



Tailored Assurance Service

Methodology

Version 2.1

June 2007

This document and its content shall only be used for the purpose for which it was issued. The copyright of this document is reserved and vested in the Crown

© Crown Copyright 2007 - All Rights Reserved

CESG

FOREWORD

This document is issued by CESG, the UK National Technical Authority for Information Assurance.

It is intended for use by HMG and other public sector organisations, together with their contractors and suppliers.

For additional copies of this document please contact:

CESG (Documentation Manager)
A2j
Hubble Road
Cheltenham
GL51 0EX
United Kingdom

Fax: (01242) 709193

Email: enquiries@cesg.gsi.gov.uk

For general queries concerning this document please contact:

CESG Customer Support Office at the above address.

Tel: 01242 709141

Fax: 01242 709193

Email: enquiries@cesg.gsi.gov.uk

Readers are encouraged to inform CESG of their experiences, good or bad, in using this document. We would especially like to know about any inconsistencies and ambiguities. Please use the feedback form at the end of this document for any comments.

Amendment History:

Version	Date	Description
2.1	1 June 2007	Version 2.0 as used in Contract negotiations but Appendix G transferred to Operating Procedures for Evaluation Companies

CONTENTS

Foreword	ii
Contents	iii
Glossary	v
I. INTRODUCTION.....	1
II. PRODUCT ASSURANCE ACTIVITIES	3
A. Functionality and Design Assessment	3
B. Development Procedures Review.....	4
C. Security Function Testing	5
D. Source Code Analysis	6
E. Vulnerability Analysis and Testing	7
F. Product Assurance Maintenance Review	8
III. SYSTEM ASSURANCE ACTIVITIES	11
A. System Architecture and Design Review	11
B. System Security Testing	12
C. Installation and Operational Procedures Review	13
D. System Assurance Maintenance Review.....	14
APPENDIX A : SECURITY TARGET TEMPLATE	A1
APPENDIX B: EVALUATION WORK PROGRAMME TEMPLATE.....	B1
APPENDIX C: EVALUATION REPORT TEMPLATE	C1
APPENDIX D: ASSURANCE MAINTENANCE PLAN TEMPLATE	D1
APPENDIX E: MAINTENANCE REPORT TEMPLATE	E1
APPENDIX F: ASSURANCE MAINTENANCE GUIDANCE.....	F1

GLOSSARY

Accreditor	The person responsible for advising the Customer that the security arrangements for their IT system/product are satisfactory and that the IT system/product may be used. The use of the term Accreditor in this document takes on the meaning of Joint Accreditation Panel where circumstances require such a Panel
AMP	Assurance Maintenance Plan
CESG	Means the National Technical Authority for IA which has the responsibility for providing guidance to Evaluation Companies and auditing their work under TAS and assuring the Accreditor that the work has been carried out to the required standard.
CNI	Critical National Infrastructure
COR	Critical Observation Report that may result in change to EWP
Customer	The HMG Department or other CNI organisation requiring the IT system
Developer	The company supplying the IT system/product required by the Customer
Evaluator	Means a person employed by an Evaluation Company to carry out Tailored Assurance Service evaluations
EWP	Evaluation Work Programme
Information	means any data, text, figures, specifications, drawings or otherwise – in any format, by either the AUTHORITY or the SUPPLIER – that provide the detail required to carry out a Task that is the subject of such Information.
IA	Information Assurance
IACS	Information Assurance and Consultancy Services
SIA	Security Impact Analysis
Sponsor	The organisation paying the Evaluation Company – this might be the HMG Department or other CNI organization or their Managed Service Provider or the Developer providing the IT system – it will depend on the precise contract arrangements between those organisations
ST	Security Target
Sub-Contractor	Means a company or companies or an individual not under the employ of the Supplier engaged by the Supplier to provide Services, Deliverables, or Supplier Personnel in accordance with the terms of this Agreement.

I. INTRODUCTION

1. This document gives a description of the assurance activities for the Tailored Assurance Service and provides a number of templates for activities associated with it. Before any of the assurance activities can start a Security Target (ST) and an associated Evaluation Work Programme (EWP) must be agreed for the IT product or system that is to be evaluated. The way they are produced and the Tailored Assurance Service operates can be found in the Tailored Assurance Service Operating Procedures document.

2. The main objective of this document is to help Evaluators ensure that IT product and system evaluations can be performed consistently to the required standard. However, it is not possible or desirable to specify every action that should be taken and there will always be a reliance on the skills, experience and motivation of the Evaluator. Therefore a deliberate decision was taken not to attempt to define the methodology too precisely.

3. The remainder of the document concentrates on the assurance activities for a successful evaluation and describes the work of the Evaluator. The structure of this document is as follows:

- Section 2: Product Evaluation Assurance Activities
- Section 3: System Evaluation Assurance Activities
- Appendix A: Security Target Template
- Appendix B: Evaluation Work Programme Template
- Appendix C: Evaluation Report Template
- Appendix D: Assurance Maintenance Plan Template
- Appendix E: Maintenance Report Template
- Appendix F: Assurance Maintenance Guidance
- Appendix G: Evaluation Company Progress Reports and Meetings

THIS PAGE IS INTENTIONALLY LEFT BLANK

II. PRODUCT ASSURANCE ACTIVITIES

A. Functionality and Design Assessment

Objectives

4. Draw conclusions on whether sufficient design information is available to understand the product in terms of components, interfaces, security functionality and dependencies.
5. Determine to what extent the design is appropriate for the intended use.
6. Understand the product in more depth for the purpose of planning effective testing of its security.

Guidelines

7. The Evaluator shall review the product functional specification and check that it meets the agreed security requirements.
8. The Evaluator shall determine whether there is any additional functionality within the product (that cannot be disabled), which could potentially be used to bypass security.
9. The Evaluator is advised that the product design should be reviewed for the following as a minimum:
 - Whether it contains sufficient security functionality information to identify all the security related components, interfaces and their dependencies (e.g. on other products or modules that are out of scope of the evaluation).
 - Consistency with the security requirements.
 - Presence (and effectiveness) of any strength-in-depth or self-protection.
 - The extent to which complexity will make vulnerabilities harder to find during the evaluation.
 - Whether it contains any obvious weak points or potential vulnerabilities e.g. potential for bypassing or deactivating components.
 - Whether aspects of the product security design could be improved based on experience of industry best practice.

Reporting in the Evaluation Report

10. Functionality and design information should be referenced or explanations given where understanding was gained by other means e.g. by discussion with the Developer.

11. A brief description of how the security functionality maps to the design should be included in an Annex to the Evaluation Report.

12. The general conclusions of each of the activities above should be summarised.

B. Development Procedures Review

Objectives:

13. Formulate a comprehensive assessment of the effectiveness of tools and procedures used during development to control security vulnerabilities.

Guidelines:

14. The approach taken by the Evaluator should have been agreed in the EWP beforehand with the Accreditor and will depend on the reliance being placed on this activity. For example it could include a Developer site visit and an audit of compliance to procedures. Alternatively, it could be by sampling of documented procedures provided by the Developer.

15. The Evaluator shall identify any tools, standards and procedures that were used for design, implementation, configuration management and testing (by the Developer).

16. The Evaluator shall determine to what extent the security functionality and vulnerable interfaces have been tested by the Developer and whether tools, procedures or software coding standards have been used to avoid common types of vulnerability.

17. If the product has already been widely used, then the number of vulnerabilities reported in recent versions can provide evidence of the effectiveness of these measures.

Reporting in the Evaluation Report

18. The Evaluation Report should briefly summarise the procedures and tools used by the Developer and comment on their overall effectiveness. The lengths to which the Evaluator audited these procedures and tools should also be summarised (unless stated in the EWP). This information will be used in building up a general picture of system or product security, which may assist further risk-based decisions. The information may also help to refine the prioritisation given to the subsequent assurance activities.

C. Security Function Testing

Objectives

19. Confirm that there are no publicly known or generic vulnerabilities in the product.
20. Test the claimed security functionality.

Guidelines

21. A thorough search for publicly known vulnerabilities¹ should be carried out. The Developer should also be asked if there are any outstanding vulnerabilities that have been reported but not yet fixed.
22. The security functionality claimed in the Security Target should be tested. This can be by a combination of independent repetition (or witnessing) of Developer tests together with new tests created by the Evaluator as required. The tests should be spread across the relevant security functionality, components and interfaces and the approach should be agreed with CESG.
23. If testing reveals problems in configuration, installation or operation or that the guidance is unclear (and these issues could result in potential vulnerabilities), then this should be reported without delay by the Evaluator to the Accreditor, Developer and CESG using an Observation Report.
24. In addition to purely security functionality tests (and if further Vulnerability Analysis and Testing (see section A.5) is excluded), the Evaluator should attempt to carry out penetration tests based on ideas developed from their understanding of the design and from knowledge of any vulnerabilities in similar types of product or system.

Reporting in the Evaluation Report

25. The extent of the public search for vulnerabilities should be described. The scope of the evaluation testing together with the results of testing should be summarised with key recommendations. Details of testing should be appended to the Evaluation Report (but where these are lengthy they can be kept as separate test records by the Evaluator and referenced in the report).
26. The configuration settings must be stated and justified. If the configuration was tied down in a specific way for the evaluation, any assumptions made during testing must be stated. Customers need to understand the limits of how they can reconfigure the product or system without potentially introducing vulnerabilities.

¹ The Evaluator should document which web sites were used to identify the publicly known vulnerabilities.

27. Test records (including plans, scripts and results) must be sufficiently detailed such that identical tests could be repeated if necessary e.g. under subsequent maintenance. These records need to be made available to CESG.

D. Source Code Analysis

Objectives

28. Determine whether potential vulnerabilities can be detected in the 'implementation' (the source code is the usual representation of the implementation to be examined).

29. Draw conclusions on the resilience of the implementation.

30. Develop ideas for advanced testing.

Guidelines

31. This activity is dependent on the Developer permitting access to source code.

32. Where applicable, automated commercial tools should be used to scan the code for common flaws and any potential problems that could result in potential vulnerabilities should be investigated manually.

33. Critical parts of the code should be identified and analysed manually e.g. the implementation of externally facing interfaces or key functionality claimed in the Security Target (such as authentication etc).

34. Any vulnerabilities, errors or inconsistencies with the design should be noted. The Evaluator should also note whether good software coding standards have been followed especially in terms of avoiding potential vulnerabilities (e.g. well known types of attack, undocumented commands and test functions).

Reporting in the Evaluation Report

35. The nature and scale of 'the implementation' should be briefly described.

36. Tools used to analyse the software should be referenced in the EWP and the conclusions summarised. Any source code analysis tools not listed in the EWP should be recorded. The purpose of all tools should be summarised.

37. A summary of the sampling approach for manual analysis should be referenced in the EWP or given, with details of which specific components and modules were analysed. Conclusions based on the guidelines above should be summarised.

E. Vulnerability Analysis and Testing

Objectives

38. Determine whether any vulnerabilities can be detected in the product by testing.

Guidelines

39. The vulnerability analysis should be based on a knowledge of the design of the product and access to source code rather than being a completely separate activity. This should allow for more efficient working, with the alternative 'black-box' approach potentially taking longer to give the same level of assurance. A strategy for the vulnerability analysis should be created in consultation with CESG and documented in the EWP.

40. Evaluators should apply tools and techniques for detecting vulnerabilities by testing. Examples of the types of attacks that should be attempted are included in the Common Criteria evaluation methodology [CEM] for EAL4, which includes a wide range of suggestions under the headings of 'bypassing', 'tampering' and 'direct attacks'. These include suggestions such as 'causing command input buffers to overflow possibly smashing the stack', along with many others.

41. The capability of the attacker should not be assumed to be 'low' but should take into account the threats that the product is intended to protect against in its intended system environment.

42. Where the evaluation activity so demands the Evaluation Company shall need to be able to develop test software or scripts, for example for overcoming bound checking or state maintenance in client side code.

Reporting in the Evaluation Report

43. The strategy for the vulnerability analysis should be summarised and the results of testing should be reported. Details of testing (including tools and techniques) should be appended to the report but where these are lengthy they can be kept as separate test records by the Evaluator and referenced in the report.

44. If the configuration was tied down in a specific way for the evaluation, any assumptions made during testing must be stated. Customers need to understand the limits of how they can reconfigure the product without potentially introducing vulnerabilities. Key recommendations should be summarised. Any assumptions about the 'attack potential' of the threat must also be clearly stated.

45. Test records must be sufficiently detailed such that identical tests could be repeated if necessary. These records need to be made available to CESG.

F. Product Assurance Maintenance Review

Objectives:

46. The objective of this activity is to provide continual assurance maintenance of the product during its operational lifecycle.

Guidelines:

47. On completion of an evaluation the Evaluation Company is responsible for recommending whether or not a product should enter a Maintenance Phase. The reasons for entering or not entering the Maintenance Phase shall be recorded in the Evaluation Report. Where a maintenance plan is drawn up then the Evaluation Company should use the Assurance Maintenance Plan (AMP) template and discuss its contents with the Accreditor, Developer and CESG.

48. The AMP will address how product updates will be assessed, for example giving guidance on categorising likely changes into security impact categories and how the various categories will be tested. If known, a roadmap for product development can also be included.

49. This activity will normally include Maintenance Reviews as follows:

- Periodically - to audit the changes implemented within the period (e.g. annually)
- as driven by events - to review proposed major changes & proposed assurance strategy

50. The periodic review will normally include:

- a check for any new vulnerabilities identified since the previous evaluation or review
- a review of the patching history and its consequences
- a review of the changes to the product detailed in the Security Impact Analysis
- an audit of sample changes to check adherence to procedures
- a review of the associated Developer tests (which should include regressions tests)
- a test of specific updated security functions, if the Developer tests are inadequate

Methodology

- an audit of the application of the operational procedures if appropriate (as required by the Accreditor).

51. Significant changes or additions to security functions, components and interfaces are likely to require re-evaluation to establish appropriate assurance. Appropriate recommendations should be included in a Maintenance Report.

Reporting in the Maintenance Report

52. Details of reporting will depend on the activities required by the AMP but will normally be in the form of a Maintenance Report. This should summarise the review activities performed, the changes reviewed, the sample changes audited and the resulting recommendations, including any changes required to the Assurance Maintenance Plan.

THIS PAGE IS INTENTIONALLY LEFT BLANK

III. SYSTEM ASSURANCE ACTIVITIES

A. System Architecture and Design Review

Objectives:

53. Draw conclusions on whether sufficient design information is available to understand the system in terms of components, interfaces, security functionality and dependencies.

54. Determine to what extent the architecture and design is appropriate for the intended use.

55. Understand the system in more depth for the purpose of planning effective testing of its security.

Guidelines:

56. The Evaluator shall review the system security architecture and design to check that they meet the agreed security requirements. Where there are gaps, the Evaluator should infer and document those gaps in discussion with the Developer.

57. The Evaluator should also consider whether there is any additional functionality (that cannot be disabled), which could potentially be used to bypass security.

58. The design should be reviewed for the following:

- Whether it contains sufficient security functionality information in order to identify all the security related components, interfaces and their dependencies (e.g. on products that are out of scope of the evaluation).
- Consistency with the security requirements.
- Presence (and effectiveness) of any strength-in-depth or self-protection.
- The extent to which complexity will make vulnerabilities harder to find during the evaluation.
- Whether it contains any obvious weak points or potential vulnerabilities e.g. potential for bypassing or deactivating components.
- Whether aspects of the security design could be improved based on experience of industry best practice.

Reporting in the Evaluation Report

59. Functionality and design information should be referenced or explanations given where understanding was gained by other means e.g. discussions with the Developer.

60. A brief description of how the security functionality maps to the design should be included and the general conclusions of each of the activities above should be summarised.

- Where weaknesses are found that require design changes or configuration changes these should be documented with recommendations.

B. System Security Testing

Objectives

61. Confirm that there are no publicly known or generic vulnerabilities in the system.

62. Test the claimed security functionality.

Guidelines

63. The security functionality claimed in the Security Target should be tested. This can be by a combination of independent repetition (or witnessing) of Developer tests together with new tests created by the Evaluator as required. The tests should be spread across the relevant security functionality, components and interfaces and the approach should be agreed with CESG.

64. If testing reveals problems in configuration, installation or operation or that the guidance is unclear (and these issues could result in potential vulnerabilities), then this should be reported by the Evaluator to the Accreditor, Developer and CESG using an Observation Report.

65. An IT Security Health Check should be carried out by a Check Team Leader. This will include the usual work activities including a search for publicly known vulnerabilities, configuration review for key components and port scanning.

66. In addition to purely security functionality tests, the Evaluator should attempt to carry out penetration tests based on ideas developed from their understanding of the design and from knowledge of any vulnerabilities in similar types of product or system. This work should supplement, rather than repeat, the work of any IT Security Health Check.

Reporting in the Evaluation Report

67. The IT Security Health Check should be reported according to CESG guidelines as normal.

Methodology

68. The Evaluation Report should summarise the scope of the Evaluator testing, together with the results and key recommendations. Details of testing should be included in the Annexes to the Evaluation Report. (Where these are lengthy they can be kept as separate test records by the Evaluator and referenced in the report).

69. If the configuration was tied down in a specific way for the evaluation, any assumptions made during testing must be stated. Customers need to understand the limits of how they can reconfigure the system without potentially introducing vulnerabilities.

70. Test records must be sufficiently detailed such that identical tests could be repeated if necessary. These records need to be made available to CESG.

C. Installation and Operational Procedures Review

Objectives:

71. Determine whether the documented procedures are appropriate for the system and follow best practice.

72. Determine whether the documented procedures are actually carried out.

Guidelines:

73. The work carried out here very much depends on the requirements of the Accreditor as detailed in the EWP.

74. Typically, it might be expected to cover aspects such as delivery, installation, administration and user guidance, configuration control, logging and auditing. Backup procedures and disaster recovery plans might also be within scope.

75. Reviewing the effectiveness of protective monitoring tools, systems and procedures is something else that could be brought within the scope of this activity.

76. The Risk Management and Accreditation Document Set² should be consulted where available.

77. The Evaluator should generally review documented procedures for best practice and can follow this up with an audit of the system to determine whether the procedures are being followed.

78. There may be some overlap with the Vulnerability Analysis and Testing activity here, which would need to be coordinated - for example checking the implementation of hardening and password policies.

² See IS2 : Risk Management and Accreditation of Information Systems

Reporting in the Evaluation Report

79. Conclusions and recommendations from the activities above should be summarised with references to documented procedures.

D. System Assurance Maintenance Review

Objectives:

80. The objective of this activity is to provide continual assurance maintenance of the system during its operational lifecycle.

Guidelines:

81. On completion of an evaluation, it is recommended that a system should enter a maintenance phase.

82. An Assurance Maintenance Plan will address how system updates will be assessed, for example giving guidance on categorising likely changes into security impact categories and how the various categories will be tested. If known, a roadmap for system development can also be included.

83. This activity will normally include Maintenance Reviews as follows:

- Periodically - to audit the changes implemented within the period (e.g. annually)
- as driven by events - to review proposed major changes & proposed assurance strategy

84. The periodic review will normally include:

- an assessment of the take up of recommendations from previous reviews
- a check for any new vulnerabilities identified since the previous evaluation or review
- a review of the patching history and its consequences
- a review of the changes to the system detailed in the Security Impact Analysis
- an audit of sample changes to check adherence to procedures
- a review of the associated Developer tests (which should include regressions tests)
- a test of specific updated security functions, if the Developer tests are inadequate

Methodology

- an audit of the application of the operational procedures if appropriate (as required by the Accreditor)
- a review of incident reports by system operators and administrators.

85. A regular IT Security Health Check is likely to be recommended as one way of addressing many of these requirements.

86. Significant changes or additions to security functions, components and interfaces are likely to require re-evaluation to establish appropriate assurance. Appropriate recommendations should be included in a Maintenance Report.

Reporting in the Maintenance Report

87. Details of reporting will depend on the activities required by the plan but will normally be in the form of a Maintenance Report. This should summarise the review activities performed, the changes reviewed, the sample changes audited and the resulting recommendations, including any changes required to the Assurance Maintenance Plan.

88. The report should particularly provide a description of the configuration management, how the changes have impacted on the assurance obtained for the original system and whether a new evaluation is needed.

THIS PAGE IS INTENTIONALLY LEFT BLANK

APPENDIX A : SECURITY TARGET TEMPLATE

<PROTECTIVE MARKING>

SECURITY TARGET

Name & Version of product/system

Reference:

Issue:

Date:

Author Details

Author Name

Author Address

Telephone Number:

Email Address:

Authorisation Details

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Background

Brief background to the project as appropriate – e.g. previous evaluations, sponsoring departments, timescales etc. Refer to risk assessments, accreditation programmes etc.

1.2 Objectives

The objectives of this Security Target are to explain the intended / potential usage of [*product or system name*] and the associated threats to information security. Also, to describe the scope of the evaluation, the security requirements, the security functionality and the selected assurance activities necessary to reduce information security risks to an acceptable level.

2 PRODUCT OR SYSTEM DESCRIPTION

2.1 Identification

This should specify the name and version number of any IT system or products that are to be the subject of the evaluation and their associated platforms.

CESG Tailored Assurance Service

For systems, where this is lengthy, the details can be appended at the end of the Security Target or where a large system is to be evaluated it might be appropriate to refer to high level design documents.

System/Product Name:

Version:

Platform(s):

2.2 Overview

This section should summarise in words and diagrams the functionality of the system or product.

2.3 Scope of Evaluation

This section should clearly summarise which security features, including components and interfaces, are included in the evaluation.

This section should also clearly summarise which security features are not included in the evaluation.

2.4 Security Architecture

This section should include relevant diagrams to illustrate the main security components of the product or system and its environment (both hardware and software), together with any interconnections (both internal and external to the product or system).

2.5 Evaluated Configuration

This section will normally be tentative until the final penetration tests have been completed to confirm details, but provide as much relevant information as is available.

2.5.1 Product or System Hardware and Firmware Components

This should list any product or system hardware and firmware security components, including component types/models/versions.

2.5.2 Product or System Software Components

This should list any product or system software security components, including component versions. List any applicable service packs and patches.

2.5.3 Hardware Environment

This should list the minimum hardware requirements for the platform and other relevant equipment, together with types/models/versions of security components.

Methodology

2.5.4 **Software Environment**

This should list any environmental security components, including component versions. List any applicable service packs and patches. Also list any security-related firmware components.

2.6 **Existing Assurance Certificates**

Include references to any previous assurance certificates that are relevant.

3 **PRODUCT OR SYSTEM SECURITY ENVIRONMENT**

For physically distributed products or systems, separate treatment of the following aspects may be required for each security domain.

3.1 **Assets**

This should define the assets that are to be protected and their potential value.

3.2 **Assumptions**

This should define the intended usage assumptions, including physical, personnel and connectivity aspects.

3.3 **Threats**

This should identify the threats to assets that are countered by the product or system.

3.4 **Security Policies**

This should include references to any policy, standards or rules with which the product or system must comply, e.g. Cabinet Office, CESG or MOD guidelines etc. Any operating system lockdown should also be referenced.

4 **SECURITY OBJECTIVES**

4.1 **Product or System Security Objectives**

This section should state the product or system security objectives. These should be sufficient to counter key aspects of the threats.

Label the objectives to help ensure that the document is readable, e.g.

O.ACCOUNT Users must be accountable for all their security relevant actions when using the product or system.

4.2 **Environmental Security Objectives**

This section should state the environmental security objectives. These, together with the security policies and assumptions, should be sufficient to counter those aspects of the threats not completely countered by the product or system security objectives.

CESG Tailored Assurance Service

Example Environmental Objective:

OE.CRYPTO SSL shall be enabled for all management traffic.

5 SECURITY FUNCTIONALITY REQUIREMENTS

5.1 Product or System Security Functions

This section should state the set of product or system Security Functions provided to meet the IT product or system security requirements. This should be written in unambiguous plain English using well defined terms.

Each Security Function should be given a unique reference to facilitate cross-reference by the Developer or Evaluator, e.g.

AUTH.1 All users shall be identified and authenticated prior to gaining access to the product or system and data held within the product or system.

The Security Functions should be grouped under various applicable headings, such as Identification & Authentication, Access Control, Accounting, Auditing, Integrity, Availability and Data Exchange.

Where applicable, indicate (e.g. in a table) whether each Security Function applies only to one specific component of a product or system, or applies separately to a number of components.

This section may include references to any predefined standard Security Functions that may be appropriate.

The Principal Security Functions should be identified as such (e.g. in a table).

5.2 Environmental Security Functions

This should be similar to section 5.1, but focussed on the dependencies of the product or system on the IT environment (i.e. those IT security requirements met by the environment).

5.3 Required Security Mechanisms

These should state any mandated security mechanisms, such as CESG password algorithms. Where applicable, these should be related to specific Security Functions.

6 ASSURANCE REQUIREMENTS

6.1 Product or System Assurance Requirements

This section should state the target assurance requirements for the product or system and its barriers, based on the Residual Risks derived from a referenced

Methodology

IS1 calculation or equivalent Risk Assessment, as agreed with the Sponsor and Accreditor.

6.2 Assurance Measures

This section should summarise the planned assurance activities, selected and tailored as appropriate, to meet the product or system assurance requirements.

The section should clearly state what assurance activities apply to each product or system Security Function or group of Security Functions.

6.3 Environmental Assurance Requirements

This section should summarise the assurance requirements for any product or system dependencies on the IT environment, as required by the Sponsor, CESA and Accreditor. The section should clearly state the assurance requirements that apply to the environmental functionality that supports a product or system Security Function or group of Security Functions. These assurance requirements are outside the scope of the evaluation. (The evaluation will check any claimed assurance certificates and that the relevant environmental functionality is correctly invoked via the Application Programming Interfaces (APIs) stated in the Security Target and that, within the rigour of the analysis, the APIs are not subject to vulnerability, e.g. bypass.)

7 RATIONALE

7.1 Security Objectives Rationale

This section should include a justification (normally in the form of a table) showing how each Security Objective is traceable to all relevant aspects of the product or system security environment (assumptions, threats & security policies). The rationale may be satisfied by mapping the threats to the objectives, assumptions and policies.

7.2 Security Functions Rationale

This section should include a justification (normally in the form of a table) showing how each Security Function is traceable to the Security Objectives used to counter the threats to the product or system.

7.3 Assurance Rationale

This section should include a justification summarising the rationale for any tailoring of the assurance activities

Annex A GLOSSARY OF TERMS

The glossary must be relevant to terms used in the ST.

Annex B REFERENCES

CESG Tailored Assurance Service

A list of *all* the referenced documents, including policies, standards, procedures and rules, together with any previous reports relevant to assurance in the product or system.

APPENDIX B: EVALUATION WORK PROGRAMME TEMPLATE

<PROTECTIVE MARKING>

EVALUATION WORK PROGRAMME

[Name & Version of product/system]

Reference:

Issue:

Date:

Task Id:

Author:

Evaluation Company Details

Evaluation Company Name

Evaluation Company Address

Telephone Number:

Subcontractor Details

Subcontractor Name

Subcontractor Address

Telephone Number:

Sponsor Details

Sponsor Name

Sponsor Address

Telephone Number:

Developer Details

Developer Name

Developer Address

Telephone Number:

Authorisation Details

TABLE OF CONTENTS

INTRODUCTION

Background

This document specifies the Evaluation Work Programme (EWP) for [Name & Version of product/system] to meet the assurance requirements of the Accreditors as specified in the Security Target [ST]. The reader of this document is assumed to be familiar with the Security Target.

Objectives

The primary objective of this EWP is to define the assurance activities required to establish whether the security functionality of the [Name & Version of product/system], together with its supporting procedures, meet the assurance requirements specified in [ST].

CESG Tailored Assurance Service

Evaluation Milestones

Start Date (Preparation Phase):	End Date (Preparation Phase):
Start Date (Evaluation Phase):	End Date (Evaluation Phase):
Development Site Audit Date:	Operational Site Audit Date:
Functional Test Date:	Penetration Test Date:
Evaluation Report (draft) Date:	Evaluation Report (Final) Date:

Evaluator Details

Evaluation Team Leader	Evaluation Team Members
Subcontractor Team Leader (Provide contact information as appropriate)	Subcontractor Team Members

EVALUATION APPROACH

The evaluation will follow the Methodology (for products or for systems as appropriate), together with any task specific guidance provided by CESG and the Accreditors. [State any specific guidance received from CESG and the Accreditor]

This section lists the selected assurance activities that will be performed during the evaluation and references the assurance rationale in [ST] for the evaluation-specific tailoring. A table may be used to provide task specific details for each activity as appropriate.

If the task is a re-evaluation of a previously evaluated or certified [Name & Version of product/system], the approach should state how any previous evaluation results can be reused. The focus of the evaluation should be on any security relevant changes since the previous evaluation.

If this is an Assurance Maintenance re-evaluation, there should be a Security Impact Analysis that can be referenced for guidance on the changes since the previous version.

If subcontractors are to be used for any assurance activities (whether generalist or specialist testing), this section should clearly indicate which activities are to be performed by the subcontractors.

This section should summarise the approach to synchronising with any other assurance activities, e.g. an IT Security Health Check, to be performed by another organisation or subcontractor, showing how the work in such activities will not be unnecessarily repeated.

This section should also summarise the strategy for any Vulnerability Analysis and Testing.

POTENTIAL VULNERABILITIES

This section summarises the initial Evaluator ideas for potential vulnerabilities that may exist in the [Name & Version of product/system], based on the [Name & Version of product/system] scoping information available during the Preparation Phase, and describes the impact of this on the assurance activities, such as vulnerability analysis and testing.

This section also summarises any potential vulnerability ideas suggested in discussion with the Accreditor and CESG.

TEST STRATEGY

This section summarises the initial ideas for the test strategy and test configurations. This includes the planned test locations and test environments (e.g. test reference system or operational system).

The planned test configurations should include the IT environment that provides realistic test scenarios. (Diagrams should be provided as appropriate.)

The test strategy should summarise the rationale for the sufficiency of the test configurations.

The independent tests should ensure that all Security Functions have been comprehensively tested by a combination of Developer and Evaluator work. Any gaps in the Developer tests should be completed by Evaluator tests where this is justified. The focus of the functional and penetration tests should be the Principal Security Functions and Interfaces, but not to the exclusion of the supporting Security Functions.

This section should also summarise any test ideas suggested in discussion with the Accreditor and CESG.

SAMPLING STRATEGY

This section details the sampling strategy for the repetition or witnessing of Developer Security Function tests. This should not normally exceed 5-10% of the Developer Security Function tests, except where problems have been found in the test evidence provided by the Developer. The tests should cover the broad range of Security Functions, Interfaces and components within the evaluated configuration.

SOURCE CODE ANALYSIS STRATEGY

This section summarises the source code analysis strategy, including the key objectives of the automated and/or manual approaches proposed.

TEST TOOLS

This section details the task-specific tools, including their purpose, that the Evaluators propose to use. This may be tabularised.

CRYPTOGRAPHIC EVALUATION

This section summarises any responsibility for and method of cryptographic evaluation (e.g. CAPS or FIPS-140). Ensure that any dependencies will be addressed, e.g. key management.

ASSURANCE DEPENDENCIES

This section summarises the method of verifying acknowledgement of any complementary assurance results (e.g. checking published certification information for any dependencies on evaluated COTS product functionality or cryptographic functionality).

Annex A GLOSSARY OF TERMS

This glossary lists all key terms referenced in the EWP.

Annex B REFERENCES

This section lists all referenced documents, including policies, standards, procedures and rules, together with any previous reports relevant to assurance in the product or system.

[ST]	[Name & Version of product/system] Security Target
[AMP]	[Product or System Name] Assurance Maintenance Plan

APPENDIX C: EVALUATION REPORT TEMPLATE

<PROTECTIVE MARKING>

TAILORED ASSURANCE SERVICE

EVALUATION REPORT No: <TSnnn or TPnnn> (Supplied by CESG)

Name & Version of product/system

Reference:

Issue:

Date:

Task Id:

Author:

Evaluation Company Details

Evaluation Company Name

Evaluation Company Address

Telephone Number:

Subcontractor Details

Subcontractor Name

Subcontractor Address

Telephone Number:

Sponsor Details

Sponsor Name

Sponsor Address

Telephone Number:

Developer Details

Developer Name

Developer Address

Telephone Number:

Authorisation Details

This should include the name(s), function(s) and signature(s), or equivalent, of the report Authoriser.

Point of Contact for Technical Queries on the Evaluation Report

Contact Name

Contact Email Address

Telephone Number

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

1.1 Summary

It is assumed the reader is familiar with the Security Target [ST] and the Evaluation Work Programme [EWP]. Results will only be reported in any detail where they were unexpected and the Security Functions failed to work properly in some way. In this case the consequences for the secure use of

CESG Tailored Assurance Service

the product or system will be discussed and recommendations made to the Accreditor on residual risk and business impact.

1.2 Summary of Results

This should state whether all the Security Functions, including the Principal Security Functions, specified in the ST were tested successfully, and, if not, this section should summarise which Security Functions failed and why (e.g. the significant security functional errors).

This section should also summarise any security vulnerabilities that need to be countered.

1.3 Observations and Recommendations

Any recommendations to the Accreditor, Sponsor and/or Developer should be clearly explained in separate subsections.

Recommendations to the Accreditor will generally relate to the Residual Risks or business impact. The Evaluation Report should highlight any additional countermeasures required, such as updated [OpDocs], and if appropriate, any additional risks to be recorded in the Security Risk Register [SRR]. It should also highlight any aspects that should be addressed during the Maintenance Phase.

Recommendations to the Sponsor will generally relate to the use or configuration of the System/Product, or to highlight any specific aspects of guidance or environmental restrictions in the ST that are particularly critical to the security of the System/Product. The Evaluation Report should highlight any impact on the [AMP].

Recommendations to the Developer are likely to include such things as recommended fixes (including configuration and design changes) to the System/Product, together with its documentation or development procedures, that should be addressed during the Maintenance Phase.

2 EVALUATION OVERVIEW

2.1 Introduction

Include the start and end dates of the Evaluation Phase.

2.2 Description of Security Features

The description should reference the security architectural description in the ST. Diagrams should be included to illustrate the architectural components

Methodology

and interfaces and any network topology where these are needed to amplify the information in the ST.

The Security Functions and Interfaces, together with the Principal Security Functions, are fully described in the ST.

2.3 Assurance Activities

This should clearly identify the assurance activities that were performed or witnessed by the Evaluation Company and if applicable, those which were performed or witnessed by a sub-contractor. Include any preliminary tests and IT Security Health Checks. (A table may be appropriate.)

2.4 Location and Date of Tests

This section should include details of all locations where the Security Function tests, IT Health Check tests and penetration tests were conducted or witnessed. If a sub-contractor conducted part of the tests, the location of the tests conducted by the sub-contractor should also be included.

The type of location (e.g. development system, reference system or operational environment) should be stated.

2.5 Test Configuration

Models and versions of each test component (hardware, firmware, software), including any patches, within the scope of the evaluation should only be included if not in the Security Target.

This section should only document changes to the test environment, test configuration and processes used compared to those described in the Evaluation Work Programme. Include a diagram of the test configuration if different to that in the Description of Security Features.

2.6 Platform Configuration

Models and versions (including service packs and hotfixes) of each platform or third party component (hardware, firmware, software) should be included here or referenced from Annex C if not included in the Security Target.

2.7 Conduct of Testing

The test method, including the evaluation methodology and approach, together with the evaluation tools and strategies for testing and sampling, is outlined in [EWP].

CESG Tailored Assurance Service

Any supplementary information regarding the test method, and/or the rationale for any deviation from the [EWP], is recorded in Annex E.

The Evaluator must confirm that any such deviation from the EWP, e.g. prioritisation of Security Functions or assurance activities, was agreed with the Sponsor, Accreditor and CESG prior to completion of the activity, and a supporting reference supplied.

3 EVALUATION RESULTS

3.1 Security Architecture

Any weaknesses or recommendations in accordance with best practice should be recorded.

3.2 Security Functional Test Results

This should state the extent to which the security functionality claims in [ST] were met, highlighting any exceptions giving rise to unresolved problems found in the Security Functions and Interfaces. Include references to the detailed results in Annexes D and F or any unresolved Observation Reports. Any specific recommendations should be highlighted.

3.3 IT Security Health Check Results

If applicable, this section should state the results and recommendations of the IT Security Health Check tests and reference the detailed results in [ITSHC Report].

3.4 Penetration Test Results

This section should state the results and recommendations of the Evaluator's penetration tests and reference the detailed results in Annexes D and G.

This section should confirm whether the System/Product is resistant to publicly known vulnerabilities and whether any potential vulnerabilities are exploitable.

3.5 Guidance Documentation

Any comments or recommendations regarding the adequacy and accuracy of the supporting installation, configuration and operational documentation related to the security functions and interfaces should be included.

Methodology

3.6 Ease of Use

Any unresolved problems related to difficulty in installing, using or misusing the System/Product should be recorded.

3.7 Development Procedures

Any weaknesses or recommendations should be recorded. Details are given in Annex C

3.8 Source Code Analysis Results

This section should state the results and recommendations of the source code analysis and reference the detailed results in Annex D. The section should confirm whether the components examined in detail contained any potential vulnerabilities and whether these are exploitable.

3.9 Disclaimers

The results in this Evaluation Report relate only to the Security Functions specified in the Security Target and only to the items tested.

The recommendations in this Evaluation Report are applicable only to the use of the System/Product in the environment specified in the Security Target.

The Tailored Assurance Service evaluation is not a guarantee of freedom from security vulnerabilities. There remains a probability that exploitable security vulnerabilities may exist in the System/Product, or the IS environment supporting the System/Product.

The issue of an Evaluation Report is not an endorsement of a system or product.

Include a statement to confirm whether the report includes any opinions or interpretations.

ANNEX A GLOSSARY OF TERMS

This glossary defines the terms used in the Evaluation Report.

AMP	Assurance Maintenance Plan
EWP	Evaluation Work Programme
ST	Security Target

ANNEX B REFERENCES

This section records the final set of deliverables used to conduct the evaluation activities detailed in this Evaluation Report, together with other key documents.

[ST]	Security Target
[EWP]	Evaluation Work Programme
[Methodology]	Tailored Assurance Service Methodology
[OpDocs]	Administration and User Guides
[ITSHC Report]	IT Security Health Check report, if applicable
[AMP]	Assurance Maintenance Plan, if applicable
[SRR]	Security Risk Register
[Fun Tests]	Security Functional Test Scripts
[Pen Tests]	Penetration Test Scripts

ANNEX C SUMMARY INFORMATION

The following sections summarise the Evaluator understandings of the System/Product and aspects related to assurance.

C1 Subsystems and Interfaces

This section summarises the security role of each System/Product subsystem or major component where it differs from the ST. It includes the mapping between the Security Functions and the System/Product subsystems. It also summarises the key interfaces.

C2 Shared Resources

A summary of sources of potential conflict (e.g. a table)

C3 Component Integration and Configuration Issues

For System/Products comprised of several components (e.g. COTS products & bespoke applications) - a summary of any integration or configuration aspects that are relevant to establishing the required assurance.

C4 Platform Dependencies

A summary of the dependencies on the platform or IT environment

C5 Developer Procedures and Tools

A summary of the key development procedures and tools, including the Configuration Management System (Name and version).

A summary of the role of the Developer's key automated tools.

C6 Delivery Procedures

A summary of the delivery procedures showing how System/Product integrity will be protected from compromise during delivery to User site using all delivery methods (e.g. CD and Internet delivery mechanisms) and how the User can check that the System/Product version is correct and untampered.

C7 Maintenance Procedures

A summary of the procedures to be used during the Maintenance Phase, addressing vulnerability procedures and showing how System/Product updates and workarounds are controlled and distributed.

Alternatively: These may be detailed in [AMP].

ANNEX D ASSURANCE ACTIVITY RESULTS

This annex summarises the results against the system and/or product assurance activities selected, in accordance with the 'Reporting' guidance. Results should be reported against individual assurance activities and not to any finer level of granularity than this. The emphasis should be on **reporting by exception**: if no problems were found then the Evaluation Report should normally include no more than 1-3 paragraphs per assurance activity, summarising the Evaluator findings.

Any unresolved issues identified by the Evaluators should be clearly described in the Evaluation Report, together with the impact on System/Product assurance. In general, these will either be actual errors or vulnerabilities discovered during testing, or failures against one or more of the key points of understanding of the Assurance Activities. Where the problem is not an error or vulnerability in the actual System/Product, the Evaluator should clearly explain its potential impact in terms of the following aspects (as appropriate to the assurance requirement):

- Evaluator testing, i.e. whether it was possible to investigate the problem or concern during subsequent assurance activities; or whether there is a risk that the Evaluators (as a result of a lack of understanding of some aspect) may have overlooked a vulnerability in the System/Product, or may have failed to execute a test which would have identified a vulnerability;

CESG Tailored Assurance Service

- secure operation of the System/Product, i.e. whether there is a risk that users or administrators of the System/Product will configure or use the System/Product in an insecure manner;
- integrity of the System/Product, i.e. whether there is a risk that the integrity of the developed or delivered System/Product could have been compromised through the introduction of a vulnerability during the process of development, production or delivery.

D1 Functionality and Design Assessment

D2 Development Procedures Review

D3 Security Function Testing

D4 System Architecture and Design Review

D5 System Security Testing

D6 Installation and Operational Procedures Review

D7 Source Code Analysis

D8 Vulnerability Analysis and Testing

ANNEX E TEST METHOD

The test method, including evaluation approach and strategies for source code analysis and testing and sampling, are documented in [EWP]. Any change to or refinement to the test method must be recorded.

The Evaluator's strategy for Security Function Testing, IT Security Health Check Testing and Penetration Testing must always be documented.

Sample sizes (e.g. for repeat tests) and samples used must be justified. Sample sizes should be sufficient to detect any systematic problems. (This Annex may reference separate documentation, if requested by the Sponsor, which should be delivered to CESG together with the Evaluation Report).

Any test tools not recorded in the EWP should also be summarised, including their name, version and purpose.

Methodology

ANNEX F SECURITY FUNCTION TEST RESULTS

The Security Function test scripts are documented in [Fun Tests].

This Annex should summarise the results for any Security Function for which the actual results were not the same as the expected results. The unique Security Function ID must be mapped to the test scripts used and the result summary for that test.

SF Id	Test Id	Results

ANNEX G PENETRATION TEST RESULTS

The penetration test scripts are documented in [Pen Tests].

This section should summarise the results for each test objective.

Test Id	Test Objective	Results

ANNEX H CRYPTOGRAPHIC FUNCTIONALITY

This should summarise the outcome of any required CAPS or FIPS-140 assessment. This may also be a useful place to clarify the role of any cryptographic functionality in the product or system (e.g. if the product or system contains minimal cryptographic functionality which did not therefore require CAPS assessment). However, if such comment is made it should be stressed that the Evaluation Report does not itself provide any endorsement or approval of the cryptographic functionality provided by the product or system.

THIS PAGE IS INTENTIONALLY LEFT BLANK

APPENDIX D: ASSURANCE MAINTENANCE PLAN TEMPLATE

<PROTECTIVE MARKING>

ASSURANCE MAINTENANCE PLAN

Name & Version of product/system

Author Details

Author Name

Author Address

Telephone Number:

Email Address:

Reference:

Issue:

Date:

Authorisation Details

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Background

This document specifies the Assurance Maintenance Plan (AMP) for [product or system Name] [product or system Version] to meet the assurance requirements of [User] specified in [ST]. It is assumed the reader is familiar with the ST.

1.2 Objectives

The objectives of this AMP are to provide the procedures for maintaining and improving the assurance in the product or system as determined in the previous Tailored Assurance Service evaluation by the Evaluator [Eval Report] and CESG [Statement], as updated by any previous Maintenance Review [Maintenance Report] or IT Security Health Check [ITSHC Report].

1.3 Purpose of Document

This document is the AMP for [product or system Name] [product or system Version].

This AMP contains the schedule and specifies the procedures relevant to the maintenance of [product or system Name], including the procedures for Change Control, Vulnerability Awareness, Patching, Testing and Maintenance Reviews.

2 MAINTENANCE SCHEDULE

This section provides the schedule of new releases planned over the next 12 months, together with the associated Maintenance Reviews or Re-evaluations.

3 VULNERABILITY AWARENESS AND PATCH PROCEDURES

This section references the procedures for vulnerability awareness and patch handling, including target for responses to problems, and summarises any differences from the previous evaluation (e.g. patch delivery procedures).

4 CHANGE PROCEDURES

This section references the change control procedures and summarises any differences from the previous evaluation.

5 TEST STRATEGY

This section summarises the strategy for maintenance tests and independent tests including assumptions and constraints underlying the test strategy.

6 PRODUCT OR SYSTEM UPDATE AND IMPACT ANALYSIS PROCEDURES

This section summarises or references the procedures for product or system updates by the Developer. Proposed changes for a future release should be summarised in an outline Security Impact Analysis (SIA) and reviewed by the Accreditor, Evaluator and CESG as appropriate, prior to implementation.

7 MAINTENANCE REVIEW PROCEDURES

This section summarises or references the procedures for Maintenance Reviews performed by the Evaluator. Maintenance Reviews are recommended prior to agreement of significant changes. They are also recommended periodically, when the SIA for a specific release has been populated with references to the assurance evidence.

Annex A GLOSSARY OF TERMS

This glossary lists all key terms referenced in the AMP.

Annex B REFERENCES

This section lists all referenced documents, including policies, standards, procedures and rules, together with any previous reports relevant to assurance in the product or system.

[ST]
[Eval Report]

Methodology

[Statement]
[Maintenance Report]
[ITSHC Report]

Annex C PRODUCT OR SYSTEM COMPONENTS

This section provides or references a definition of all product or system components, including hardware and software subsystems or components, each categorised as Security Enforcing, Security Relevant or Security Irrelevant but only where this differs from the ST. Sufficient detail should be included to enable changes in these components to be categorised as Security Enforcing, Security Relevant or Security Irrelevant.

For Residual Risks in the range 13.5 to 14.4, specific (groups of) product or system source code and configuration files should be included.

THIS PAGE IS INTENTIONALLY LEFT BLANK

APPENDIX E: MAINTENANCE REPORT TEMPLATE

<PROTECTIVE MARKING>

TAILORED ASSURANCE SERVICE
MAINTENANCE REPORT No: <TSnnn or TPnnn> (Supplied by CESG)

Name & Version of product/system

Reference:

Issue:

Date:

Task Id:

Author:

Evaluation Company Details

Evaluation Company Name
Evaluation Company Address
Telephone Number:

Subcontractor Details

Subcontractor Name
Subcontractor Address
Telephone Number:

Sponsor Details

Sponsor Name
Sponsor Address
Telephone Number:

Developer Details

Developer Name
Developer Address
Telephone Number:

Authorisation Details

This should include the name(s), function(s) and signature(s), or equivalent, of the report Authoriser.

Point of Contact for Technical Queries on the Maintenance Report

Contact Name
Contact Email Address
Telephone Number

TABLE OF CONTENTS

Executive Summary

- Summary of changes
- Observations & Recommendations

Maintenance Overview

CESG Tailored Assurance Service

- Introduction
- Maintained Configuration
- Maintenance Activities
- Changes Reviewed and Audited
- Location and Date
- Test Configuration
- Platform Configuration
- Conduct of Testing

Maintenance Results

- Correctness and Completeness of Security Impact Analysis
- Security Functional Test Results
- IT Security Health Check results
- Guidance Documentation
- Disclaimers

Annex A Glossary of Terms

Annex B References

APPENDIX F: ASSURANCE MAINTENANCE GUIDANCE

INTRODUCTION

This part of the documentation provides guidance on the Assurance Maintenance of previously evaluated systems and products. It provides guidance on the contents of the Assurance Maintenance Plan (AMP) and the categorisation of changes for the Security Impact Analysis (SIA).

GENERAL GUIDANCE

When entering into 'Assurance Maintenance', a system operator or system maintainer will be responsible for producing and signing up to an agreed Assurance Maintenance Plan covering a specified maintenance period. They will need to keep to the plan in order to maintain assurance continuity.

There is no fixed format or prescribed approach for such a Tailored Assurance Service Assurance Maintenance Plan. It may depend for example on the nature of the system and threats, issues found during Maintenance Reviews, re-evaluations, Accreditor requirements and proposed changes to the system. However, some guidance on generating such a plan is given here and in the Assurance Maintenance Plan Template.

The plan should be kept as simple as possible and can reference other documents where needed (to be provided along with the plan). The most important thing being that it should be acceptable to the Accreditor, system operator and CESG. The AMP should be updated as appropriate during each annual Maintenance Review.

During the Maintenance Phase, a Security Impact Analysis is recommended to document the changes, together with their impacts, for a specific release of the system or product. This can be used as the basis for Maintenance Reviews.

MAINTENANCE SCHEDULE

Any planned product or system updates (i.e. new releases) should be identified, together with any unscheduled updates that may have already happened since the last evaluation or Maintenance Review. The main reason for any update should be summarised, including the expected major changes to product or system components. Obviously there is no commitment to keep to the proposed schedule - it is just a tool for planning.

Maintenance Reviews that require support by CESG and/or the Evaluator should be identified. These will include an annual Maintenance Review and any intermediate Maintenance Review required for a product or system update that includes major proposed product or system changes.

CESG Tailored Assurance Service

Any planned Re-evaluation should be identified, particularly where the security architecture is known to be due for change.

VULNERABILITY AWARENESS AND PATCH PROCEDURES

This should address the procedures and resources in place to maintain vulnerability awareness (e.g. in-house monitoring, CHECK service or other contractor) and the response if new vulnerabilities are made public. The specific procedures should be referenced. Summarise any change to the patch procedures (e.g. delivery procedures), where different to the previous evaluation.

The AMP should include the timescales within which patches will normally be applied (e.g. next planned release).

TEST STRATEGY

How will operational system changes (planned or otherwise) be tested? In particular how will the security aspects be tested before changes are made to the operational system? Will the tests be conducted on the operational system or a reference system? Will regression tests be included? Will the security tests used in the original evaluation be reused? The AMP should reference the test plan, procedures, data and test configuration as appropriate.

Include the strategy for scheduled independent testing. For example, this might be an annual IT Security Health Check or (where the Maintenance Schedule indicates major changes) it could involve IT Security Health Checks of key parts of the system throughout the year. It may also include Evaluator tests.

PRODUCT OR SYSTEM UPDATE AND MAINTENANCE REVIEW PROCEDURES

One of the goals of Assurance Maintenance is to let the product or system operator get on with running the product or system without external interference. However, there is a need to keep CESG, the Accreditor, the System Change Control Board and the Evaluator informed of security-related changes to the product or system, including its documentation, and for CESG, the Accreditor and/or the Evaluator to review any proposed major changes before they happen.

Note that a Maintenance Review could consist of a phone call in some cases. The result of a review could be:

- No need for further action
- Independent scrutiny (e.g. check configurations, witness testing)
- IT Security Health Check of certain components
- Re-evaluation

Methodology

- A statement that the proposed change would be unacceptable, with rationale why security or assurance is undermined

To support the agreed Maintenance Schedule, the *Security Relevant* and *Security Enforcing* components of the system need to be identified and listed. Further guidance on the categorisation of changes is provided below under 'Example Change Definitions'.

GUIDANCE ON PRODUCT OR SYSTEM UPDATES AND MAINTENANCE REVIEWS

Product or System Updates

The product or system operator will provide CESG, the Accreditor and the Evaluator with details of product or system changes that have been carried out at agreed intervals (e.g. every 3 months). This will list all *Minor*, *Medium* and *Major* changes to *Security Relevant* or *Security Enforcing* components and their security impact. These details may be in the form of a Security Impact Analysis document, which should be provided prior to each product or system update and should provide the relevant security information to support Maintenance Reviews and any other related security reviews.

Security Impact Analysis

For a specific product or system update, this document summarises each identified product or system change and the associated impact on the previous evaluation deliverables (including Security Target, architecture, design, test material, source code (if applicable), product or system components and operational documentation). Each change should be categorised as Minor, Medium or Major.

The Security Impact Analysis should highlight any change to the Risk Analysis and identify any new or changed security risks that need to be reflected in the Security Risk Register. Risk changes should be identified as Critical, Major or Minor.

Maintenance Reviews

A review with CESG, the Accreditor and/or Evaluator will be required:

- Before Major changes to Security Relevant or Security Enforcing components.
- Before Medium changes to Security Enforcing components.
- At the request of CESG, the Accreditor or system operator.
- Every 12 months at the least.

EXAMPLE CHANGE DEFINITIONS

Example Security Enforcing and Relevant Components

(Note that these examples are based on a system for Residual Risk in the range 11.5 to 14.4 of IS1)

Security Irrelevant	Security Relevant	Security Enforcing
Disabled Operating System components	Operating System components that support the product or system (e.g. separation mechanisms on which the product or system depends)	Operating System audit functions that provide product or system Security Functions
Routers that are out of scope (outside the LSE)	Routers in scope (no ACL)	Routers with ACL
Disabled firewall functionality	Firewall interfaces that are relied upon to maintain separation between transactions.	Firewall components that implement the transaction rules of the firewall security policy
Management components that cannot be directly attacked.	Management components that need to be hardened from attacks by unauthorised users.	Management components providing I&A functions against unauthorised user communities.

Example Definitions of Changes

Major:

Core network functionality e.g. new types of service or traffic.

Customer access methods.

Management connectivity (e.g. for third party support).

New platform, software or connection.

Significant platform upgrade (e.g. workstation or server with new processor architecture)

Significant software upgrade.

System architecture change.

Medium:

Incremental operating system upgrade (minor functionality change).

Minor Hardware upgrade (same family but faster processor, RAM etc).

Minor Software upgrade (e.g. patch that carries some functionality change).

Change to security policy (e.g. for configuring firewalls or routers).

Methodology

Minor:

Security patch (not changing intended functionality, but corrects a specified fault).

Don't need to include in updates:

Adding users, routers, etc.

Add individual hosts to firewall rule-sets (but no change in policy).

Change to ACL configuration (but no change in policy).

Update content checking rules (e.g. for intrusion detection).

THIS PAGE IS INTENTIONALLY LEFT BLANK

.....
(INSERT PROTECTIVE MARKING ON COMPLETION)

Methodology

CUSTOMER FEEDBACK FORM

CESG Information Assurance Policy and Standards welcomes feedback. **Please add an appropriate protective marking** and use this form to send any comments to:

Customer Support
CESG
A2j
Hubble Road
Cheltenham GL51 0EX
(for the attention of CESG Commercial Services)

Fax: 01242 709193
Email: enquiries@cesg.gsi.gov.uk

PLEASE PRINT

Name of Document: CESG Tailored Assurance Service Methodology, Version 2.1
Name:
Department/Company Name and Address:
Your Contact Details:
Comments:

June 2007

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on 01242 221491 x30306 (non-sec) or email infoleg@gchq.gsi.gov.uk

.....
(INSERT PROTECTIVE MARKING ON COMPLETION)

.....
(INSERT PROTECTIVE MARKING ON COMPLETION)

CESG Tailored Assurance Service

THIS PAGE IS INTENTIONALLY LEFT BLANK

June 2007

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on 01242 221491 x30306 (non-sec) or email infoleg@gchq.gsi.gov.uk

.....
(INSERT PROTECTIVE MARKING ON COMPLETION)