course of business delivery. History will show few accidental breaches and lessons will have been learnt from them when they do occur.</p> <p>Typically where the organisation meets Level 2 on the IA Maturity Model</p> <p>Unless there is evidence to the contrary this will normally be appropriate to the normal user in most Government Departments and similar organisation.</p>
LOW	<p>Where the threat actor group is extremely well behaved, takes security seriously, is very security aware and conscientious, and is reliable.</p> <p>The group are extremely well trained in the need for secure practices and there is little evidence of accidental breaches. Those that do occur are fully investigated and lessons implemented to prevent re-occurrence.</p> <p>Typically where the organisation meets Level 3 on the IA Maturity Model.</p> <p>Unless there is evidence to the contrary this will normally be appropriate to the normal user in organisations such as in intelligence organisations, key military organisations, organisations undertaking safety-critical work and the system administrators in most government organisations.</p>

Table 7 - Threat Levels for Accidents

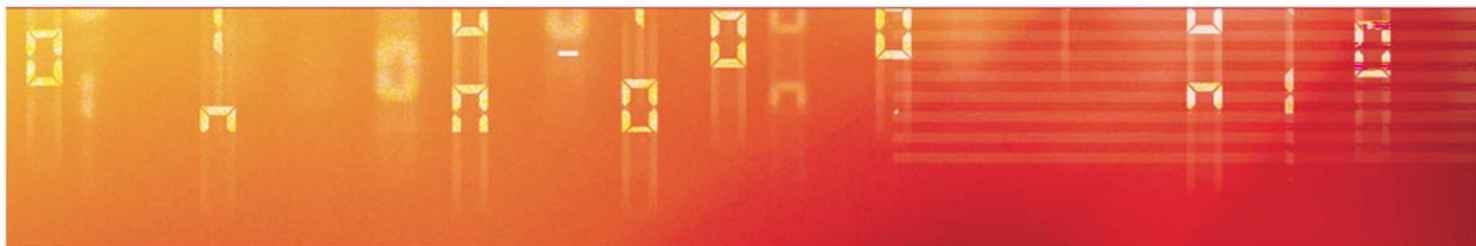
Technical Risk Assessment

Step 5: Identify the Specific Risks and Estimate Risk Levels

100. Step 5 is one of the key parts of the risk assessment process. It results in the production of a list of risks and generates a risk level for each.

101. The process to complete Form 5 is:

- Create a Form 5 for each FoI/threat actor group combination (and repeat the following steps for each form);
- Record an identifying number for the form, the FoI under consideration, the threat actor group and the threat actor types that are in the group. Record the minimum clearance of the group and any influencing threat sources. All of this information is available from Forms 3 and 4.
- For each property of C, I and A record the maximum BIL of the FoI in column 5.1. This information is available from Form 3.
- For each property of C, I and A determine which compromise methods apply for the threat actor group. Use Appendix C to provide guidance, however professional judgement is required. Not all compromise methods will necessarily apply and the Analyst may wish to modify the way the compromise method is stated to provide more detail in the assessment. Record the compromise methods in column 5.2.
- The appropriate threat level for the threat actor group has been evaluated in Step 4. This value should be replicated in column 5.3.
- Finally the risk level can be evaluated by combining threat level and BIL according to Table 8 below. This risk level should be recorded in column 5.4 and provided with a unique identifier in column 5.5.



Form 5 – Risk Assessment					
	Form 5 Number	There will be a number of Form 5s so it is helpful to number them			
	Focus of Interest	Record the applicable Fol <i>The Secret ICT System</i>			
	Threat Actor Group	There will be one Form 5 for each identified threat actor group for each Fol. <i>Users of the Secret Database</i>			
	Threat Actor Types	<i>Normal User</i>			
Threat Actor Clearance			Taken from Form 4: SC		
Influencing Threat Sources			Taken from Form 4: <i>FIS of Country X</i>		
	5.1	5.2	5.3	5.4	5.5
Property	Max BIL	Compromise Method	Threat Level	Risk Level	Risk ID
C	5	Record each relevant compromise method	Form 4	Table 8	
		<i>Deliberately Releases</i>	<i>Moderate</i>	<i>Medium - High</i>	
I					
A					
NOTES					

Form 5 - Risk Assessment

Technical Risk Assessment

		Threat Level					
		Negligible	Low	Moderate	Substantial	Severe	Critical
Business Impact of Risk Realisation (Business Impact Level - BIL)	BIL0	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low
	BIL1	Very Low	Very Low	Very Low	Low	Low	Low
	BIL2	Very Low	Low	Low	Medium	Medium	Medium
	BIL3	Very Low	Low	Medium	Medium	Medium-High	Medium-High
	BIL4	Low	Medium	Medium	Medium-High	High	High
	BIL5	Medium	Medium	Medium-High	High	High	Very High
	BIL6	Medium	Medium	Medium - High	High	Very High	Very High

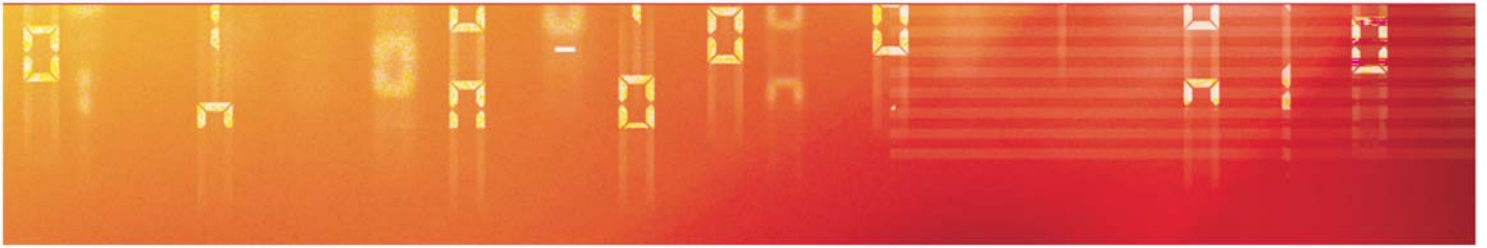
Table 8 - Risk Levels

Step 6: Prioritise and Present the Risks

102. The final Step is Step 6. The purpose of this step is solely to present a consolidated and prioritised list of risks in a relatively easily understood format. It is a natural breakpoint at which to review the assessment.

103. Form 6 (below) should be completed:

- Sort the risks into priority order with the highest risk level. The risk ID, description and risk level should be recorded in columns 6.1, 6.2 and 6.3;
- The description should provide an understandable textual description of the risk in business language;
- Risks may be colour coded to aid ease of understanding.



Form 6 – Prioritised Risk List		
6.1 Risk ID	6.2 Description	6.3 Risk Level
Form 5	Each risk should be described in normal language	Form 5
	<i>A Normal User (influenced by FIS of Country X) may deliberately release information from The Secret ICT System compromising its confidentiality and leading a possible business impact of BIL5.</i>	<i>Medium - High</i>

Form 6 - Prioritised Risk List

Technical Risk Assessment

Appendix A: Business Impact Level Tables

Introduction

1. This Appendix provides a framework to allow organisations to assess the Business Impact Level (BIL) for compromises of the confidentiality integrity or availability of information and ICT systems. The business impact level scale ranges from 0 (no impact) to 6 (extreme impact). The business impact of a loss of confidentiality, integrity and availability should be assessed as independent properties for any given asset or set of assets.
2. A number of tables are provided that describe business impact statements for various sectors of the UK. The aim is to provide a common set of standards that lead to a consistent approach to the assessment of business impact. Tables have been written from the perspective of UK society. This means that it should be possible to compare impact from across different sectors more readily.

Using the tables

3. It is unlikely that all definitions associated to a particular Impact Level in any given table will apply. Some will be relevant, others not. It is also probable that definitions from more than one business area, sub-category and impact level may apply. In these cases, judgement is required to select the most appropriate in the environment in question.

Selecting the Correct Table

4. Business areas and sub-categories are defined within the table and should be selected on the basis of those, which most closely relate to the asset under consideration. For example, if you are a local authority your business area is primarily providing a public Service and there are a number of sub-categories applicable. For example the loss of availability of a system supporting a key transport mechanism, may impact both sub-categories of Transport (direct loss of transport impact) and Finance (the economic effect on business of a lack of transport). Where more than one category is relevant then the worst-case business impact should be selected.

Impacts to Confidentiality and Protective Markings

5. Where a UK Protective Marking is applied to an asset there is a direct correlation between this and business impact level. The Protective Markings of PROTECT, RESTRICTED, CONFIDENTIAL, SECRET and TOP SECRET directly match to business impact levels 2, 3, 4, 5 and 6 respectively. This is a one-way relationship. It is not the case that an asset with a business impact level of 5 for

confidentiality necessarily should be marked SECRET. This is especially true of impacts to aggregated data. GPG 9 provides further guidance on managing aggregation.

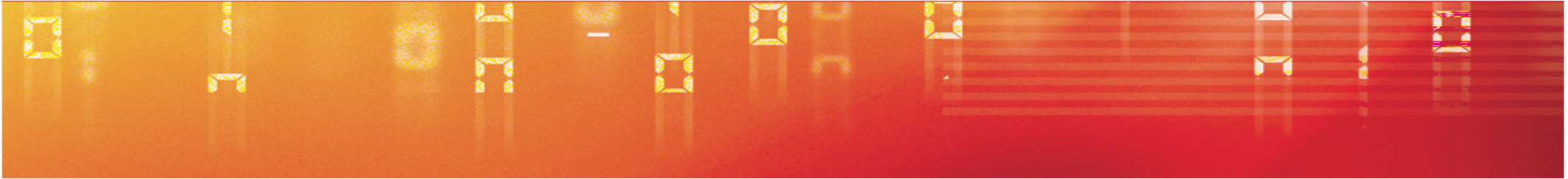
Terminology

6. Many impact level definitions are provided with a descriptive adjective, for example 'minor' or 'major'. In this context they are simply portraying a level of importance to the impact in a particular business environment. There are a number of relative terms used within the table, and their use is not precisely defined, rather it is appropriate to the business function in question. For example, 'medium term' in one case may mean 2 to 5 days, but in another case may mean up to 3 years. Interpretations may be used as long as they can be justified in the RMADS and accepted by the Accreditor.

Technical Risk Assessment

Sub Category	BIL 0	BIL 1	BIL 2	BIL 3	BIL 4	BIL 5	BIL 6
Impact on life and safety	None	None	Inconvenience or discomfort to an individual	Risk to an individual's personal safety or liberty	Risk to a group of individual's security or liberty	Threaten life directly leading to limited loss of life	Lead directly to widespread loss of life
Impact on political stability	None	None	None	Minor loss of confidence in Government	Major loss of confidence in Government	Threaten directly the internal political stability of the UK or friendly countries	Collapse of internal political stability of the UK or friendly countries
Impact on military operations	None	Minimal delay to or loss of minor supply service	Loss of a number of minor supply services	Make it more difficult to maintain the operational effectiveness or security of UK or allied forces (e.g. compromise of UK forces training materials or supply procedures)	Cause damage to the operational effectiveness or security of UK or allied forces (e.g. compromise of a logistics system causing re-supply problems without causing risk to life)	Cause severe damage to the operational effectiveness or security of UK or allied forces (e.g. compromise of the operational plans of units of company size or below in a theatre of military operations)	Cause exceptionally grave damage to the operational effectiveness or security of UK or allied forces (e.g. compromise of the operational plans of units of battalion size or above in a theatre of military operations)
Impact on foreign relations	None	None	None	Cause embarrassment to Diplomatic relations	Materially damage diplomatic relations (e.g. cause formal protest or other sanctions).	Raise international tension, or seriously damage relations with friendly governments	Directly provoke international conflict, or cause exceptionally grave damage to relations with friendly governments
Impact on international trade negotiations	None	None	None	Disadvantage a major UK Company	Disadvantage a number of major UK Companies	Disadvantage the UK in international negotiations (e.g. advance compromise of UK negotiation strategy or acceptable outcomes, in the context of a bilateral trade dispute)	Severely disadvantage the UK in international negotiations (e.g. advance compromise of UK negotiation strategy or acceptable outcomes, in the context of a major EU or WTO negotiating round)
Impact on intelligence operations	None	None	None	Damage unique intelligence operations in support of intelligence requirements at JIC Priority Three or less.	Halt unique intelligence operations in support of intelligence requirements at JIC Priority Three or less, or damage unique intelligence operations in support of requirements at Priority Two	Halt unique intelligence operations in support of intelligence requirements at JIC Priority Two, or damage unique intelligence operations in support of intelligence requirements at JIC Priority One. Cause damage to UK or allied intelligence capability	Halt unique intelligence operations in support of intelligence requirements at JIC Priority One. Cause severe damage to UK or allied intelligence capability

Table A1 – Defence, International Relations, Security and Intelligence



Sub Category	BIL 0	BIL 1	BIL 2	BIL 3	BIL 4	BIL 5	BIL 6
Impact on life and safety	None	None	Inconvenience or cause discomfort to an individual	Risk to an individual's personal safety or liberty	Risk to a group of individuals safety or liberty.	Threaten life directly leading to limited loss of life	Lead directly to widespread loss of life
Impact on provision of emergency services	None	Minor disruption to service activities that requires reprioritisation at the local level to meet expected levels of service	Minor disruption to emergency service activities that requires reprioritisation at the area or divisional level to meet expected levels of service	Disruption to emergency service activities that requires reprioritisation at the county or organisational level to meet expected levels of service	Disruption to emergency service activities that requires reprioritisation at the national level (e.g. one police force requesting help from another) to meet expected levels of service	Disruption to emergency service activities that requires emergency powers to be invoked (e.g. military assistance to the emergency services) to meet expected levels of service	Threaten directly the internal stability of the UK or friendly countries leading to widespread instability
Impact on crime fighting	None	None	None	Hinder the detection, impede the investigation, or facilitate the commission of low-level crime (i.e. crime not defined in legislation as "serious crime"), or hinder the detection of serious crime	Impede the investigation of, or facilitate the commission of serious crime (as defined in legislation)	Cause major, long-term impairment to the ability to investigate serious crime (as defined in legislation)	Cause major, long-term impairment to the ability to investigate serious organised crime (as defined in legislation).
Impact on judicial proceedings	None	None	Minor failure in local Magistrates courts	Cause a low-level criminal prosecution to collapse; cause a conviction for a low-level criminal offence to be declared unsafe or referred for appeal.	Cause a serious crime prosecution to collapse; cause a conviction for a serious criminal offence to be declared unsafe or referred for appeal	Cause a number of criminal convictions to be declared unsafe or referred to appeal (e.g. through persistent and undetected compromise of an evidence-handling system)	Major long term damage to UK judicial system

Table A2 – Public Order, Public Safety and Law Enforcement

Technical Risk Assessment

Sub Category	BIL 0	BIL 1	BIL 2	BIL 3	BIL 4	BIL 5	BIL 6
Impact on public finances	None	Loss to Public Sector of up to £10,000	Loss to Public Sector of up to £1 million	Loss to HMG/Public Sector of £millions	Loss to HMG/ Public Sector of £10s millions, up to £100 million	Short term material damage to national finances or economic interests (to an estimated total of £100s millions to £10 billion)	Major, long term damage to the UK economy (to an estimated total in excess of £10 billion)
Impact on UK trade and commerce	None	None	Undermine the financial viability of a number of UK small businesses	Undermine the financial viability of a minor UK-based or UK-owned organisation	Undermine the financial viability of a major UK-based or UK-owned organisation	Material damage to international trade or commerce, directly and noticeably reducing economic growth in the UK	Major, long term damage to global trade or commerce, leading to prolonged recession or hyperinflation in the UK

Table A3 – Trade, Economics and Public Finance

Sub Category	BIL 0	BIL 1	BIL 2	BIL 3	BIL 4	BIL 5	BIL 6
Inconvenience and impact on public confidence in public services	None	Likely to reduce an individual citizen's perception of that service (e.g. a compromise leading to the cancellation of a hospital appointment)	Likely to reduce the perception of that service by many citizens (e.g. compromise leading to an outpatient clinic closing for a day, with cancellation of appointments)	Likely to result in undermined confidence in the service provider generally (e.g. public failures at a hospital leading to noticeable lower public confidence in that hospital)	Likely to result in undermined confidence in the service at a national level (e.g. compromise of national patient information databases leading to undermined confidence in the NHS)	May lead to a loss of public trust in the service severe enough to cause a noticeable drop in citizens using the service through mistrust, with consequent risk to life	May lead to a complete breakdown in public trust, black market services thrive, consequent widespread loss of life or critical impact on continuity of government
Impact on public finances	None	Likely to cause a loss to the Public sector of up to £10,000	Likely to cause a loss to the Public sector of up to £1 million	Likely to cause a loss to HMG/ Public sector of £millions	Likely to cause a loss to HMG/ Public sector of £10s millions, up to £100 million	May cause short term material damage to national finances or economic interests (to an estimated total of £100s millions to £10 billion)	May cause major, long term material damage to the UK economy (to an estimated total in excess of £10 billion)
Impact on non-public finances	None	Minor financial loss to an individual or business (typically up to £100)	Significant financial loss to an individual or business	Severe financial loss to any individual such as unemployment or loss of a small UK business	Devastating financial loss for an individual, or severe economic loss leading to loss of a large company or employer or a number of small businesses	Material financial loss to the UK economy, leading to loss of a number of large organisation or severe damage to entire market sectors	Extensive financial losses across the economy leading to significant long-term damage to the UK, such as wide spread unemployment and recession
Locally provisioned services with an impact on the personal safety of citizens (e.g. sheltered accommodation)	None	None	Low risk to an individuals personal safety (e.g. the compromise of the address of a victim of abuse, where there is a low risk of further abuse if such information became known)	Directly lead to a risk to an individuals personal safety (e.g. the compromise of the address of a victim of abuse, where there is a reasonable risk of further abuse if such information became known)	Serious risk to any individual's personal safety (e.g. the compromise of the address of a victim of abuse, where serious further abuse is likely if such information became known)	Threaten life directly (e.g. the compromise of witness protection information, where there is a real risk of attempted murder if the information became known)	Directly threaten or lead to wide spread loss of life (particularly social care and environmental health services)

Technical Risk Assessment

Sub Category	BIL 0	BIL 1	BIL 2	BIL 3	BIL 4	BIL 5	BIL 6
Locally provisioned services with an impact on the health of citizens (e.g. waste disposal)	None	Disruption to a local service	Disruption, compromise or flawed working of local services which could pose a risk to health (e.g. spread of disease)	Authority-wide disruption, compromise or flawed working of services which could pose an increased risk to health (e.g. spread of disease)	Significant authority-wide disruption, compromise or flawed working of services which could lead to major health risks	Major disruption or compromise of a Local Authorities services, or critical faults within these services, which could lead to severe health risks and limited loss of life	Catastrophic disruption or compromise of a number of Local Authority services, or catastrophic faults within these services, which could lead to severe health risks and widespread loss of life
Locally provisioned services with no impact on health or safety of citizens (e.g. library services, land use and planning services)	None	Cancellation of services to a small number (up to 10) of citizens (e.g. closure of a library or other facility)	Cancellation of services to a number (up to 100) of citizens (e.g. closure of a library or other facility)	Cancellation of multiple services to a number (up to 1000) of citizens leading to significant individual financial losses	Loss of major services provided by a Local Authorities leading to major financial losses to the Local Authority or Citizens	Total loss of major services provided by a Local Authorities leading to severe financial losses to the Local Authority or devastating losses to Citizens.	Total loss of major services provided by a number of Local Authorities leading to severe financial losses to the Local Authorities and Citizens, leading to major economic damage.
Locally provisioned services in support of the Civil Contingencies Act	None	Isolated or minor incident to which a Local Authority is not able to react within a few days which affects a small number of citizens	Isolated or minor incident to which a Local Authority is not able to react within a few days which affects a number of citizens/local businesses	Significant incident to which a Local Authority is not able to react within 24 hours which affects a large number of citizens/local businesses - e.g. significant flooding, fire, contamination or explosion.	Major incident to which a Local Authority is not able to react within 24 hours which affects a large number of citizens/local businesses - e.g. major flooding, fire, contamination, explosion or CNI failure.	Major incident to which a Local Authority is not able to react within 12 hours which affects a large number of citizens/local businesses - e.g. major flooding, fire, contamination, explosion or CNI failure	Major incident to which several Local Authorities are not able to react within 12 hours which affects a large number of citizens/local businesses - e.g. major flooding, fire, contamination, explosion or CNI failure.

Table A4 – Public Services

Sub Category	BIL 0	BIL 1	BIL 2	BIL 3	BIL 4	BIL 5	BIL 6
Communications	None	Local loss of telecoms for a few hours	Local loss of telecoms for up to 12 hours	Local loss of telecoms for up to 24 hours	Loss of telecoms in a region for up to 24 hours	Loss of telecoms nationally for up to a week	Loss of telecoms nationally for more than 1 week
Power	None	Local outages causing disruption for a few hours	Local outage causing disruption for up to 12 hours	Loss of power in a region causing disruption for up to 24 hours	Loss of power in a region causing disruption for up to a week	Loss of power in a region causing disruption for more than 1 week	Loss of power nationally affecting the whole of the UK for more than 1 week
Finance	None	Minimal impact (less than £10,000)	Minor loss to a Financial Company (less than £1 million)	Major loss of a Leading Financial company of £millions	Major loss of a Leading Financial Company of £10s millions	Severe losses to UK Business of up to £100s millions	Severe financial losses to UK Business of £10s billions
Transport Note: Data based on the National Risk Assessment Impact Scale	None	Minor disruption of a key local transport systems for up to 12 hours	Minor disruption of a key local transport systems for up to 24 hours	Disruption of a number of key local transport systems for up to 24 hours	Major disruption of key regional transport systems for up to a week	Severe national disruption of key transport systems for up to a month	Severe national disruption of key transport systems for over a month
Water and Sewage	None	Breakdown of local water supplies and/or sewage service for a small number (<10) of people for more than a day	Breakdown of local water supplies and/or sewage service for a small number (<50) of people for more than a week	Breakdown of local water supplies and/or sewage service for a number (up to 100) of people or prolonged drought (up to 1 months)	Breakdown of local water supplies and/or sewage service for over 100 people or prolonged drought (up to 1 months)	Breakdown of regional water supplies and/or sewage service (effecting >100 people) or prolonged drought (up to 3 months)	Total breakdown of national water supplies and/or sewage service (effecting >100 people) or prolonged drought (> 3 months)
Food and Consumables	None	Local disruption to the distribution of some essential goods, fuel, raw materials, medicines and/or food for up to a week	Local disruption to the distribution of some essential goods, fuel, raw materials, medicines and/or disruption of food for up to a month	Regional disruption to the distribution of some essential goods, fuel, raw materials and medicines and/or widespread disruption of food for up to a week	Regional disruption to the distribution of some essential goods, fuel, raw materials and medicines and widespread disruption of food for up to a month	National disruption to the distribution of essential goods, fuel, raw materials and medicines and widespread disruption of food for up to a month	National disruption to the distribution of essential goods, fuel, raw materials and medicines and widespread disruption of food for over a month

Table A5 – Critical National Infrastructure (CNI)

Technical Risk Assessment

Sub Category	BIL 0	BIL 1	BIL 2	BIL 3	BIL 4	BIL 5	BIL 6
Impact on health and safety of the Citizen	None	Minor injury or illness with a quick (within one week) and complete recovery to an individual	Compromise an individual's personal safety or security.	Minor injuries to a group of individuals or serious injury to an individual involving slight to moderate pain for 2-7 days. Thereafter some pain/discomfort for several weeks. Some restrictions to work and/or leisure activities over several weeks/months. After 3-4 months return to normal health with no permanent disability.	Serious injury to several individuals or compromise of a group of individuals personal safety	Permanent incapacitating injury or illness to an individual, Moderate to severe pain for 1-4 weeks. Thereafter some pain gradually reducing, but may recur when taking part in some activities. Some permanent restrictions to leisure and possibly some work activities and may directly threaten their life.	Permanently incapacitating injury or illness to many individuals that may lead to widespread loss of life.
Impact on the Privacy of the Citizen	None	Loss of control of a citizen's personal data beyond those authorised by the citizen.	Loss of control of many citizens' personal data beyond those authorised by each citizen.	Loss of control of a citizen's sensitive data beyond those authorised by the citizen. A compromise to the identity or financial status of an individual citizen.	Loss of control of many citizens' sensitive or financially significant personal data beyond those authorised by each citizen. A compromise to the identity or financial status of many citizens. Increased vulnerability to criminal attack.	Widespread compromise of identity management systems or personal financial systems across the UK.	The collapse of identity management systems or personal financial systems across the UK.
Impact on the Identity of the Citizen.	None	Illicit access using one individual's identity on behalf of another would cause inconvenience to the victim.	Illicit access using one individual's identity on behalf of another would allow the entry of incorrect information, thereby causing distress, or access to payments intended for that person or could further a subsequent impersonation attack on that individual.	Illicit access using several individual's identities would allow the entry of incorrect information, thereby causing distress, or access to payments intended for those people or could further subsequent impersonation attacks on several individuals.	Illicit access using many (thousands of) individual's identities would allow the entry of incorrect information, thereby causing distress, or access to payments intended for those people or could further subsequent impersonation attacks on many individuals.	Illicit access would facilitate a serious crime, such as blackmail or long-term fraud or disrupt an on-going legal process or provide the means of creating an illicit real world identity for an individual or several individuals.	Illicit access could lead to the loss of liberty or life of an individual or several individuals.

Sub Category	BIL 0	BIL 1	BIL 2	BIL 3	BIL 4	BIL 5	BIL 6
Utilisation of Public Services	None	Minimal disruption or inconvenience in service delivery to an individual. For example an individual has to re-submit an address or re-register for a service.	Minimal disruption to a group of individuals or significant disruption in service delivery or distress to an individual. For example availability to a set of personal information is lost, requiring resubmission of identity evidence before minor services can be delivered (e.g. library lending)	Significant disruption to service delivery for a number of individuals, such as nation wide. For example loss of ability to deliver a non-essential service nation wide	Substantial disruption to service delivery to a large group of individuals, perhaps nationally. Lack of services may directly threaten the safety or wellbeing of an individual or a small group. For example, loss of personal entitlement information for social security payments	Severe disruption to service delivery to a large group of individuals, that may directly threaten safety or lead to limited loss of life, for example limited loss of sensitive police records.	Severe and widespread disruption to service delivery, which may directly lead to widespread loss of life, for example severe loss of availability of many medical records
Embarrassment or distress	None	Short term, minimal embarrassment to an individual	Short-term distress or significant embarrassment to an individual, such as compromise of their financial credit score	Prolonged distress for an individual citizen, short-term distress or significant embarrassment for many citizens. For example permanent loss of professional standing for an individual Loss, leading to identity theft for an individual	Prolonged and severe distress for a significant number of citizens, or extreme distress for an individual. For example, total compromise of an individual's medical history or partial compromise for a group. Loss, leading to identity theft for a group of individuals	Severe distress to an individual to the extent that it may lead to loss of life (for example compromise of witness protection information). Widespread and severe distress to a large group of individuals, possibly nation wide	Severe and extreme distress to a large group of individuals, leading directly to widespread loss of life. For example the total compromise of an entire nation wide witness protection scheme
Personal Finance	None	Minor loss of money for an individual, no more than an individual annoyance	Major financial loss for an individual, but not involving any financial hardship, or minor loss for a small group of individuals	Significant loss of income for an individual, such that it has a short-tem impact on the individual's way of life or causes some financial hardship.	Substantial loss of income for a significant group of individuals that causes financial hardship. Financially devastating for an individual for example personal bankruptcy and repossession of home.	Financially devastating for a large group of individuals for example wide spread personal bankruptcy and repossession of homes.	Financial impacts are wide spread to the extent that major long-term damage is caused to the UK economy.

Table A6 – Personal / Citizen¹

¹ CESG acknowledges the contribution of the BCS to the content of this table.

Technical Risk Assessment

Appendix B: Modelling Technique

Introduction

1. This appendix defines the modelling technique to assist with Step 1 of the Risk Assessment method. This is a suggested technique and therefore not a mandated part of this standard. Any modelling technique that enables the required information to be presented, agreed and analysed can be used, particularly where another modelling technique (such as engineering modelling techniques) is already used within the project. The modelling technique used should be agreed with the business and the Accreditor.
2. The Modelling Technique described here is an adaptation of the Domain Based (DBSy¹) approach that was originally developed to support the Ministry of Defence. It requires only a basic drawing package.
3. The objective of an IS1 model is to:
 - Identify the information assets that need protection;
 - Identify the people (threat actors), who may be in a position to accidentally or deliberately compromise the assets;
 - Provide a framework to be able to discuss the system and connections with the Accreditor and other interested parties;
 - Allow easier identification of appropriate FoI.
4. The essential information required to develop the model includes:
 - Information storage and exchange requirements for the system;
 - The system(s) and/or services that directly or indirectly support the implementation of the business and information exchange requirements;
 - The places where users of the system work and that contain equipment.

Risk Analysis and Analysis Scope

5. Often, systems will depend upon the services and defences that are provided by other systems. In some cases, responsibility for applications is separate from the responsibility for the infrastructure that supports them, and the applications will rely on that infrastructure for some of their protection.

¹ DBSy is a trademark owned by QinetiQ.

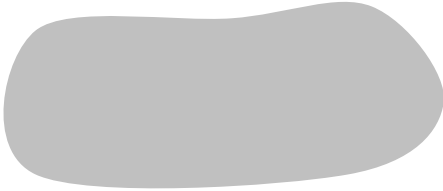

6. The IS1 modelling technique identifies assets to which the IS1 risk method will be applied. An asset will be in what the modelling technique terms a "scope" depending primarily on who is responsible for providing and protecting that asset.
7. To support the variety of ways in which a project uses and relies upon others, or provides a service on which others can rely, the IS1 modelling technique includes the concepts of:
 - **Accreditation Scope:** This includes all of the capability and services for which the project is responsible for delivering. This will typically be the same as the scope of the project;
 - **Analysis Scope:** This includes everything that is part of the risk assessment. This includes everything that is part of the project and reliance scope as well as considering business information exchange requirements and system connections;
 - **Reliance Scope:** This 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.

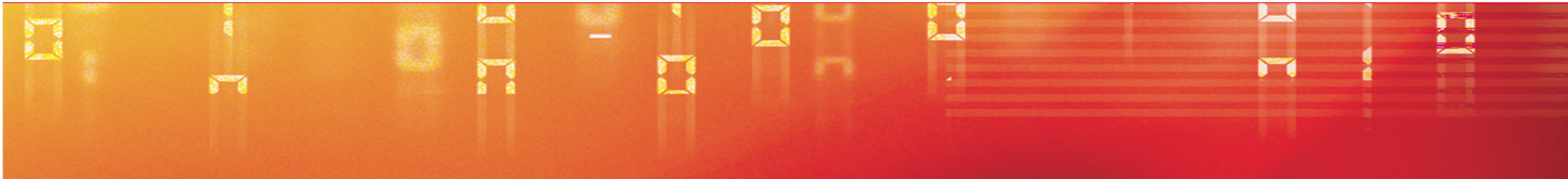
Model Concepts

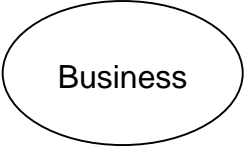
8. To enable the graphical model to represent the wide range of project and system relationships that occur within Government, there are different graphical symbols for different combinations of assets and functions.
9. IS1 Models consist of the following types of object and relationship:
 - Business objects;
 - Connection objects (one-way and bi-directional);
 - Support objects;
 - Place objects;
 - 'Uses the services of' relationship;
 - 'Contains' relationship.

Technical Risk Assessment

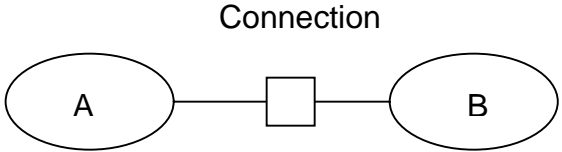
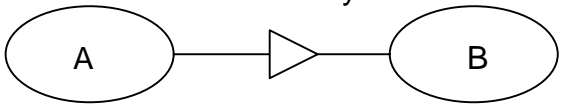
Modelling Reference Guide

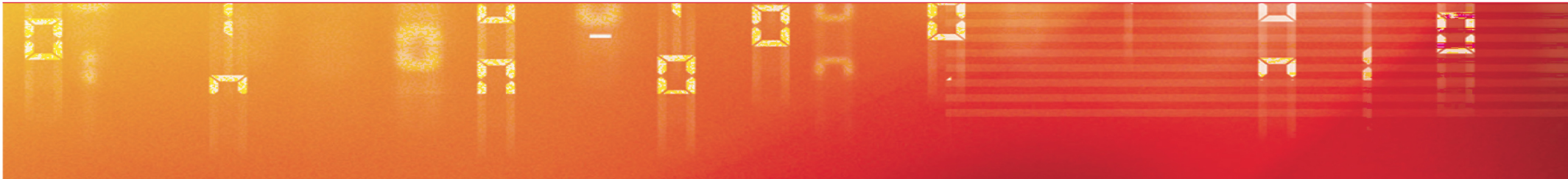
Symbol description	Graphic	Represents
Shaded freeform shape	<p>Accreditation Scope</p> 	<p>The accreditation scope identifies which objects in the model are the responsibility of a project, usually those will be the subject of an accreditation decision.</p> <p>The risk method will be applied to the object(s) within this scope to identify and rank the risks. The Risk Management and Accreditation Documentation (RMADS) will record the application of this standard to the system that is being accredited.</p>
Freeform shape with dot and dash boundary	<p>Reliance Scope</p> 	<p>The reliance scope is the set of objects, in the model, upon which an accreditation decision places some dependence. The reliance scope always includes the accreditation scope.</p> <p>Normally, the application of this risk method to those objects will have been carried out by someone else. The RMADS will need to demonstrate that the assumptions of those risk assessments are valid.</p>





<p>Named ellipse with solid boundary</p>	<p>Business Object</p> 	<p>A Business Object represents:</p> <ul style="list-style-type: none"> • One or more information assets; • Optionally the people who need to use the information to achieve some specific business objectives. These will be the account holders of the system; • Equipment and software used to store, view and process the information. <p>By default, the equipment and software in a business object includes all of the infrastructure, services and network management that supports the business and enables the business to be distributed across different geographical locations. However, in some cases it will be necessary to model some parts of the implementation as separate support objects.</p> <p>Note: readers familiar with DBSy should be aware that a business object is not the same as a DBSy domain. This is because DBSy domains are concerned with requirements, independent from implementation detail. IS1 model objects represent an actual or proposed implementation.</p>
--	--	---

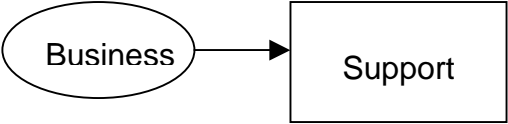
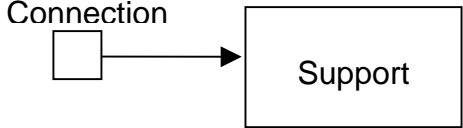
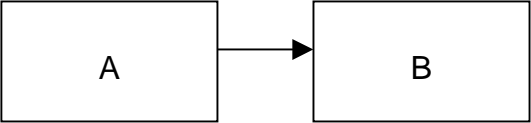
Technical Risk Assessment

<p>Solid line with named square between ellipses</p>	<p>Connection Object</p> 	<p>A connection object represents:</p> <ul style="list-style-type: none"> • Information exchange requirements between two or more business objects; • The equipment, software and services that support the information exchange; • The people who manage the equipment and provide the service. <p>By default, the support component of a connection object includes all the infrastructure, supporting management and communications services. However, in some cases it will be necessary to model some parts of the implementation as a separate support object(s).</p>
<p>Solid line with named triangle between ellipses</p>	<p>One way Connection Object</p> 	<p>A connection object that only permits a one-way transfer of information.</p> <p>People in business object B cannot use this connection to supply any information to people in business object A.</p>

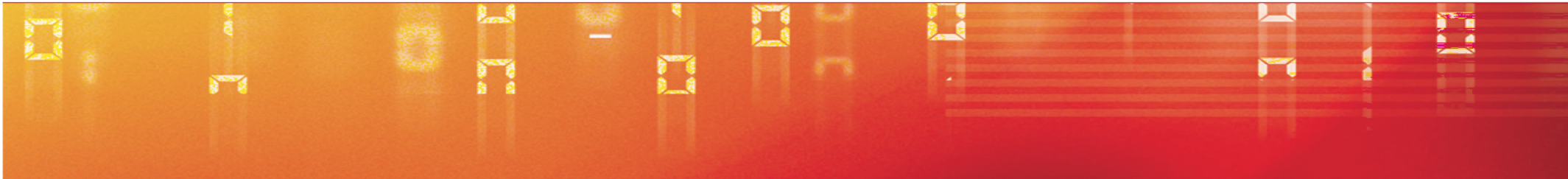


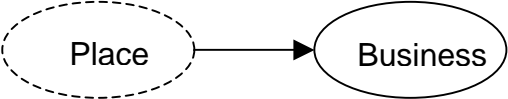
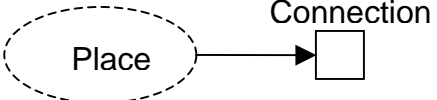
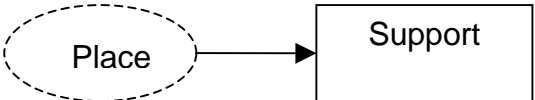
<p>Named rectangle with solid boundary</p>	<p>Support Object</p> <div style="text-align: center;">  </div>	<p>A support object represents:</p> <ul style="list-style-type: none"> • The equipment and software that provide services in support of others; • The people who manage the equipment and provide the service. <p>A support object will be needed in the following cases:</p> <ul style="list-style-type: none"> • Some part of the implementation is in a different project or reliance scope to the requirements it supports; • The same services support several objects.
<p>Named ellipse with dashed boundary</p>	<p>Place Object</p> <div style="text-align: center;">  </div>	<p>A place object represents the physical locations where people work and where equipment is located. It represents the people who have legitimate access to a particular kind of site, building or room, but who are not necessarily account holders for the systems/equipment they contain.</p>

Technical Risk Assessment

<p>Arrow from an solid ellipse to a rectangle</p>	<p>'Uses the services of'</p> 	<p>Shows that a system provides supporting services to a business object.¹ A support object is shown separately to a business object if it is in a different project or reliance scope or because it provides services to more than one object.</p>
<p>Arrow from a square (or triangle) to a rectangle</p>	<p>'Uses the services of'</p> 	<p>Shows that a system provides supporting services to a connection object. A support object is shown separately to a connection object if it is in a different project or reliance scope or because it provides services to more than one object.</p>
<p>Arrow from a rectangle to a rectangle</p>	<p>'Uses the services of'</p> 	<p>Shows that a system provides supporting services to another support object. Support objects are shown separately if they are in a different project or reliance scope or because they provide services to more than one object.</p>

¹ Note in all cases with relationships indicated by arrows the direction of the arrow follows the construction of the sentence: “the Business uses the support of the Support object” implies the arrow points from the Business to the support object.



<p>Arrow from a dashed ellipse to a solid ellipse</p>	<p>'Contains'</p> 	<p>The place represents the location of equipment that implements the business object and lets the account holders interact with the software acting on their behalf in the business object.</p>
<p>Arrow from a dashed ellipse to a square (or triangle)</p>	<p>'Contains'</p> 	<p>The place represents the location of equipment and/or system managers for supporting infrastructure and services.</p>
<p>Arrow from a dashed ellipse to a rectangle</p>	<p>'Contains'</p> 	<p>The place represents the location of equipment and/or system managers for supporting infrastructure and services.</p>

Technical Risk Assessment

Appendix C: Threat Actor Type and Compromise Methods

1. The purpose of this Appendix is to provide descriptions for type of threat actors that could be considered as potentially having capability, opportunity and motivation to attack a FoI. In addition this appendix provides an indicative list of compromise methods that could be used by each of these threat actor types.
2. Note that the threat actor type is relative to the FoI. For example a Privileged User of one FoI could be a Normal User of another FoI and an Information Exchange Partner for yet another. Also an individual may well be have more than one type with respect to a single FoI; e.g. a person may be a Bystander as well as a Supplier.

Definitions of Threat Actor Types

3. When conducting an IS1 assessment, Departments should consider the opportunity threat actors have to launch attacks on ICT systems and information. It can be considered that threat actors have an opportunity to attack an ICT system and its information by virtue of their relationship with the FoI. The following threat actor types have been grouped into 'families' of threat actor that reflect their relationship with the FoI. These can be slimmed down or expanded by the Analysts to reflect the specific requirements of their own FoI. Note that threat actor groups can be members of multiple families. The purpose of these groupings is that it may help when thinking about similar applicable compromise method detail.

System and Service Users

4. This family of threat actor types would be those that have authorised logical access to the FoI itself and any service it provides for example through provision of a web based service, a kiosk (walk in) type service or through provision of a shared service. This group could include:
 - Privileged User (PU)
 - Normal User (NU)
 - Service Consumer (SC)
 - Shared Service Subscriber (SSS)

Direct Connections

5. This family of threat actors would be those that are not authorised users of the systems or services provided by the FoI, but have business or network

connections to facilitate business information exchange or the provision and management of services used within the FoI. This group could include:

- Information Exchange Partner (IEP)
- Service Provider (SP)

Indirect Connections

6. This family of threat actors would be those that are not connected to the FoI for business purposes but have connections to those that are directly connected to the FoI for business purposes or those that share services and infrastructure with the FoI this group could include:

- Indirectly Connected (IC)

Supply Chain

7. This family of threat actor types would be those that have access to hardware and software before the FoI commissions or are those that are responsible for implementation, configuration or management of the FoI. This group could include:

- Supplier (SUP)
- Handler (HAN)

Physically Present

8. This family of threat actor types would be those that can attack the FoI by virtue of being in the physical locality, either through authorised or unauthorised access or general physical proximity. This group could include:

- Privileged User (PU)
- Normal User (NU)
- Bystander (BY)
- Person Within Range (PWR)
- Physical Intruder (PI)

Technical Risk Assessment

Description of Threat Actor Types

9. The following section provides indicative descriptions for types of threat actor.

Bystander (BY)

10.A Bystander is someone with authorised physical access to a place where the equipment within the focus of interest is located and/or account holders work, but with no business need to handle equipment or logically access the system. Typically this will include cleaners and visitors but could (for example) include hotel staff if portable equipment is left on hotel premises. (People with a need to physically handle equipment would normally be of type Handler).

Handler (HAN)

11.A Handler is someone whose business role requires physical access to the equipment within the focus of interest, but who is not a registered user and does not usually have logical access to the operational system, but may have temporary supervised access for test purposes. This includes people who transport equipment, test repair or replace hardware or dispose of obsolete or damaged equipment. This may also include postal or courier services.

Indirectly Connected (IC)

12.An Indirectly Connected threat actor does not have legitimate or authorised business connectivity to the FoI. They may however, be able to access or make use of business or network connections because of onward connections from business partners or through networks to which the FoI has a direct connection e.g. the Internet. Where Departments have direct or indirect connections to the Internet this threat actor type could include all Internet users. This indirect connectivity could allow threat actors to mount business traffic-borne or network based attacks against the FoI.

Information Exchange Partner (IEP)

13.An Information Exchange Partner is someone who needs, as part of their business, to exchange information with the focus of interest, whether through direct or indirect electronic connection or media exchange. The person may be an originator, recipient or both, of information in support of normal business. Note there must be a need to exchange information, not merely an ability to exchange information; people with the ability but not the need are Indirectly Connected.

Person Within Range (PWR)

14.A threat actor of type Person Within Range is someone who is in range of electronic, electromagnetic and any other emanations from the equipment within the FoI. This applies whether the emanations are unintentional, intentional or as the result of tampering, and hence is very broad ranging. In addition this threat

actor type due to their presence within range of emanations, transmissions and communications may be in a position to jam communication paths. This type could be considered as including people who may:

- Intercept unintentional electromagnetic emanations (TEMPEST);
- Intercept radio and wireless network transmissions;
- Passively intercept signals from transmission wires;
- Remotely probe a system other than by intercepting its intentional traffic, e.g., by reading transmissions from an implanted hardware bug;
- Remotely disrupt equipment, for example by using a High Intensity Radio Frequency transmitter (HIRF gun);
- Disrupt an external communications path, for example by jamming a radio or wireless network link.

Normal User (NU)

15.A Normal User is a registered user or account holder who uses the applications, services and equipment within the FoI to store, process, handle and exchange information in support of business objectives. These users would be provided with 'standard' facilities and system privilege as defined in the Departments policy.

Physical Intruder (PI)

16.A Physical Intruder is someone who gains unauthorised physical access to equipment within the FoI, typically by breaking in to the premises in which the FoI equipment is sited. This may include the traditional office, data centres or locations where remote working is carried out.

Privileged User (PU)

17.A Privileged User is a registered user or account holder who manages the applications, services, equipment and security defences within the focus of interest. A threat actor of this type can usually not be constrained in the same way as a Normal User and as such is modelled as a separate threat actor type.

Technical Risk Assessment

Service Provider (SP)

18. A Service Provider is someone who provides services to the Fol, including but not limited to, communications, shared databases, Internet access, web-site hosting, resource sharing, archive services or intrusion detection services and who by virtue of controlling that service could compromise any Security Property of the Fol.

Service Consumer (SC)

19. A Service Consumer is someone who makes use of services advertised or provided by the Fol. Services provided by the Fol may require that consumers are registered for access control purposes or allow unregistered physical or logical access to a publically available service (e.g. an Internet website or 'walk in' kiosk). Service Consumers may use services provided by the system (such as view a website) but are not Normal Users.

Shared Service Subscriber (SSS)

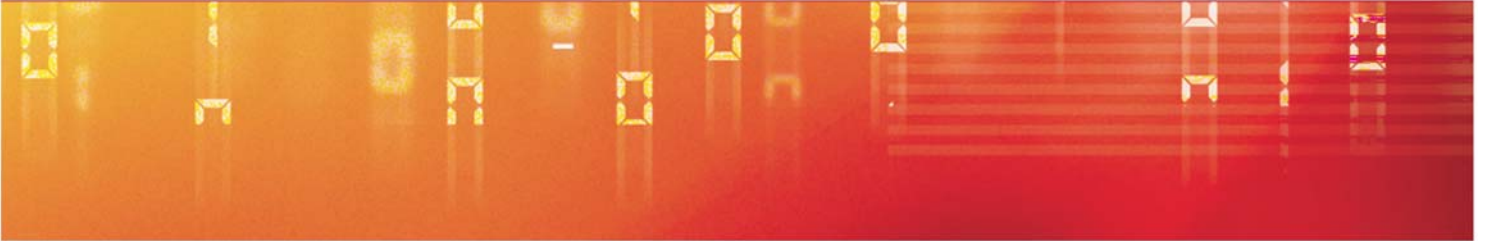
20. A Shared Service Subscriber applies only where a shared service is within the reliance scope. A Shared Service Subscriber is someone who is an authorised user of services used by a Fol, but who is not a registered user of systems or services within the Fol. This threat actor could compromise the Fol by attacking the shared service. For example, a Fol may rely upon a shared service such as power distribution. If actions of other customers of that power distribution network make in unavailable, this could in turn affect availability of the Fol.

Supplier (SUP)

21. A threat actor of type Supplier is someone in the supply chain who provides, maintains or otherwise has access to software or equipment. This threat actor type may be aware of the system and its security characteristics and be in a position to provide equipment deliberately modified or configured to allow or facilitate compromise of any security property.

Compromise Methods Available to Threat Actors

22. The tables below define the compromise methods available to each threat actor type with respect to the properties of confidentiality, integrity and availability. This includes accidental as well as deliberate compromise. The compromise methods are stated in broad terms and the intention is that all possible attacks will fall into one of the compromise methods identified in the table. However, it is possible that particular attacks may fall into more than one compromise method.



23. Discretion is required in application of these tables. The Analyst should feel free to add specific compromise methods for their system if they feel this would enable a better or more refined analysis of risk. In any case, as more information becomes known about a system then the Analyst should decompose the particular compromise methods to provide detailed risks specific to the system under consideration. For further information see Chapter 2, *Risk Management Lifecycle*.

Malware

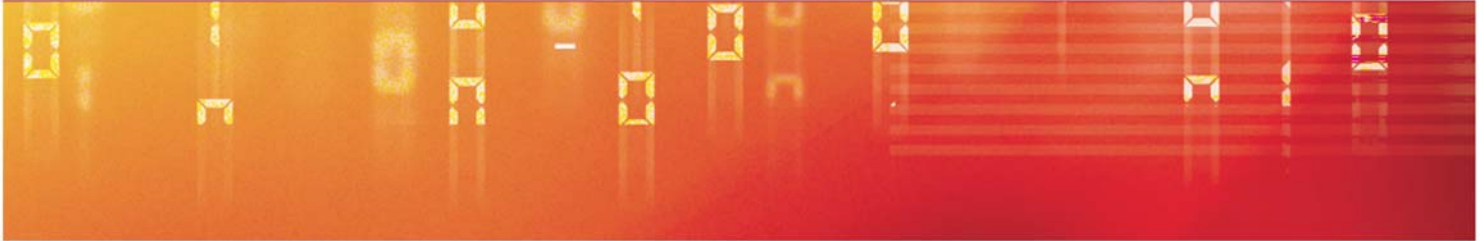
24. The treatment of malware can be difficult to analyse in the IS1 risk assessment method. The following guidance can be applied:

- The individual or organisation who creates and/or deploys the malware can be considered as the threat source, as it is them who wish the malware to compromise hosts;
- The threat actor is the individual or group whose actions cause the malware to be able to compromise an asset. For example if a user accidentally introduces malware by opening an infected email attachment, which then causes the system to crash, then they can be considered to have 'Accidentally Disrupted' an asset.

25. Table C1 (below) provides a correlation of threat actor type to compromise method.

Technical Risk Assessment

Threat Actor Type	Compromise Methods		
	Confidentiality	Integrity	Availability
Bystander (BY)	Observes Information from Passively observes information in the environment		
	Impersonates a user of Impersonates a legitimate user to compromise any Security Property		
	Tampers with equipment in Tampers with equipment in any way to compromise any Security Property, including simply stealing equipment or media.		
Handler (HAN)	Tampers with equipment in Tampers with equipment in any way to compromise any Security Property		
Indirectly Connected (IC)	Misuses Business or Network connections to or from Compromise any Security Property		
Information Exchange Partner (IEP)	Misuses Business or Network connections to or from Compromise any Security Property of the Fol		
Person Within Range (PWR)	Intercepts traffic to or from Intercept communications or emanations from the Fol (including physical media in transit, wired and wireless networks)	Injects information into Makes unauthorised changes to information transmitted on Fol communication links (including interfering with physical media links, wired and wireless networks)	Jams Denys communication links to of from the Fol (including physical media links, wired and wireless networks)
Normal User (NU)	Accidentally releases information from Performs actions which Accidentally result in the inappropriate release of information	Accidentally disrupts Performs actions which accidentally result in the compromise of Integrity or Availability	
	Deliberately releases information from Performs deliberate actions which result in the inappropriate release of information	Deliberately disrupts Performs deliberate actions which result in the compromise of Integrity or Availability	

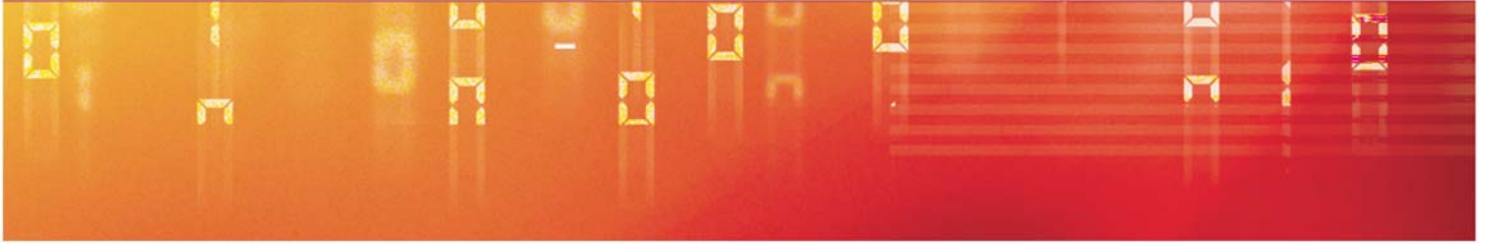


Threat Actor Type	Compromise Methods		
	Confidentiality	Integrity	Availability
	<p>Changes the configuration of Changes the system to facilitate a compromise of any Security Property</p>		
Physical Intruder (PI)	<p>Tampers with equipment in Tampers with equipment in any way to compromise any Security Property, including simply stealing equipment or media</p>		
Privileged User (PU)	<p>Accidentally releases information from Performs actions which Accidentally result in the inappropriate release of information</p>	<p>Accidentally disrupts Performs actions which accidentally result in the compromise of Integrity or Availability</p>	
	<p>Deliberately releases information from Performs deliberate actions which result in the inappropriate release of information</p>	<p>Deliberately disrupts Performs deliberate actions which result in the compromise of Integrity or Availability</p>	
	<p>Changes the Configuration of Changes the system to facilitate a compromise of any Security Property</p>		
Service Provider (SP)	<p>Intercepts traffic from or to Intercepts information that passes through the provided service</p>	<p>Corrupts Accidentally or deliberately corrupts information that passes through the provided service</p>	<p>Disrupts Accidentally or deliberately disrupts either the provided service or information that passes through the provided service</p>
Service Consumer (SC)	<p>Misuses Business or Network connections to or from Attacks the FoI using their business or network connectivity to <u>a service</u> provided by the FoI to compromise any Security Property of the FoI or the service it provides (e.g. a website).</p>		
	<p>Tampers with equipment provided by Tampers with equipment that delivers a service provided by the FoI (e.g. a kiosk) in any way that compromises any Security Property of the FoI itself or the service, including simply stealing equipment or media, installing unauthorised equipment and making unauthorised changes.</p>		

Technical Risk Assessment

Threat Actor Type	Compromise Methods		
	Confidentiality	Integrity	Availability
Shared Service Subscriber (SSS)	<p>Misuses Business or Network connections <i>to or from</i></p> <p>Attacks the Fol using business or network connectivity provided by a <u>shared service</u> to compromise any Security Property of the Fol. This includes both where the Fol is targeted through the shared service or where the effect on the Fol is from untargeted or "collateral damage" from an attack on the <u>shared service</u>.</p>		
Supplier (SUP)	<p>Tampers with equipment <i>in</i></p> <p>Tampers with equipment, either software or hardware, before it is supplied to the business to compromise any Security Property</p>		

Table C1 – Correlation of Threat Actor type and Compromise Method.



THIS PAGE IS INTENTIONALLY LEFT BLANK

Technical Risk Assessment

Appendix D: Worked Example

Introduction

1. This worked example is designed to illustrate application of the IS1 method. The scenario is entirely fictitious and the solution should not be considered as one to illustrate the method and not necessarily be a technical exemplar. Not all possible form entries are shown, as this is not necessary for illustration of the method.

Scenario

2. A new government initiative to regulate participation in dangerous sports has led to a new licensing system. Northern Lode is a new national ICT system that will hold details of licence applications and allow assessment of sensitive information and intelligence to make licensing judgements. Northern Lode has been assessed to have a security profile of 4, 3, 3 for C, I and A respectively.
3. Northern Lode will allow email (up to RESTRICTED) to another new ICT system, Southern Lode. Southern Lode has been assessed to have a security profile of 3, 3, 3. This system deals with the administrative aspects of licence applications and has a requirement to receive information by email (up to RESTRICTED) from Local Police Forces (where licences will be applied for). Southern Lode will make use of the existing accredited Police email service that is supported by the Police Intranet.
4. Southern Lode has a WiFi capability and there is a requirement for users to be able to connect to services using it.
5. There is an additional requirement for users of Southern Lode to be able to email and web browse to the Internet.
6. There are 20 Northern Lode users who all hold SC clearance. Of these there are 2 administrators. There are 50 Southern Lode users, who hold BS clearances as do all partners in the Local Police Forces.
7. Both Northern and Southern Lode are located on existing (approved) HMG premises. All visitors, cleaners and maintenance staff either hold BS clearance or will be escorted. All locations containing Northern Lode equipment or working are additionally kept in a secure area only accessible to SC cleared staff.

Step 1

- 8. The first step of IS1 is to analyse and catalogue the system. An IS1 model has been created based upon the information contained within the scenario.
- 9. The project has been tasked with creating both Southern and Northern Lode as well as email between them and email and web to the Internet. All of these objects are therefore within the accreditation scope and subject to accreditation as part of this project. The Secure Area, HMG Offices and Police Email are already approved but we rely on services they provide. They are therefore in the reliance scope.

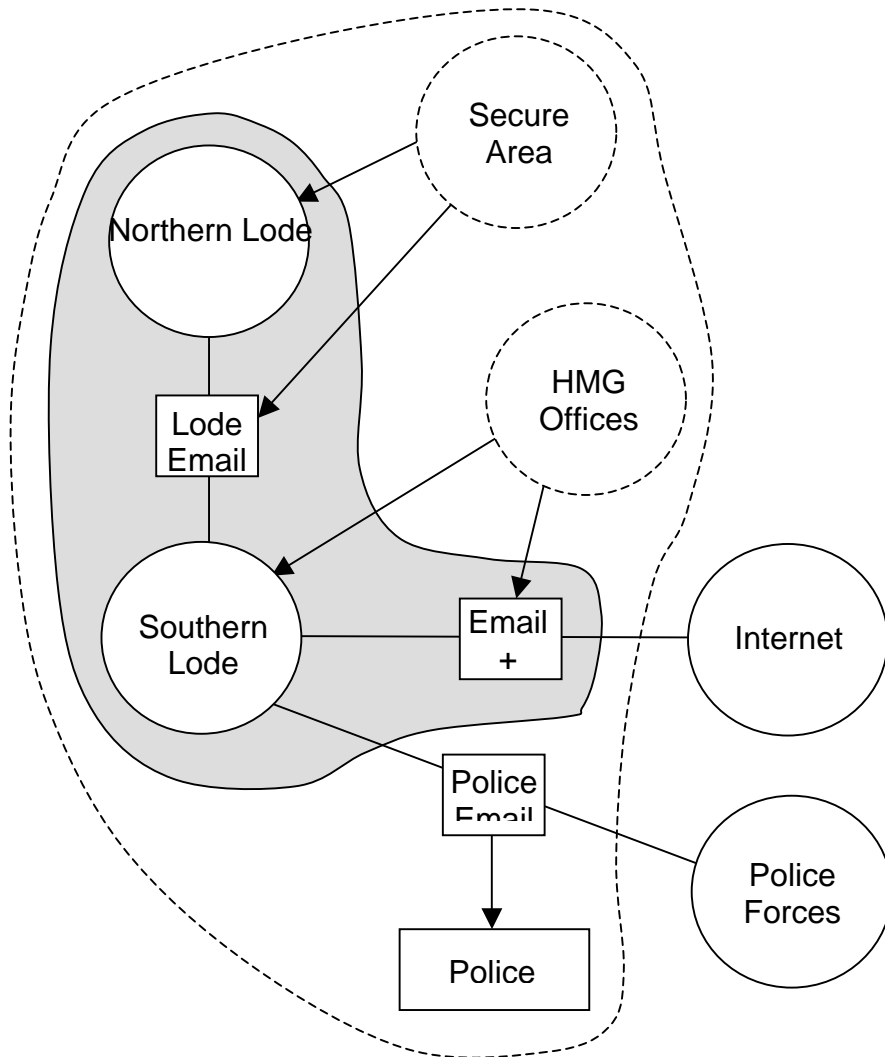


Figure D1 – Northern Lode Model

Technical Risk Assessment

10. The completed Form 1 is shown below. This simply records all of the assets within the accreditation scope, provides a description and records the maximum business impact level for each of C, I and A.

Form 1 – Asset List				
1.1 Asset Identifier	1.2 Description/Notes	1.3 Impact Levels		
		C	I	A
1 – Northern Lode	All of the information, hardware and software that comprise Northern Lode	4	3	3
2 – Southern Lode	All of the information, hardware and software that compromise Southern Lode	3	3	3
3 – Lode Email	All of the hardware and software that make up the email exchange capability, from Northern to Southern Lode	3	3	3
4 – Email + Web	All of the hardware and software that make up the email and web browsing capability from Southern Lode to the Internet	1	1	1

Step 2

11. Step 2 aims to define and assess threat sources. In this case advice was sought from the Accreditor about what particular threat sources were of concern. It was agreed that Criminal Gangs and Political Activists were applicable.

12. An in-house threat assessment was conducted using Tables 1, *Threat Source Capability* and 2, *Threat Source Priority* to derive the level of threat from Table 3, *Threat Levels*. These assessments required judgement based upon the Analysts experience and were agreed with the Accreditor. It was decided that both of these threat sources would try to influence threat actors and that they may also both be threat actors in their own right.

Form 2 – Threat Sources								
2.1 Source Name	2.2 Description (and Rationale)	Property	2.3 Capability (Table 1)	2.4 Priority (Table 2)	2.5 Threat Level (Table 3)	2.6 Source of Threat Assessment	2.7 Influencer Y/N	2.8 Threat Actor Y/N
1 - Criminal Gangs	Organised Criminal Gangs who would wish to gain information from the Northern Lode system.	C	4	3	Substantial	In-House	Y	Y
		I	4	2	Moderate	In-House	Y	Y
		A	4	2	Moderate	In-House	Y	Y
2 - Political Activists	Activists who disagree with the principle of licensing.	C	2	2	Negligible	In-House	Y	Y
		I	2	2	Negligible	In-House	Y	Y
		A	3	4	Moderate	In-House	Y	Y
Notes/Rationale:								

Technical Risk Assessment

Step 3

13. The purpose of Step 3 is to define the focus of interest. That is, what collection of assets will be grouped for the purpose of any given risk assessment. The first Fol (All of Northern Lode) contains the Northern Lode asset as well as the connection object between Northern and Southern Lode. The email connection has been included as functions of the email solution may be important in protecting Northern Lode. Similarly the Fol All of Southern Load contains the Southern Lodes asset as well as the Email + Web connection object.

Form 3 – Focus of Interest					
3.1 Fol Name	3.2 Assets	3.3 Rationale	3.4 Max Impacts		
			C	I	A
All of Northern Lode	Northern Lode Lode Email	This includes the Lode Email. This is because the hardware and software in the Lode Email exchange object may play a role in protecting Northern Lode.	4	3	3
All of Southern Lode	Southern Lode Email + Web	This includes the Internet Email and Web. This is because the hardware and software in this exchange object may play a role in protecting Southern Lode.	3	3	3

Step 4

14. The purpose of Step 4 is to define and record threat actor groups and to evaluate the threat that they pose. As the threat actors are specific to the set of assets under consideration for any risk assessment, one Form 4 is required for each identified FoI. In the vase of the Northern Lode project there are two Fols, so there will be two Form 4s.
15. Each threat actor group's native capability and motivation has been assessed using Tables 4 and 5. Threat sources that may attempt to influence threat actors have been identified for each group and an assessment has been made to determine by how much the threat actors capability and motivation would be enhanced, giving a final threat level.

All of Northern Lode

16. Five threat actor groups have been identified for the FoI All of Northern Lode. These are:
 - Users of Northern Lode, compromising just the Normal Users of the system;
 - Admins of Northern Lode, compromising those, which are Privileged Users of the system;
 - All of Southern Lode. As there is an information exchange requirements between Northern and Southern Lode, Southern Lode users will be Information Exchange Partners. In this case normal users and administrators of Southern Lode have been collected together as just one threat actor group. If the Analyst had felt that they needed to separate them out they could have selected two threat actor groups (both IEPs) and conducted a separate assessment for each;
 - A threat actor group call Rest of World has been defined to include anybody who may physically intrude into location hosting elements of Northern Lode and also anybody who is indirectly connected (the Internet is indirectly connected). As the Rest of World could include anybody at all an assumption has been made that this would include the threat sources;
 - A bystanders threat actor group called Cleaners and visitors has been identified. This encompasses all SC cleared individuals who may have unescorted access to Northern Lode. The scenario states that all others will be escorted.

All of Southern Lode

17. Four threat actor groups have been identified for the FoI, All of Southern Lode. These are:

Technical Risk Assessment

- All Northern Lode users. This group includes all users of Northern Lode who are information exchange partners to Southern Lode;
- Southern Lode Users comprise the normal users of Southern Lode. Note that there are no administrators of Southern Lode defined in the scenario. This may be an area where the Accreditor would wish to see evidence as to whether there are privileged users or not based upon their analysis of this IS1 assessment;
- A group called Rest of World has been defined which would include everybody including the threat sources. This includes Information Exchange Partners as there is a business requirement to exchange information with the Internet (so those partners could include anybody). Additionally there is a stated business requirement for users to use WiFi. For this reason, the threat actor group Person Within Range has been included (as anybody may be within range of the WiFi signal outside of the office);
- A threat actor group that includes a number of bystanders has been identified. Anybody not holding BS clearances will be escorted.

Fol		All of Northern Lode				Form 4 – Threat Actors					
4.1 Threat Actor Group Name	4.2 TA Types	4.3 Clearance	Property	4.4 Native Capability	4.5 Native Motivation	4.6 Native Threat Level	4.7 Dominant Influencing Threat Source	4.8 Enhanced Capability	4.9 Enhanced Motivation	4.10 Enhanced Threat Level	4.11 Final Threat Level
Users of Northern Lode	NU	SC	C	2	2	Negligible	Criminal Gangs	2	3	Low	Low
			I	2	2	Negligible	Criminal Gangs	2	2	Negligible	Negligible
			A	2	2	Negligible	Political Activists	2	3	Low	Low
			Accidental Compromise								
Admins of Northern Lode	PU	SC	C	3	2	Low	Criminal Gangs	3	3	Moderate	Moderate
			I	3	2	Low	Criminal Gangs	3	2	Low	Low
			A	3	2	Low	Political Activists	3	3	Moderate	Moderate
			Accidental Compromise								
All Southern Lode users	IEP	BS	C	3	2	Low	Criminal Gangs	3	3	Moderate	Moderate
			I	3	2	Low	Criminal Gangs	3	2	Low	Low
			A	3	2	Low	Political Activists	3	4	Moderate	Moderate
			Accidental Compromise								
Rest of World	PI IC	UC	C	4	3	Substantial					Substantial
			I	4	2	Moderate					Moderate
			A	3	4	Moderate					Moderate
			Accidental Compromise								
Cleaners and Visitors	BY	SC	C	1	2	Negligible	Criminal Gangs	2	3	Low	Low
			I	1	2	Negligible	Criminal Gangs	2	2	Negligible	Negligible
			A	1	2	Negligible	Political Activists	2	3	Low	Low
			Accidental Compromise								

Technical Risk Assessment

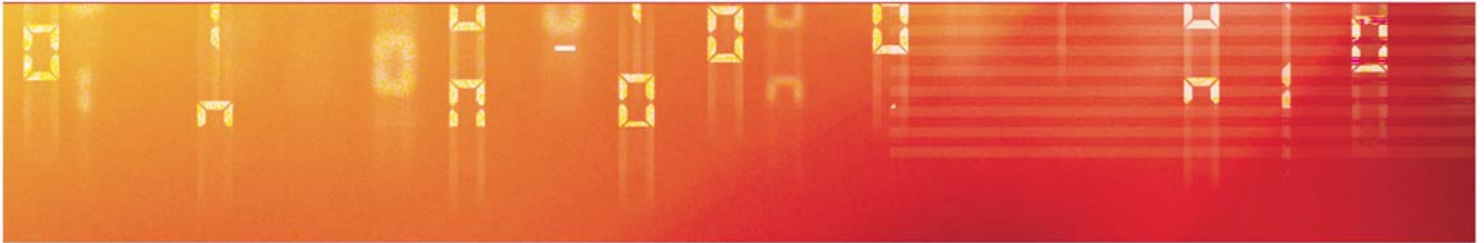
Fol		All of Southern Lode				Form 4 – Threat Actors						
4.1 Threat Actor Group Name	4.2 TA Types	4.3 Clearance	Property	4.4 Native Capability	4.5 Native Motivation	4.6 Native Threat Level	4.7 Dominant Influencing Threat Source	4.8 Enhanced Capability	4.9 Enhanced Motivation	4.10 Enhanced Threat Level	4.11 Final Threat Level	
All Northern Lode users	BY IEP	SC	C	3	2	Low					Low	
			I	3	2	Low					Low	
			A	3	2	Low						Low
			Accidental Compromise									
Southern Lode users	NU	BS	C	2	2		Criminal Gangs	2	3	Low	Low	
			I	2	2		Criminal Gangs	2	2	Negligible	Negligible	
			A	2	2		Political Activists	2	3	Low	Low	
			Accidental Compromise									
Rest of World	PI IEP PW R	UC	C	4	3	Substantial					Substantial	
			I	4	2	Moderate					Moderate	
			A	3	4	Moderate					Moderate	
			Accidental Compromise									
Visitors, cleaners, maintenance staff	BY	BS	C	1	2	Negligible	Criminal Gangs	2	3	Low	Low	
			I	1	2	Negligible	Criminal Gangs	2	2	Negligible	Negligible	
			A	1	2	Negligible	Political Activists	2	3	Low	Low	
			Accidental Compromise									

Form 5

18. A number of Form 5s are required; one for each threat actor group per FoI. For each threat actor group the Analyst has examined the available compromise methods and determined applicable ones for this scenario. The Form 5s shown do not therefore show every possible compromise method as set out in Appendix C.
19. The assessed threat level for each threat actor group, for each property of C, I and A has been assessed in Form 4. These values have been transposed into the applicable Form 5.
20. Finally the threat level is combined with the maximum business impact level to provide the risk level.

Technical Risk Assessment

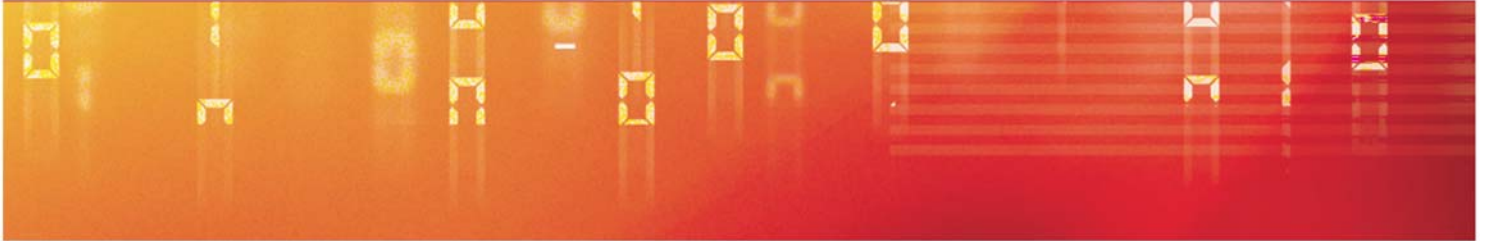
Form 5 – Risk Assessment					
	Form 5 Number	1			
	Focus of Interest	All of Northern Lode			
	Threat Actor Group	Users of Northern Lode			
	Threat Actor Types	NU			
Threat Actor Clearance		SC			
Influencing Threat Sources		Confidentiality: Criminal Gangs Availability: Political Activists			
	5.1	5.2	5.3	5.4	5.5
Property	Max BIL	Compromise Method	Threat Level	Risk Level	Risk ID
C	4	Accidentally releases information from All of Northern Lode	Moderate	Medium	1.1
		Deliberately releases information from All of Northern Lode	Low	Medium	1.2
A	3	Deliberately disrupts All of Northern Lode	Low	Low	1.3
		Changes the configuration of All of Northern Lode	Low	Low	1.4
NOTES					



Form 5 – Risk Assessment					
	Form 5 Number	2			
	Focus of Interest	All of Northern Lode			
	Threat Actor Group	Admins of Northern Lode			
	Threat Actor Types	PU			
Threat Actor Clearance		SC			
Influencing Threat Sources		Confidentiality & Integrity: Criminal Gangs Availability: Political Activists			
	5.1	5.2	5.3	5.4	5.5
Property	Max BIL	Compromise Method	Threat Level	Risk Level	Risk ID
C	4	Accidentally releases information from All of Northern Lode	Moderate	Medium	2.1
I	3	Accidentally disrupts All of Northern Lode	Moderate	Medium	2.2
A	3	Accidentally disrupts All of Northern Lode	Moderate	Medium	2.3
		Deliberately disrupts All of Northern Lode	Moderate	Medium	2.4
		Changes the configuration of All of Northern Lode	Moderate	Medium	2.5
NOTES					

Technical Risk Assessment

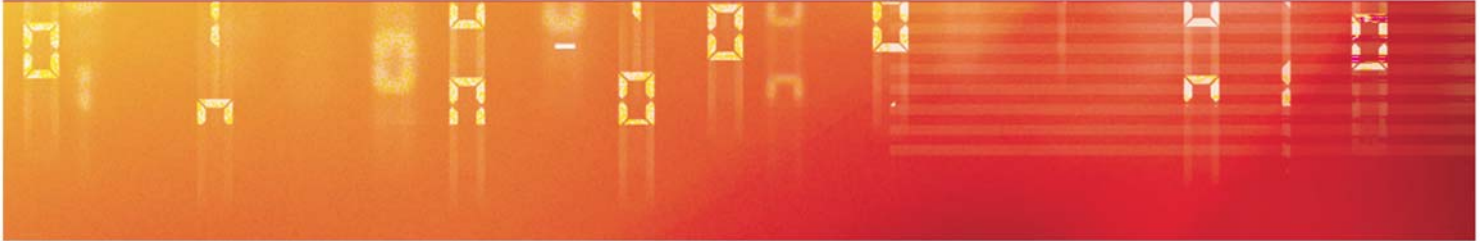
Form 5 – Risk Assessment					
		Form 5 Number	3		
		Focus of Interest	All of Northern Lode		
		Threat Actor Group	All Southern Lode Users		
		Threat Actor Types	IEP		
Threat Actor Clearance			BS		
Influencing Threat Sources			Confidentiality & Integrity: Criminal Gangs Availability: Political Activists		
	5.1	5.2	5.3	5.4	5.5
Property	Max BIL	Compromise Method	Threat Level	Risk Level	Risk ID
C	4	Misuses business or Network connections to or from All of Northern Lode	Moderate	Medium	3.1
I	3	Misuses business or Network connections to or from All of Northern Lode	Low	Low	3.2
A	3	Misuses business or Network connections to or from All of Northern Lode	Moderate	Medium	3.3
NOTES					



Form 5 – Risk Assessment					
	Form 5 Number	4			
	Focus of Interest	All of Northern Lode			
	Threat Actor Group	Rest of World			
	Threat Actor Types	PI, IC			
Threat Actor Clearance			UC		
Influencing Threat Sources					
	5.1	5.2	5.3	5.4	5.5
Property	Max BIL	Compromise Method	Threat Level	Risk Level	Risk ID
C	4	Tampers with equipment in All of Northern Lode	Substantial	Medium -High	4.1
		Misuses business or Network connections to or from All of Northern Lode	Substantial	Medium -High	4.4
I	3	Tampers with equipment in All of Northern Lode	Moderate	Medium	4.2
		Misuses business or Network connections to or from All of Northern Lode	Moderate	Medium	4.5
A	3	Tampers with equipment in All of Northern Lode	Moderate	Medium	4.3
		Misuses business or Network connections to or from All of Northern Lode	Moderate	Medium	4.6
NOTES					

Technical Risk Assessment

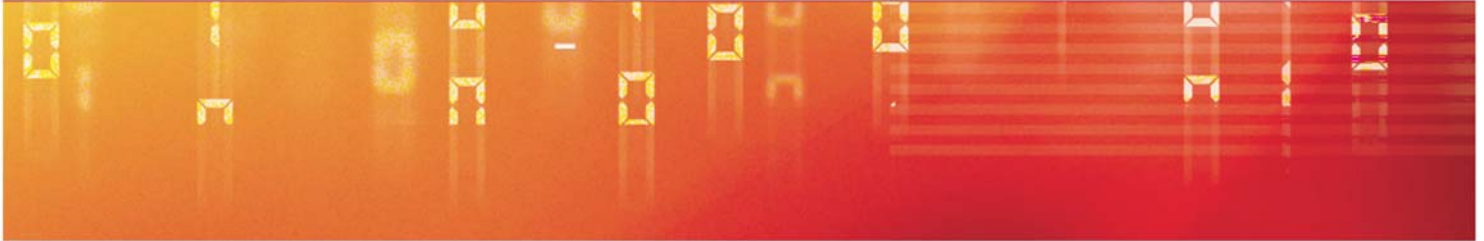
Form 5 – Risk Assessment					
	Form 5 Number	5			
	Focus of Interest	All of Northern Lode			
	Threat Actor Group	Cleaners and Visitors			
	Threat Actor Types	BY			
Threat Actor Clearance		SC			
Influencing Threat Sources		Confidentiality: Criminal Gangs Availability: Political Activists			
	5.1	5.2	5.3	5.4	5.5
Property	Max BIL	Compromise Method	Threat Level	Risk Level	Risk ID
C	4	Observes information from All of Northern Lode	Low	Medium	5.1
		Impersonates a user of All of Northern Lode	Low	Medium	5.2
A	3	Tampers with equipment in All of Northern Lode	Low	Low	5.3
NOTES					



Form 5 – Risk Assessment					
	Form 5 Number	6			
	Focus of Interest	All of Southern Lode			
	Threat Actor Group	All Northern Lode Users			
	Threat Actor Types	BY, IEP			
Threat Actor Clearance		SC			
Influencing Threat Sources					
	5.1	5.2	5.3	5.4	5.5
Property	Max BIL	Compromise Method	Threat Level	Risk Level	Risk ID
I	3	Impersonates a user of All of Southern Lode	Low	Low	6.1
		Misuses business or Network connections to or from All of Southern Lode	Low	Low	6.2
A	3	Misuses business or Network connections to or from All of Southern Lode	Low	Low	6.3
NOTES					

Technical Risk Assessment

Form 5 – Risk Assessment					
	Form 5 Number	7			
	Focus of Interest	All of Southern Lode			
	Threat Actor Group	Southern Lode Users			
	Threat Actor Types	NU			
Threat Actor Clearance		BS			
Influencing Threat Sources		Confidentiality: Criminal Gangs Availability: Political Activists			
	5.1	5.2	5.3	5.4	5.5
Property	Max BIL	Compromise Method	Threat Level	Risk Level	Risk ID
C	3	Accidentally releases information from All of Southern Lode	Moderate	Medium	7.1
		Deliberately releases information from All of Southern Lode	Low	Low	7.3
A	3	Accidentally disrupts All of Southern Lode	Moderate	Medium	7.2
		Changes the configuration of All of Southern Lode	Low	Low	7.4
NOTES					



Form 5 – Risk Assessment					
	Form 5 Number	8			
	Focus of Interest	All of Southern Lode			
	Threat Actor Group	Rest of World			
	Threat Actor Types	PI, IEP, PWR			
Threat Actor Clearance			UC		
Influencing Threat Sources					
	5.1	5.2	5.3	5.4	5.5
Property	Max BIL	Compromise Method	Threat Level	Risk Level	Risk ID
C	3	Tampers with equipment in All of Southern Lode	Substantial	Medium	8.1
		Misuses business or Network connections to or from All of Southern Lode	Substantial	Medium	8.2
		Intercepts traffic from or to All of Southern Lode	Substantial	Medium	8.4
A	3	Misuses business or Network connections to or from All of Southern Lode	Moderate	Medium	8.3
		Jams All of Southern Lode	Moderate	Medium	8.5
NOTES					

Technical Risk Assessment

Form 5 – Risk Assessment					
		Form 5 Number	9		
		Focus of Interest	All of Southern Lode		
		Threat Actor Group	Visitors, Cleaners, Maintenance Staff		
		Threat Actor Types	BY		
Threat Actor Clearance			BS		
Influencing Threat Sources			Confidentiality & Integrity: Criminal Gangs Availability: Political Activists		
	5.1	5.2	5.3	5.4	5.5
Property	Max BIL	Compromise Method	Threat Level	Risk Level	Risk ID
C	3	Observes information from All of Southern Lode	Low	Low	9.1
		Impersonates a user of All of Southern Lode	Low	Low	9.2
I	3	Impersonates a user of All of Southern Lode	Negligible	Very Low	9.3
A	3	Impersonates a user of All of Southern Lode	Low	Low	9.4
		Tampers with equipment in All of Southern Lode	Low	Low	9.5
NOTES					

Step 6

21. The final step is to simply take the risks generated in the collection of Form 5s and present them. Form 6 shows each risk identified and has been ordered to show the highest risk levels first. The description is produced so that it is a meaningful statement for a non-specialist to be able to understand.

Form 6 – Prioritised Risk List		
6.1 Risk ID	6.2 Description	6.3 Risk Level
4.4	Rest of World, as an Indirectly Connected threat actor, misuses business or network connections to or from All of Northern Lode, compromising its confidentiality and having a potential Business Impact of BIL 4.	Medium-High
4.1	Rest of World, as a Physical Intruder, tampers with equipment in All of Northern Lode, compromising its confidentiality and having a potential Business Impact of BIL 4.	Medium-High
5.1	Cleaners and Visitors (influenced by Criminal Gangs), as Bystanders, observe information from All of Northern Lode, compromising its confidentiality and having a potential Business Impact of BIL 4.	Medium
5.2	Cleaners and Visitors (influenced by Criminal Gangs), as Bystanders, impersonate a user of All of Northern Lode, compromising its confidentiality and having a potential Business Impact of BIL 4.	Medium
2.1	Admins of Northern Lode, as a Privileged User, accidentally releases information from All of Northern Lode, compromising its confidentiality and having a potential Business Impact of BIL 4.	Medium
3.1	All Southern Lode users (influenced by Criminal Gangs), as Information Exchange Partners, misuses business or network connections to or from All of Northern Lode, compromising its confidentiality and having a potential Business Impact of BIL 4.	Medium
1.2	Users of Northern Lode (influenced by Criminal Gangs), as Normal Users, deliberately release information from All of Northern Lode, compromising its confidentiality and having a potential Business Impact of BIL 4.	Medium

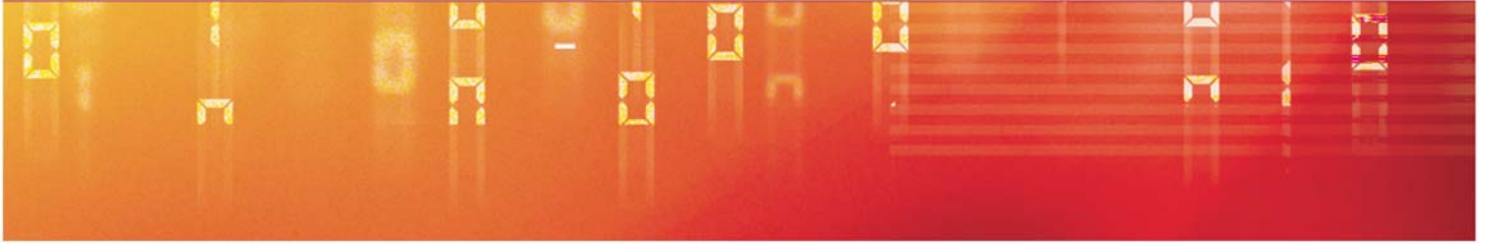
Technical Risk Assessment

1.1	Users of Northern Lode, as Normal Users, accidentally releases information from All of Northern Lode, compromising its confidentiality and having a potential Business Impact of BIL 4.	Medium
4.5	Rest of World, as Indirectly Connected, misuse business or network connections to or from All of Northern Lode, compromising its integrity and having a potential Business Impact of BIL 3.	Medium
2.3	Admins of Northern Lode, as Privileged Users, accidentally disrupt All of Northern Lode, compromising its availability and having a potential Business Impact of BIL 3.	Medium
8.4	Rest of World, as a Person Within Range, intercepts traffic from or to All of Southern Lode, compromising its confidentiality and having a potential Business Impact of BIL 3.	Medium
8.5	Rest of World, as a Person Within Range, jams All of Southern Lode, compromising its availability and having a potential Business Impact of BIL 3.	Medium
4.6	Rest of World, as Indirectly Connected, misuses business or network connections to or from All of Northern Lode, compromising its availability and having a potential Business Impact of BIL 3.	Medium
3.3	All Southern Lode users (influenced by Political Activists), as Information Exchange Partners, misuse business or network connections to or from All of Northern Lode, compromising its availability and having a potential Business Impact of BIL 3.	Medium
2.5	Admins of Northern Lode (influenced by Political Activists), as Privileged Users, change the configuration of All of Northern Lode, compromising its availability and having a potential Business Impact of BIL 3.	Medium
2.4	Admins of Northern Lode (influenced by Political Activists), as Privileged Users, deliberately disrupt All of Northern Lode, compromising its availability and having a potential Business Impact of BIL 3.	Medium
4.3	Rest of World, as Physical Intruders, tamper with equipment in All of Northern Lode, compromising its availability and having a potential Business Impact of BIL 3.	Medium
4.2	Rest of World, as Physical Intruders, tamper with equipment in All of Northern Lode, compromising its integrity and having a potential Business Impact at BIL 3.	Medium

8.1	Rest of World, as Physical Intruders, tamper with equipment in All of Southern Lode, compromising its confidentiality and having a potential Business Impact of BIL 3.	Medium
7.2	Southern Lode users, as Normal Users, Accidentally disrupt All of Southern Lode, compromising its availability and having a potential Business Impact of BIL 3.	Medium
8.3	Rest of World, as Information Exchange Partners, misuse business or network connections to or from All of Southern Lode, compromising its availability and having a potential Business Impact of BIL 3.	Medium
8.2	Rest of World, as Information Exchange Partners, misuse business or network connections to or from All of Southern Lode, compromising its confidentiality and having a potential Business Impact of BIL 3.	Medium
7.1	Southern Lode users, as Normal Users, accidentally release information from All of Southern Lode, compromising its confidentiality and having a potential Business Impact of BIL 3.	Medium
2.2	Admins of Northern Lode, as Privileged Users, accidentally disrupt All of Northern Lode, compromising its integrity and having a potential Business Impact of BIL 3.	Medium
9.4	Visitors, cleaners, maintenance staff (influenced by Political Activists), as Bystanders, impersonate a user of All of Southern Lode, compromising its availability and having a potential Business Impact of BIL 3.	Low
1.4	Users of Northern Lode (influenced by Political Activists), as Normal Users, change the configuration of All of Northern Lode, compromising its availability and having a potential Business Impact of BIL 3.	Low
9.5	Visitors, cleaners, maintenance staff (influenced by Political Activists), as Bystanders, tamper with equipment in All of Southern Lode, compromising its availability and having a potential Business Impact of BIL 3.	Low
1.3	Users of Northern Lode (influenced by Political Activists), as Normal Users, deliberately disrupt All of Northern Lode, compromising its availability and having a potential Business Impact of BIL 3.	Low
6.2	All Northern Lode users, as Information Exchange Partners, misuses business or network connections to or from All of Southern Lode, compromising its integrity and having a potential Business Impact of BIL 3.	Low

Technical Risk Assessment

6.1	All Northern Lode users, as Bystanders, impersonate a user of All of Southern Lode, compromising its integrity and having a potential Business Impact of BIL 3.	Low
7.3	Southern Lode users (influenced by Criminal Gangs), as Normal Users, deliberately release information from All of Southern Lode, compromising its confidentiality and having a potential Business Impact of BIL 3.	Low
6.3	All Northern Lode users, as Information Exchange Partners, misuse business or network connections to or from All of Southern Lode, compromising its availability and having a potential Business Impact of BIL 3.	Low
5.3	Cleaners and Visitors (influenced by Political Activists), as Bystanders, tamper with equipment in All of Northern Lode, compromising its availability and having a potential Business Impact of BIL 3.	Low
3.2	All Southern Lode users (influenced by Criminal Gangs), as Information Exchange Partners, misuse business or network connections to or from All of Northern Lode, compromising its integrity and having a potential Business Impact of BIL 3.	Low
7.4	Southern Lode users (influenced by Political Activists), as Normal Users, changes the configuration of All of Southern Lode, compromising its availability and having a potential Business Impact of BIL 3.	Low
9.1	Visitors, cleaners, maintenance staff (influenced by Criminal Gangs), as Bystanders, observe information from All of Southern Lode, compromising its confidentiality and having a potential Business Impact of BIL 3.	Low
9.2	Visitors, cleaners, maintenance staff (influenced by Criminal Gangs), as Bystanders, impersonate a user of All of Southern Lode, compromising its confidentiality and having a potential Business Impact of BIL 3.	Low
9.3	Visitors, cleaners, maintenance staff (influenced by Criminal Gangs), as Bystanders, impersonate a user of All of Southern Lode, compromising its integrity and having a potential Business Impact of BIL 3.	Very Low



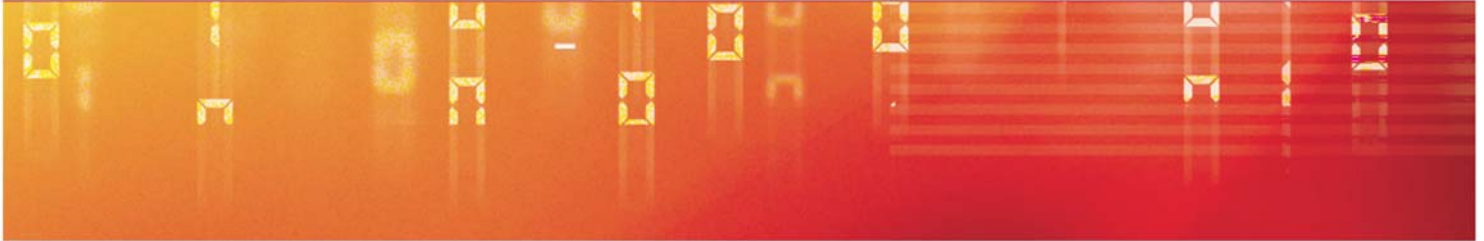
THIS PAGE IS INTENTIONALLY LEFT BLANK

Technical Risk Assessment

Appendix E: Blank Forms

1. This appendix provides each of the forms used within the IS1 method.

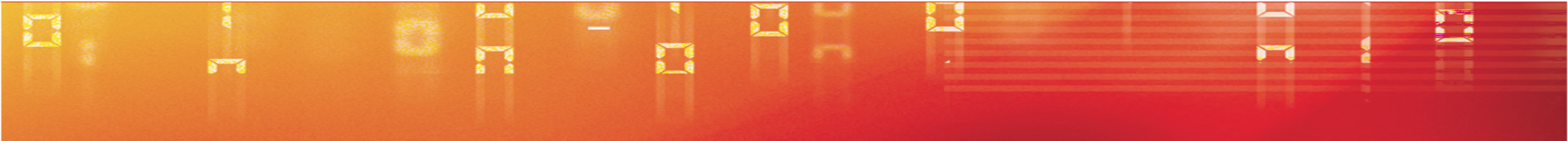
Form 1 – Asset List				
1.1 Asset Identifier	1.2 Description/Notes	1.3 Impact Levels		
		C	I	A



Form 2 – Threat Sources								
			2.3	2.4	2.5	2.6	2.7	2.8
2.1 Source Name	2.2 Description (and Rationale)	Property	Capability (Table 1)	Priority (Table 2)	Threat Level (Table 3)	Source of Threat Assessment	Influencer Y/N	Threat Actor Y/N
Provide a sensible name for the source	Describe the threat source and provide rationale why they are relevant.	C						
		I						
		A						
		C						
		I						
		A						
		C						
		I						
		A						
Notes/Rationale:								

Technical Risk Assessment

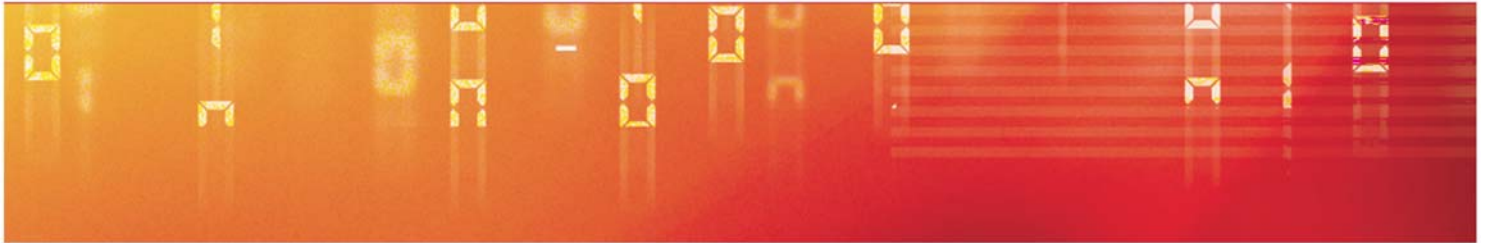
Form 3 – Focus of Interest					
3.1 Fol Name	3.2 Assets	3.3 Rationale	3.4 Max Impacts		
			C	I	A
Create a name for the Focus of Interest	List all assets that fall within that Fol (your model should help)	Why have you chosen this collection of assets as an Fol?			



Fol		There will be one Form 4 for each Fol. Identify the Fol here.				Form 4 – Threat Actors					
4.1 Threat Actor Group Name	4.2 TA Types	4.3 Clearance	Property	4.4 Native Capability	4.5 Native Motivation	4.6 Native Threat Level	4.7 Dominant Influencing Threat Source	4.8 Enhanced Capability	4.9 Enhanced Motivation	4.10 Enhanced Threat Level	4.11 Final Threat Level
			C	Refer to Table 4	Refer to Table 5	Refer to Table 6	Record if any	Refer to Form 2 and Table 4	Refer to Form 2 and Table 5	Refer to Table 6	Either of 4.6 or 4.10
			I								
			A								
			Accidental Compromise								Refer to Table 7
			C								
			I								
			A								
			Accidental Compromise								
			C								
			I								
			A								
			Accidental Compromise								

Technical Risk Assessment

Form 5 – Risk Assessment					
	Form 5 Number	There will be a number of Form 5s so it is helpful to number them			
	Focus of Interest	Record the applicable FoI			
	Threat Actor Group	There will be one Form 5 for each identified threat actor group for each FoI.			
	Threat Actor Types				
Threat Actor Clearance			Taken from Form 4		
Influencing Threat Sources			Taken from Form 4		
	5.1	5.2	5.3	5.4	5.5
Property	Max BIL	Compromise Method	Threat Level	Risk Level	Risk ID
C		Record each relevant compromise method	Form 4	Table 8	
I					
A					
NOTES					



Form 6 – Prioritised Risk List		
6.1 Risk ID	6.2 Description	6.3 Risk Level
Form 5	Each Risk should be described in normal language	Form 5

Technical Risk Assessment

References

- [a] HMG IA Standard No. 2, The Risk Management and Accreditation of ICT Systems & Services, Issue 3.1, October 2008 (Not Protectively Marked).
- [b] HMG Security Policy Framework, 2009. Tiers 1-3 (Not Protectively Marked) available at: <http://www.cabinetoffice.gov.uk>
- [c] A National Information Assurance Strategy, June 2007. Available at: <http://www.cabinetoffice.gov.uk>
- [d] ISO/IEC 27001:2005, *Information Security Management Systems*. Further information on International and British Standards is available from the British Standards Institute (BSI)
- [e] Security: e-Government Strategy Framework. Policy and Guidelines v4.0, September 2002. Available at <http://www.cabinetoffice.gov.uk>
- [f] CESG Good Practice Guide No. 9, Taking Account of the Aggregation of Information, Issue 1.2, March 2009 (Not Protectively Marked).

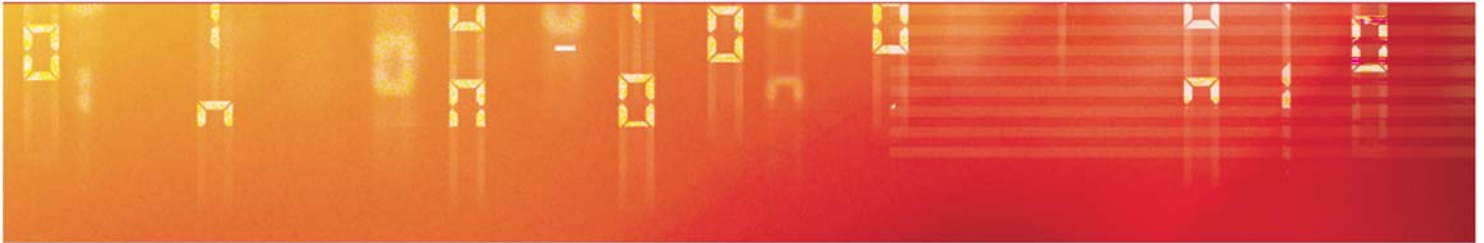
Glossary

Accreditation	Accreditation is the formal assessment of the ICT system against its IA requirements, resulting in the acceptance of residual risks in the context of the business requirement. It is a prerequisite to approval to operate.
Accreditation Scope	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.
Aggregation	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.
Analysis Scope	The analysis scope includes everything that is part of the risk assessment. This includes everything that is part of the project and reliance scope as well as considering business information exchange requirements and system connections.
Analyst	The Analyst is the person(s) who are considered to be conducting the risk assessment and risk treatment activities; the person following the method.
Asset	Anything that has value to the organisation, its business operations and its continuity.
Assurance	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 (extrinsic assurance).
Availability	The property of being accessible and usable upon demand by an authorised entity.
Baseline Control Set	The Baseline Control Set contains a single set of protective controls that should be considered as the HMG baseline to manage information risk.
Business Impact	The result of an information security incident on business functions and the effect that a business interruption may have

Technical Risk Assessment

upon them.

Capability	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.
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals, entities, or processes
Control Objectives	A Control Objective describes functionally the purpose of a control but may not define how that control will be achieved or implemented.
Compromise Method	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.
Critical National Infrastructure (CNI)	The CNI is those infrastructure assets that are vital to the continued delivery and integrity of the essential services upon which the UK relies.
Focus of Interest (Fol)	A focus of interest 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.
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
Motivation	Motivation is a measure of how much a threat actor desires to attack and compromise an asset or group of assets.
PIA	Privacy Impact Assessment
Priority	Priority is a measure of how much a threat sources desires a compromise of an asset or group of assets.

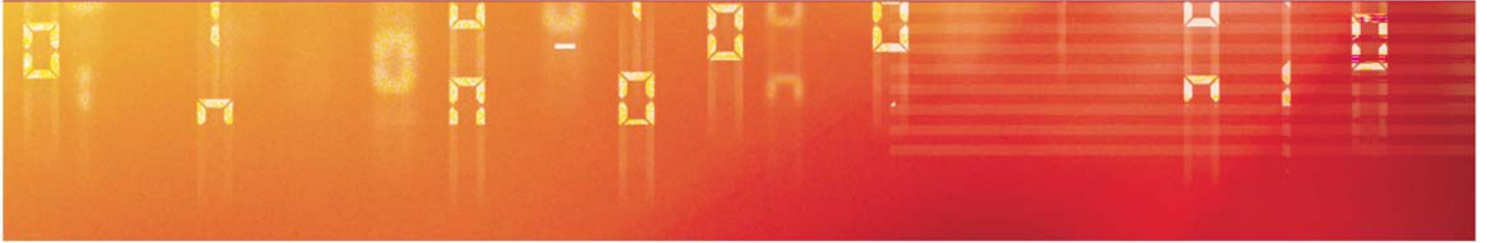


Reliance Scope	The reliance scope identifies capability and services that the Accreditation Scope relies upon, but is not directly supplied by the project. A trusted risk assessment and accreditation of these components is required in order to rely upon them without further analysis.
Risk	The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation.
Risk Appetite	Risk appetite is logically a function of the organisation's capacity to bear risk, which should not be exceeded."
Risk Assessment	The overall process of risk analysis and risk evaluation
Risk Level	Risk level is a combination of threat level and business impact level. The elements of likelihood and vulnerability cannot be assessed in a generic sense and in the early stages of a risk assessment may not be known. A risk level is therefore an indicative assessment of risk.
Risk Management	Process of coordinating activities to direct and control an organisation with regard to risk
Risk Management & Accreditation Document Set (RMADS)	The documentation, often a portfolio, which specifies the risk management measures, accreditation policy, and status of an ICT system.
Risk Tolerance	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 accept for a particular project or programme.
Risk Treatment	The process of selection and implementation of measures to modify risk (reduce, avoid, transfer or accept).
Risk Treatment Plan	The plan should contain detail on the risks that have to be reduced. It provides details on the countermeasures that are being applied and the ownership of them. It will also record the implementation status of each countermeasure.
Security Case	The security case describes how all of the identified risks have been satisfactorily treated. It includes the list of risks a

Technical Risk Assessment

description of application of all controls, the Assurance Plan and any functional or assurance gaps that may be present.

Segmentation Model	The Segmentation model provides a framework that ensures that controls are both appropriate and proportionate to manage the risks to an ICT system. The Segmentation Model has four Segments, which provide a description of the types and capabilities of threat that are considered at each level.
Senior Information Risk Owner (SIRO)	Member of senior management board with responsibility for IA governance and risk ownership in the organisation on behalf of the board.
Snapshot Risk Assessment	A snapshot risk assessment follows the IS1 method, however it recognises the limitations of understanding of risk components at the early stage of a project. This risk assessment is therefore intended to inform the organisation of the types and magnitudes of risk that will require management in order to help make a decision about whether to proceed.
Threat	A potential cause of an incident that may result in harm to a system or organisation.
Threat Actor	A threat actor is a person who actually performs an attack or, in the case of accidents, will cause the accident.
Threat Actor Group	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.
Threat Actor Type	Each threat actor belongs to one or more threat actor types according to the degree and type of access to an asset.
Threat Level	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.



Threat Source

A threat source is a person or organisation that desires to breach security and ultimately will benefit from a compromise in some way.

Vulnerability

A weakness of an asset or group of assets that can be exploited by one or more threats.

Technical Risk Assessment

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
A2j
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

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

PLEASE PRINT

Your Name:

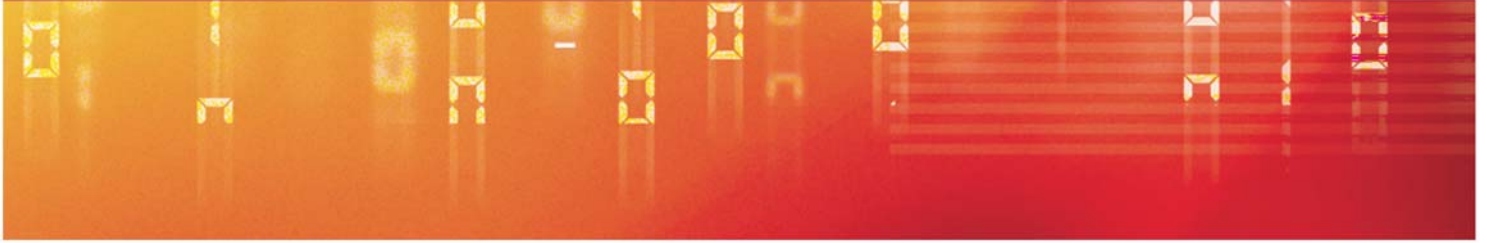
Department/Company Name and Address:

Phone number:

Email address:

Comments:

UNCLASSIFIED



UNCLASSIFIED

UNCLASSIFIED

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.

UNCLASSIFIED

UNCLASSIFIED

IA
CESG
B2h
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX

Tel: +44 (0)1242 709141
Fax: +44 (0)1242 709193
Email: enquiries@cesg.gsi.gov.uk

© Crown Copyright 2009. Communications on CESG telecommunications systems may be monitored or recorded to secure the effective operation of the system and for other lawful purposes.

UNCLASSIFIED