



Tailored Assurance Service

Operating Procedure for Evaluations

Version 1.0

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
1.0	June 2007	Copied from paras 8-18 and 77 to end of version 0.7 used in Contract negotiations

Operating Procedure for Evaluations

CONTENTS

Foreword	ii
Contents	iii
References	iv
Glossary	v
I. INTRODUCTION.....	1
A. Outline of Tailored Assurance Service.....	1
II. INITIATING A TAILORED ASSURANCE SERVICE EVALUATION	5
A. Background	5
B. Evaluation of a new IT system and typical Contract Model.....	5
C. Specialist Test House	7
D. Cryptography & TEMPEST	8
III. THE CONDUCT OF EVALUATIONS	9
A. Commercial Impartiality	9
B. Product Evaluation.....	9
C. System Evaluation	10
IV. FUNDAMENTAL PRINCIPLES	13
A. Understanding	13
B. Competence	13
C. Objectivity	14
D. Repeatability	14
E. Prioritisation	15
V. EVALUATION PHASES	17
A. Preparation Phase	17
B. EVALUATION PHASE	19
C. REPORTING PHASE	21
D. MAINTENANCE PHASE	22
E. Assurance Maintenance Plan	23
APPENDIX A : TOP LEVEL RESPONSIBILITIES	A1
APPENDIX B: ORGANISATION AND MANAGEMENT CONTEXT	B1
Customer Feedback Form	at end of document

REFERENCES

- [a] ISO/IEC 27001 : 2005. Information Security Management Standard.
- [b] JSP 440 – MOD Joint Service Publication 440. The Defence Manual of Security.
- [c] HMG Infosec Standard No. 2, Risk Management and Accreditation of Information Systems, Issue 2.0 (July 2005) (under review).
- [d] CSIA Claims Tested Mark Scheme.
www.cabinetoffice.gov.uk/csia/claims_tested_mark/
- [e] TAS Methodolgy.
- [f] TAS Operating Procedure for Evaluation Companies.
- [g] TAS Contract and Schedules.

Operating Procedure for Evaluations

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
Authority	Means the 'The Secretary of State for Foreign and Commonwealth Affairs (Acting through GCHQ of which CESG is the Information Assurance arm)'
CAM	Customer Account Manager
CESG	Means GCHQ's Information Assurance (IA) arm and as the National Technical Authority bears the responsibility for reviewing and auditing the Evaluation Company work and providing assurance to the Accreditor.
CNI	Critical National Infrastructure
Contract	Means the Tailored Assurance Service Framework contract.
COR	Critical Observation Report that may result in change to EWP
Customer	The HMG Department or other CNI organisation requiring the evaluation of an IT system or product
Developer	The company supplying the IT system/product required by the Customer
EWP	Evaluation Work Programme
HMG	Her Majesty's Government
IA	Information Assurance
IACS	Information Assurance and Consultancy Services
IT	Information Technology
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 or product – it will depend on the precise contract arrangements between those organisations
SSA	Service & Supply Arrangement, an agreement that exists between CESG and other government departments and certain public bodies

THIS PAGE IS INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. Outline of Tailored Assurance Service

1. An overview of the Service is as follows:
 - i. The Tailored Assurance Service is designed to meet the needs of HMG Infosec Standard No.1 (IS1) and *equivalent* documents like the MOD's JSP440, which are based on risk analysis and countermeasures.
 - ii. The Tailored Assurance Service is appropriate for residual risks¹ in the range 11.5 to 14.4. Where the residual risk is 11.4 or less, the solution can be found by the appropriate use of alternatives such as the CSIA Claims Tested Mark Scheme, ISO/IEC 27001: 2005 audit and IT Health Checks. Where the residual risk is 14.5 or higher, then CESG should be contacted to discuss possible approaches. The Tailored Assurance Service will be introduced during 2Q07 and a Pilot phase is expected to run for 18 months. During this phase the approach may well be changed as circumstances dictate. Fast Track and SYSn will be phased out.
 - iii. The evaluations will focus on the technical issues and the procedural aspects associated with the technical security but the procedural aspects do not include physical or personnel security. As far as availability is concerned, the evaluations can consider resilience against malicious denial of service attacks but in general will not consider reliability or redundancy.
 - iv. Accreditors must make final decisions on whether the risks are acceptable and it is their responsibility to ensure that all aspects of security have been covered to their satisfaction.
 - v. All relevant documentation, including example templates for a Security Target, Evaluation Work Programme, Evaluation Report and Assurance Maintenance Plan will be available on the CESG website and are provided in the TAS Methodology document.
2. The Tailored Assurance Service is intended to be used in a flexible way and so where appropriate can be used with platforms or components that have been evaluated using alternative approaches such as Common Criteria (CC) or ITSEC.
3. The service is intended for a wide range of IT products and systems ranging from simple software components to national infrastructure networks. Therefore, a

¹ Note that the residual risk concept will be changed in the new IS1 but the precise nature of these changes is not known

CESG Tailored Assurance Service

toolbox of activities is provided that enables each evaluation to be tailored as appropriate. A summary of these activities is provided in the table below.

Product Assurance Activities
Development Procedures Review
Functionality & Design Assessment
Security Function Testing (including search for publicly known or generic vulnerabilities)
Vulnerability Analysis & Testing (penetration testing)
Product Assurance Maintenance Review
Source Code Analysis

System Assurance Activities
System Architecture & Design Review
System Security Testing
Installation & Operational Procedures Review
System Assurance Maintenance Review

Table 1 – Assurance Activities

4. For residual risks in the range 13.5 to 14.4 further work may be required but given the wide range of products and systems that are evaluated and the multitude of threat environments, this will be decided on a case by case basis by CESG in consultation with the Accrerator.
5. The Accrerator will have the flexibility to decide which of the above activities are most appropriate for their system. The activities are described in more detail in the TAS Methodology document.
6. For example, it may be that procedures for installing and configuring a system will be reviewed separately during the normal accreditation process. In that case, there may be no need to include this activity.
7. Alternatively, if there is a lack of evidence in one area it may be possible to compensate by greater evidence in another. For example, it could be that a Developer can only offer limited evidence for development standards but this could be counteracted by increased effort in vulnerability analysis and testing.

Operating Procedure for Evaluations

8. It may not be necessary to evaluate the whole IT system in most instances just the key barriers and interfaces.
9. Evaluations may only be carried out by an approved Evaluation Company or CESH to a specification detailed in a document called the Evaluation Work Programme (EWP) [see TAS Methodology document for standard template]. The Evaluation Company will on all occasions consult with CESH and the Accreditor on the content and construction of the EWP and later the Evaluation Company will ensure the Evaluation Report carries any recommendations and/or audit reports emanating from CESH .
10. The Evaluation Company will agree a delivery timeline with the Sponsor and one of the deliverables will be the Evaluation Report and any change to the timeline (similarly any change to the Evaluation Company and Sponsor contract that impacts upon CESH) should be cascaded down through Change Control to CESH immediately the change becomes known to the Evaluation Company.
11. In some cases, CESH (or other Government) staff or their Suppliers may be used on some assurance activities where the project has sufficient priority within CESH.

THIS PAGE IS INTENTIONALLY LEFT BLANK

II. INITIATING A TAILORED ASSURANCE SERVICE EVALUATION

A. Background

12. The Tailored Assurance Service is designed for Sponsors who need to have tested an IT system or an IT product to be used in a particular IT system.

13. It has also been constructed to allow IT systems and products to be tested in a flexible way rather than relying on a fixed assurance level such as Common Criteria EAL3. Thus there is no fixed menu of assurance activities but rather a tool box of various assurance activities that could be undertaken and allows the evaluation to be tailored in a way appropriate to the IT system or product and the threats to it. The scenario below shows when a decision can be made about what is to be tested and in what way.

B. Evaluation of a new IT system and typical Contract Model

14. Figure 1 shows a typical situation (although alternative procurement relationships can be entertained within TAS). Here a Customer (either an HMG Department or other CNI organization) needs to acquire a new IT system. Where it is a major IT system for an HMG Department, then CESG's Customer Account Manager (CAM) for that HMG Department can be assumed to know about the system and CESG may have provided consultancy advice under a CESG Service and Supply Agreement (SSA) to help the HMG Department prepare and assess the ITT for the new IT system. The Customer has specified that the system must be assured using the Tailored Assurance Service.

15. The Customer wants the Developer to contract with a Tailored Assurance Service Evaluation Company with the expectation that CESG (in its role as the National Technical Authority) would be contracted to the Evaluation Company to provide technical guidance and audit.

16. Only when the selected system architecture is sufficiently firm can the Evaluation Work Programme (EWP) be constructed and the purpose of the EWP shall be to determine the parts of the system to be tested and the rigour of the testing (i.e. the assurance activities to be carried out). The EWP is owned by the Sponsor and constructed by the Evaluation Company (being the organisation contracted to undertake the evaluation) with input taken from CESG, the Accreditor and the Customer.

CESG Tailored Assurance Service

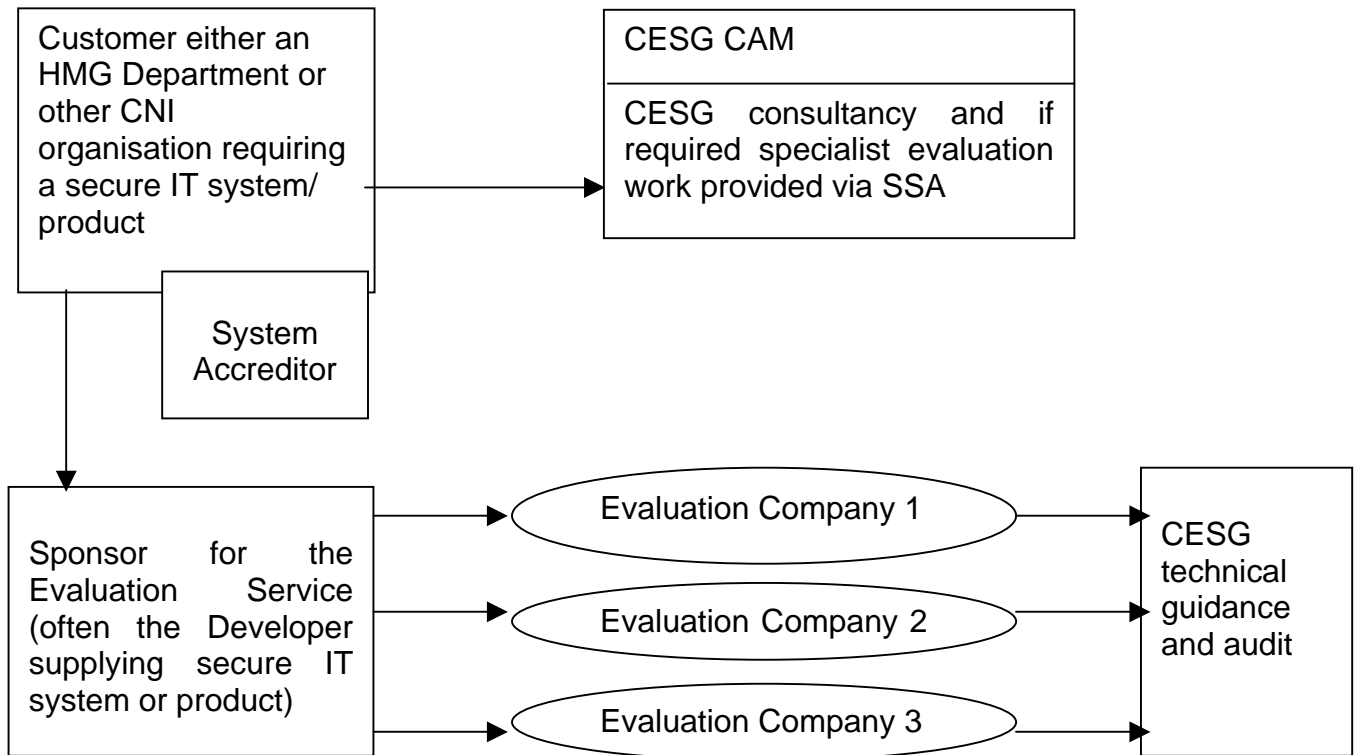


Figure 1 – Typical Contract Model

17. Where parts of the evaluation are to be undertaken by a third party, e.g. CESG or a Specialist Test House then the Evaluation Company shall form a separate contract with the third party (unless the third party is CESG) and that contract shall clearly identify that risk in the final Sponsor deliverables remains with the Evaluation Company. If the third party is CESG then the work will be undertaken using a contract or SSA between the Customer and CESG.

18. Alternative scenarios are:

- HMG Department contracting through an SSA with CESG for technical guidance and audit (which is a nuisance for the HMG Department), or
- HMG Department might contract with a Managed Service Provider who contracts with a Developer to supply the IT system or product.

19. The Customer or Developer should contact the appropriate CAM or the CESG Infosec Assurance and Consultancy Services (IACS) Management Office to answer any initial questions. If both the Customer and Developer wish to proceed, they should complete in full the IACS Questionnaire. Following the return of the IACS Questionnaire, CESG will comment on whether the Tailored Assurance Service approach is appropriate.

Operating Procedure for Evaluations

20. If CESH consider the approach inappropriate, then they will take no further part in the evaluation.

21. If CESH are willing to support the evaluation, the Evaluation Company and CESH shall create a formal contract within which the key personnel of both parties e.g. the Evaluation Company project manager and the CESH Service Delivery Manager roles and responsibilities will be recorded. CESH will effectively become a sub-contractor to the Evaluation Company and the Evaluation Company shall take on the primary supplier role and all the responsibilities that ensue.

22. The ability to respond flexibly yet in a controlled manner is necessary in the light of rapidly changing technology and threats to HMG IT systems. The latter is a key feature built into the Service arising from Customer recommendation. Such activity attracts its own contracting challenges, which the HMG Department and Developer need to resolve. In particular the Evaluation Company may not be able to estimate how much evaluation effort is required until the plans are mature.

23. CESH has limited resource over which it maintains tight control thus it is incumbent upon the Evaluation Company to provide the earliest possible notification to CESH should it require CESH to act as a sub-contractor.

24. Appendix A lists the responsibilities of some of the main players in a TAS evaluation.

C. Specialist Test House

25. A Specialist Test House is a company that specialises in testing one or more of the following :

- anti malware
- biometrics
- cryptography
- data erasure
- intrusion detection/prevention
- smartcards
- electromagnetic emanations
- telecoms products & systems
- other hardware
- other types of technology as may be identified by CESH from time to time.

CESG Tailored Assurance Service

26. Where a Specialist Test House is required to test particular aspects of the functionality of an IT system, then the Evaluation Company shall consult with the Accreditor and CESG and obtain their input prior to selecting the Specialist Test House.

27. Generalist Testing consists of all other testing that has not been specified as one of the above Specialist Testing categories.

D. Cryptography & TEMPEST

28. Systems and products containing a limited amount of cryptography can be handled within the framework of a Tailored Assurance Service evaluation. If cryptography provides the main, or very significant, security measure, then the Developer may be advised to have the system's or product's cryptography and its implementation independently assessed under CESG's Assisted Products Scheme (CAPS), the CESG assurance service aimed specifically at cryptography, or under FIPS140-2. CESG will guide the Developer on the most appropriate route. CESG can also be contracted to provide consultancy on this subject should it be required.

29. Where electromagnetic emanations are a security concern, then CESG needs to be consulted and work by a CESG approved TEMPEST test laboratory may be required.

III. THE CONDUCT OF EVALUATIONS

A. Commercial Impartiality

30. The Evaluation Company shall, upon request by the Authority, be able to demonstrate in writing its independence of a Developer who has been selected by the Customer to supply the IT system or product. An Evaluation Company must be demonstrably independent of the Developer and of the consortium (where the Developer is part of a consortium delivering the IT system or product that is to be evaluated) and other companies belonging to the parent companies of the Developer and consortium:

- The Evaluation Company shall be responsible for ensuring that all work performed by the evaluators will be independent of the development of the IT product or system under evaluation.
- It shall be the Evaluation Company's responsibility to ensure that the Evaluator is free from any commercial, financial or other pressures that might influence their technical judgement and shall be able to demonstrate such should the Authority or the Customer seek such assurance.

31. The Evaluation Company shall offer two types of evaluation:

- IT product and/or
- IT system.

B. Product Evaluation

32. A product in this context is defined as a component used within a system that acts as a security countermeasure (for particular attack paths). Carrying out an evaluation of such a product will give some assurance that a greater capability would be needed to exploit vulnerabilities in the system than believed likely from the current threats to the system and will give a degree of risk reduction as defined in tables in IS1.

33. Product evaluations should be tailored to a particular system environment and will make many assumptions in order to save on time and cost. Obviously the fewer assumptions that are made, the more likely that the results can be applied to different systems. Evaluations may also reveal certain risks that might be acceptable in one case but not another. Details of any such risks would also have to be provided to CESG with the right to use the information to protect other systems.

34. Product evaluations are based on a number of assurance activities that should be tailored according to requirements. However, for the purposes of IS1 certain activities are recommended in order to attain a nominal equivalence to Common Criteria Evaluation Assurance Levels (EALs). This does not mean that the

CESG Tailored Assurance Service

evaluation approach will be the same as Common Criteria (or recognised internationally), it just means that they are considered to be equivalent as far as the IS1 risk treatment is concerned.

35. For information purposes EAL2/EAL3 equivalence is provided by the following activities:

- Functionality and design assessment.
- Development procedures review
- Security function testing (including search for publicly known or generic vulnerabilities)
- Product assurance maintenance review

36. EAL4 equivalence is:

- Functionality and design assessment
- Development procedures review
- Security function testing
- Source code analysis
- Vulnerability analysis and testing
- Product assurance maintenance review

37. Evaluators should also consider a review of “Installation and Operational Procedures” to determine how easy it is to install and configure the product in a secure state.

C. System Evaluation

38. A system evaluation will include a number of products that need to be evaluated. However, in many cases this evaluation can take the form of system security testing and can be covered by the overall Security Target. When products or system components form key barriers or require a higher level of assurance, they should have a separate Security Target and follow the distinct product methodology described above.

39. A system evaluation provides evidence for Accreditors and will be an independent review of the technical security measures taken for systems being accredited according to IS1. The IS1 standard does not specify levels to which an accredited system should be evaluated and therefore this type of evaluation does not claim to be equivalent to Common Criteria EALs.

Operating Procedure for Evaluations

40. It is quite possible that one or more product evaluations of key security 'barriers' (at appropriate levels) could be used in addition to an overall system evaluation.

41. The exact nature of the evaluation should be tailored subject to the Accreditor requirements (or guidance provided under contract by CESG). However the likely components are as follows:

- System architecture and design review
- System security testing
- Installation and operational procedures review
- System assurance maintenance review.

42. The vulnerability analysis and testing (penetration testing) of systems must be performed by an approved CHECK Team Leader except where the technology to be tested falls outside the testing undertaken by the CHECK Scheme. In the latter case the choice of evaluator needs to be agreed with CESG.

43. The Evaluation Report should summarise the effectiveness of countermeasures in the areas described above. The Evaluation Company must include an Assessment Statement from CESG about the outcome of the evaluation summarising the main points for the Accreditor. The result should not be referred to as a Pass or Fail but offer conclusions where there are serious deficiencies. Ultimately it is the decision of the Accreditor whether to accept such recommendations on behalf of the Customer.

THIS PAGE IS INTENTIONALLY LEFT BLANK

IV. FUNDAMENTAL PRINCIPLES

A. Understanding

Principle: Evaluator understanding (equivalent to that of a product or system designer) of the security architecture, design, implementation, operation and the technical capability of the potential threat agents is the key to gaining assurance.

44. It is an essential factor that the Sponsor shall need to be obliged in any ensuing contract between the Evaluation Company and the Sponsor to provide the design information. To prepare for instances where the Developer (who may not be the Sponsor) provides insufficient documentation or none at all then the Evaluator is advised to ensure that such situations are covered in the ensuing contract and typically this would be through formal recorded discussion.

45. The Evaluation Company is responsible for ensuring that its evaluation staff understand the requirement.

46. CESG shall take the liaison role through contract with the Evaluation Company and:

- be consulted on how the Evaluation could be undertaken
- be consulted on the appropriate level of skills and effort
- be consulted on a suitable Evaluation Work Programme
- be consulted for additional advice and guidance as the evaluation proceeds.

B. Competence

Principle: Evaluators shall be able to demonstrate the necessary experience and skills to perform the required assurance activities.

47. For example, when carrying out source code analysis the Evaluation Company is advised that to be successful then their evaluator must have some experience with:

- the programming language in question
- industry best practice
- causes of common vulnerabilities
- use of appropriate tools

CESG Tailored Assurance Service

- an ability to interpret the results.

C. Objectivity

Principle: Evaluation results shall be obtained with the minimum of subjective judgement or opinion.

48. The Evaluation Company shall ensure that the evaluation is conducted against predetermined documented evaluation criteria that shall have been discussed and agreed with the Sponsor during the evaluation planning stage (see TAS Methodology). Any subjective judgements shall be clearly identified underpinned by salient facts. The Evaluation Report shall also include any identified residual risks and recommendations for how such risks could be satisfactorily resolved.

D. Repeatability

Principle: A repeated evaluation of the same product or system to the same requirements shall (in most cases) yield the same results.

49. This principle is aimed at spreading cost-effective best practice throughout the Evaluation Companies. Typically this would mean that different evaluators would work to the same standards. (ie a common understanding of the TAS Methodology) Thus given the same product or system, Security Target and agreed prioritisation of requirements, different Evaluators would usually obtain the same overall results.

50. For the purposes of clarity the Evaluation Company understands that repeatability does not take precedence over an Evaluation Company's decision to select new approaches that could uncover previously unidentified vulnerabilities.

51. One of the deliverables that the Evaluation Company shall incorporate in any contract with a Sponsor shall be appropriately detailed test records (plans, configurations, procedures, scripts and results) that are to be made available to CESG.

Operating Procedure for Evaluations

E. Prioritisation

Principle: Evaluation activities shall be prioritised to make the best use of available resources

52. The Evaluation Company understands that evaluations will be constrained by time and budget. To demonstrate this understanding, the Evaluation Work Programme shall clearly demonstrate that all reasonable care has been taken to prioritise the agreed activities using available skilled resources.

53. Changes to the prioritisation may only take place through normal Contract Change Control processes and the Evaluation Company shall ensure that such a process is included in any contract with a Customer/Developer.

THIS PAGE IS INTENTIONALLY LEFT BLANK

V. EVALUATION PHASES

54. An evaluation will generally have four phases:

- **Preparation:** Production of Security Target and Evaluation Work Programme.
- **Evaluation:** Evaluation of the IT product or system.
- **Reporting:** Production of the Evaluation Report and CESG Assessment Statement.
- **Maintenance:** Implementation of the Assurance Maintenance Plan.

A. Preparation Phase

55. This phase begins with CESG working either as a sub-contractor to the Evaluation Company or under an SSA with the Customer or in the least likely situation under contract with the Developer. CESG will work with the Customer, Accreditor and the Developer to provide input to the Security Target and the Evaluation Work Programme.

56. Unless agreed otherwise between the Sponsor and the Evaluation Company, the Sponsor arranges for the Security Target to be produced with input from those named above and approved as being suitable and accurate by the Accreditor and CESG. Due regard will be given to the Customer's IT security requirements and the environment in which the IT system or product will be operating. It is advisable that someone familiar with security evaluations (which could be the evaluator) helps produce the Security Target.

57. The Security Target should describe the security architecture of the IT product or system and give a sufficiently clear and detailed description of the product or system so it can be accurately scoped for Evaluation Work Programme purposes. It should also describe threats and assumptions and specify the key security features to be evaluated. For more detail see TAS Methodology.

58. To make effective use of available resources, the Security Target should give prioritisation to the functionality and interfaces that counter the most important threats or that are of most significance in countering threats. For example, they may remove a significant threat rather than just mitigating against it or just protecting against an improbable threat. These functions and interfaces are known as Principal Security Functions and Interfaces. It should be noted that even functions and interfaces not normally considered to carry out a security function can actually be Principal Security Functions and Interfaces if they are exposed to external threats because there are risks related to the use of malformed data and privilege escalation (e.g. from buffer overflow attacks).

CESG Tailored Assurance Service

59. For the Tailored Assurance Service, the assurance activities will also be prioritised in the Security Target, as this is a key feature of the service.

60. An Evaluation Work Programme is to be created by the Evaluation Company and input and contributions will be required by all those named herein i.e. Evaluation Company, CESG, Accreditor, Customer and the Developer. It is important that the Accreditor is able to approve the contents of the Evaluation Work Programme but it shall remain the responsibility of the Evaluation Company to undertake the activities and maintain the Evaluation Work Programme in line with any changes the Evaluation Work Programme may undergo throughout the duration of the Evaluation. This document is normally drafted by the Evaluator and describes the work to be performed in terms of the assurance activities and the relative level of effort required for each activity. TAS Methodology describes the content of an Evaluation Work Programme.

61. If appropriate, an initial version may be prepared by the Sponsor or their consultants to assist with the selection of the Evaluation Company, which will then finalise the Evaluation Work Programme later. The final version is normally produced after the scope of the evaluation and the assurance requirements have been defined in the Security Target.

62. Prior to the start of the evaluation, the Sponsor in consultation with CESG and the Accreditor must agree the Evaluation Work Programme with the Evaluation Company. Where the Developer makes changes to the design of the system that materially affects its IT security or if threats to the system have changed, then the Evaluation Work Programme shall need to be changed. The means of making such change shall be through the TAS Contract Change Control procedure the terms of which the Evaluation Company shall incorporate in its contract with the Sponsor.

63. At defined steps in the Evaluation Work Programme the Evaluation Company must share their findings with CESG, the Accreditor and the Sponsor. Where findings do not accord with the claims in the Security Target then the Evaluator must notify CESG, the Accreditor and Sponsor. The Evaluator shall consult with those named hereto and provide a revised plan that shall be formalised through the aforementioned Change Control procedures. CESG must have the right to initiate changes.

64. The Evaluation Work Programme shall identify the key threats and objectives and the Principal Security Functions and Interfaces in the Security Target as well as ;

- identifying all assurance activities including those that are of lower priority, or have been addressed by other means in the Security Target;
- identifying the emphasis placed on the different activities in the Evaluation Work Programme.

Operating Procedure for Evaluations

65. Where a Security Function or Interface is not considered to be a principal one, the Evaluation Company shall ensure that due diligence is given to assuring the associated security aspects and reflect the effort required in the Evaluation Work Programme.

66. To complete the Preparation Phase, the Security Target and the Evaluation Work Programme need to be approved by all concerned.

67. Following approval of the Evaluation Work Programme, the evaluators must complete the programme of work defined within the Evaluation Work Programme, unless the results of the evaluation suggest some reprioritisation is appropriate. In the latter case, an updated Evaluation Work Programme must be agreed with the Accreditors and CESG.

B. Evaluation Phase

Evaluator Role

68. The evaluation will be based on the Security Target and Evaluation Work Programme and will take due regard of the assurance activities in the TAS Methodology. The evaluator is free to work alongside the Developer to seek out additional supporting evidence and may propose small fixes that can be made during the evaluation (these should be recorded and notified to the Accrerator, Sponsor and CESG). Any significant issues should be reported separately in writing using Critical Observation Reports indicating their severity to the Accrerator, Sponsor and CESG immediately they are identified together with any recommendations for a resolution of the issue and any attendant costs that might accrue.

CESG Role

69. Throughout the evaluation CESG can be placed under contract to provide technical guidance and audit to the Evaluation Company and Accrerator. The nature of CESG's involvement and any key milestones or review points shall be agreed during the Preparation Phase. For example, CESG needs to review the plans for penetration testing, once the design of the IT product or system is understood in detail by the evaluators consequently the contract between CESG and the Evaluation Company should incorporate such activity.

Developer Role

70. During the course of the evaluation, cooperation from the Developer will be important. They (or the Customer) will need to provide some or all of the following, depending on the tailored Evaluation Work Programme and the contract between the Evaluation Company and the Sponsor:

- Assistance in understanding the design and implementation
- Functional specifications and design documents

CESG Tailored Assurance Service

- Access to source code
- The product or system in its appropriate configuration
- Technical support during testing.
- Access to the development environment to audit the development procedures
- Information on any known vulnerabilities
- Installation and operational procedures and evidence that they are implemented correctly
- Access to a test environment built to the conditions declared in the Security Target.

71. Developers should bear in mind that the goal of the evaluators is to be in a position (at the end of the process) where they could explain the design to someone who has limited experience of it, in the presence of someone who has a detailed knowledge of it. Moreover, the principal aim of gaining this understanding is to determine how best to test the security functions and interfaces and to identify any security weaknesses.

72. When the Customer contracts with the Developer, they should make sure the documentation and support listed above is available. A lack of documentation or support is likely to affect the approach to the evaluation or even the assurance that can be achieved. Where warranted by timeliness and risk, draft documentation will be acceptable in the early stages of an evaluation.

Customer and Accreditor Role:

73. The Customer and Accreditor are required to play an active role during the progress of the evaluation, e.g. including the following circumstances:

- Agreement of the Security Target and Evaluation Work Programme
- Issues that could affect the completion date or the assurance achieved
- Priorities that need to be reviewed
- Testing that will be in the operational environment.

74. The Developer is responsible for any resolution of issues identified during the Evaluation Phase and the Evaluation Company is responsible for updating the Evaluation Work Programme.

C. Reporting Phase

Principle: An Evaluation Report will conclude to what extent the claims defined in the Security Target have been met and whether it was possible to test them at the appropriate level of rigour.

75. The Evaluation Company shall ensure that any ensuing contract with a Sponsor has as one of its deliverables an Evaluation Report. The report should summarise the results in plain English, list any security vulnerabilities or major functionality errors, and highlight any additional residual risks and their business impact. Statements in the report regarding risks should make clear their relevance in a system context and identify whether they are generic to the product or due to a specific system configuration.

76. The contents of the report shall not just make pass or fail statements but draw conclusions for each of the assurance activities, any identified risks will be described together with recommendations for mitigation. Any difficulties in drawing conclusions shall be highlighted e.g. where the Developer has not despite the terms of the ensuing contract provided the required information. A description of the Evaluation Report format is provided in TAS Methodology which gives guidance on what should be reported as a minimum for each of the assurance activities. Additional guidance is in TAS Methodology.

77. Detailed evaluation and test records, sufficient to support future assurance maintenance work, must be retained and be available for reuse when required in any future evaluation providing continued maintenance support. Such records must also be made available to CESG.

78. The Evaluation Company shall provide a copy of the Evaluation Report to the Sponsor, Accreditor and CESG. The parties will review the Evaluation Report and report back to the Evaluation Company in writing commenting upon their findings. This is an important part of the process to ensure that there are no misunderstandings.

79. Upon receipt of the final draft of Evaluation Report, CESG will issue an Assessment Statement to the Accreditor and the Customer which will be included in the Evaluation Report. This is an obligation that either the Evaluation Company or HMG Department will have to place upon CESG through a contractual relationship. This statement will confirm to what extent the evaluation has been completed and summarise the significance of the main findings, highlighting any security risks and their business impact. It will describe the connection of the results to IS1 and any additional information that may be required. At this point the Tailored Assurance evaluation of the IT system or product is complete.

80. Unless stated otherwise the Security Target and Evaluation Report will not be publicly released and may have a protective marking.

CESG Tailored Assurance Service

81. In addition to assisting Customers with meeting the requirements of IS1, Customers wishing to comply with the system accreditation requirements of IS2 should note that the Evaluation Report may be a form of 'inspection report' and thus, together with the Security Target, contributes to the requirements for an Accreditation Document Set.

Validity of results

Principle: The results of an evaluation are applicable only to a specific targeted environment.

82. The Evaluation Work Programme and the Security Target will define the scope of the evaluation. If a system or product needs to be used for a different application or in other environments, then it is quite likely that a re-evaluation will be required. This is because the nature of the prioritisation and scoping decisions taken may no longer be valid and because residual risks may not be acceptable.

83. In some instances there may be a requirement for the evaluator to investigate the potential consequences of the product or system being used outside the defined configuration.

84. System evaluations will only be valid for one customer. The exception to this rule is where a Developer offers a solution that can be shared amongst a number of Customers. In such instances the approach and residual risks still need to be accepted by the appropriate Accreditors (e.g. through a joint accreditation panel).

D. Maintenance Phase

Principle: Ongoing assurance in a product or system is important and should be considered wherever possible when using the Tailored Assurance Service.

85. In the majority of cases, products will be modified and patched and systems will be updated and reconfigured continuously. Also, previously unknown vulnerabilities may come to light. Furthermore configuration errors can happen with time.

86. Therefore most evaluated IT products and systems should undergo some form of assurance maintenance while they remain in use.

87. Thus after an IT system/product has undergone a Tailored Assurance evaluation, the Customer is advised by CESG to maintain the assurance. The Customer needs to contract with the same or a different Evaluation Company for the maintenance phase.

88. CESG involvement must also be contracted either through an SSA with the HMG Department or through the Evaluation Company.

Operating Procedure for Evaluations

E. Assurance Maintenance Plan

89. The means of achieving continued assurance in the product or system is through an Assurance Maintenance Plan (AMP). An example AMP is provided in the AMP Template see TAS Methodology. It is recommended that this plan is produced during the initial evaluation of the IT system or product. The selected Evaluation Company is responsible for creating and updating the AMP with input from CESG, the Accreditor and the Sponsor.

90. The plan needs to be regularly reviewed by CESG, the Accreditor and the Customer in the light of changing threats to the IT system or product and changes to the IT system or product itself.

91. Maintenance may typically involve an Evaluation Company in a scheduled security audit of any changes and (for systems) an IT Health Check 6 or 12 months after completion of evaluation, with CESG guidance as appropriate. It may also involve CESG and/or the Evaluation Company in a review of any proposed major update during the year to check the security impact.

92. To facilitate the maintenance audits, the Customer will need to supply the evaluators with the updated evidence (design information, security impact analysis etc) and access to the updated IT product or system.

93. Significant changes or additions to security functions, interfaces and components are likely to require re-evaluation to re-establish appropriate assurance. If the requirement for re-evaluation is agreed by the Accreditor and Customer, then the relevant assurance activities needed to address the changes since the previous evaluation should normally be repeated under a separate evaluation task, reusing any previous maintenance or evaluation results as appropriate.

THIS PAGE IS INTENTIONALLY LEFT BLANK

APPENDIX A : TOP LEVEL RESPONSIBILITIES

Customer

Decides to procure IT product or system.

Commissions a threat assessment for the IT product or system.

Contracts IT product or system to be evaluated under the Tailored Assurance Service.

Agrees Evaluation Work Programme with CESA and Accreditor.

Accepts evaluated product or system.

Arranges any user corrective actions for Critical Observation Reports (COR).

Implements Assurance Maintenance Plan.

Accreditor:

Reviews the threat assessment and decides its fitness for purpose.

Prioritises the principal security functions and evaluation activities

Agrees Evaluation Work Programme with CESA and Sponsor.

Reviews the Security Target including scope of evaluation and decides its fitness for purpose.

Advises on resolution of CORs

Decides with CESA whether to change Evaluation Work Programme.

Receives the CESA Audit Statement on the outcome of the evaluation and uses it as input to the accreditation process.

Reviews the Assurance Maintenance Plan.

CEA Security Consultant

Reviews the threat assessment.

Agrees Evaluation Work Programme with Accreditor and Sponsor.

Reviews the Security Target and decides its fitness for purpose.

Reviews the Evaluation Work Programme and decides its fitness for purpose.

Approves the evaluators proposed by the Evaluation Company.

Approves Specialist Evaluation Company where one is required.

Monitors the evaluation, discusses technical issues with the evaluator and witnesses penetration tests.

Advises on resolution of CORs.

Decides with Accreditor whether to change Evaluation Work Programme and reprioritise activities.

Reviews the Evaluation Report in draft form.

Produces the CESA Assessment Statement on the outcome of the evaluation.

Reviews the Assurance Maintenance Plan.

System or Product Developer:

Provides access to design information and source code and negotiates access to third party intellectual property where necessary.

Either produces the Security Target or facilitates its preparation by the evaluator.

Provides clarification on CORs.

CESG Tailored Assurance Service

Implements changes to system or product to mitigate vulnerabilities found during the evaluation.

Produces the Assurance Maintenance Plan or facilitates its preparation by the Evaluator.

Evaluator:

Produces the Security Target if requested.

Produces and maintains the Evaluation Work Programme.

Identifies candidate Specialist Evaluation Company where needed.

Conducts the evaluation.

Maintains a comprehensive technical record of evaluation activities and observations.

Identifies design and/or implementation issues that would prevent achievement of the Security Target (or are highly likely to do so) and promptly issues Critical Observation Reports (CORs) to document these to the Accreditor, Developer and CESG.

Holds the master copies of CORs and documents their resolution.

Produces the Evaluation Report.

Prepares the Assurance Maintenance Plan if requested

Conducts the Maintenance Reviews

Produces the Maintenance Reports

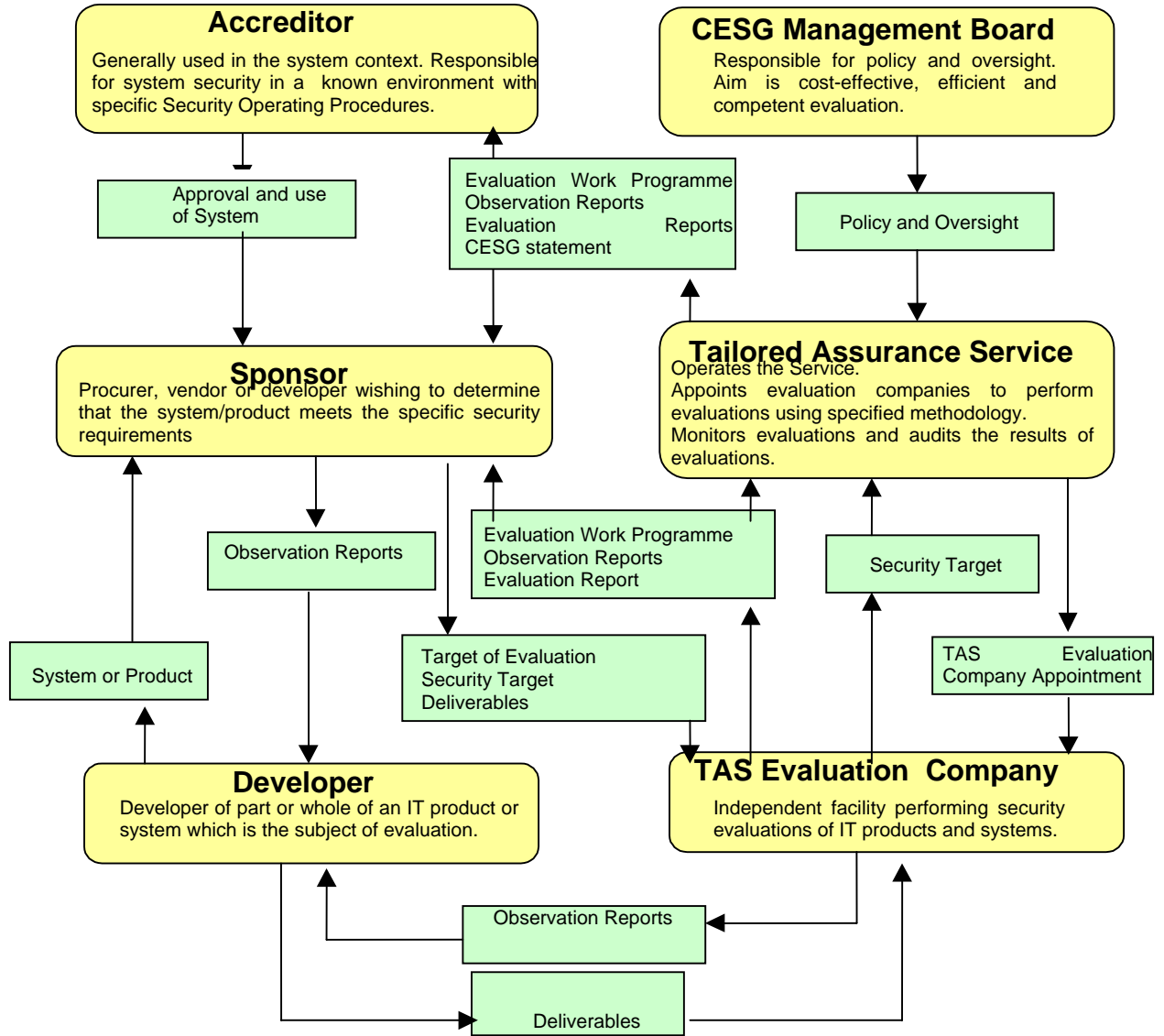
Head of the Tailored Assurance Service

Accepts a product or system for evaluation under the scheme.

Approves release of the CESG Assessment Statement.

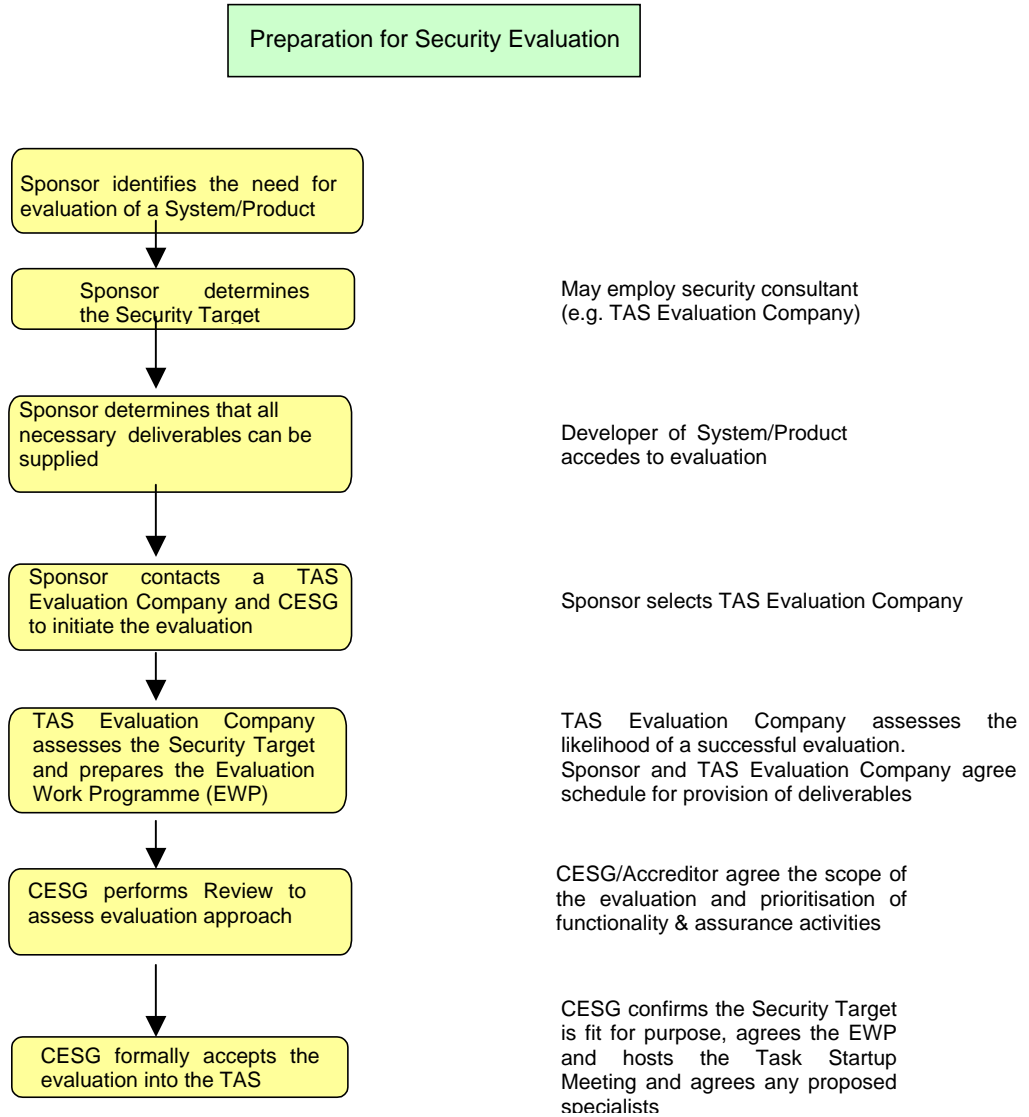
Directs cessation or redirection of evaluation work if advised by the Accreditor and the CESG Security Consultant that evaluation activities are no longer addressing the known critical IA issues.

APPENDIX B: ORGANISATION AND MANAGEMENT CONTEXT

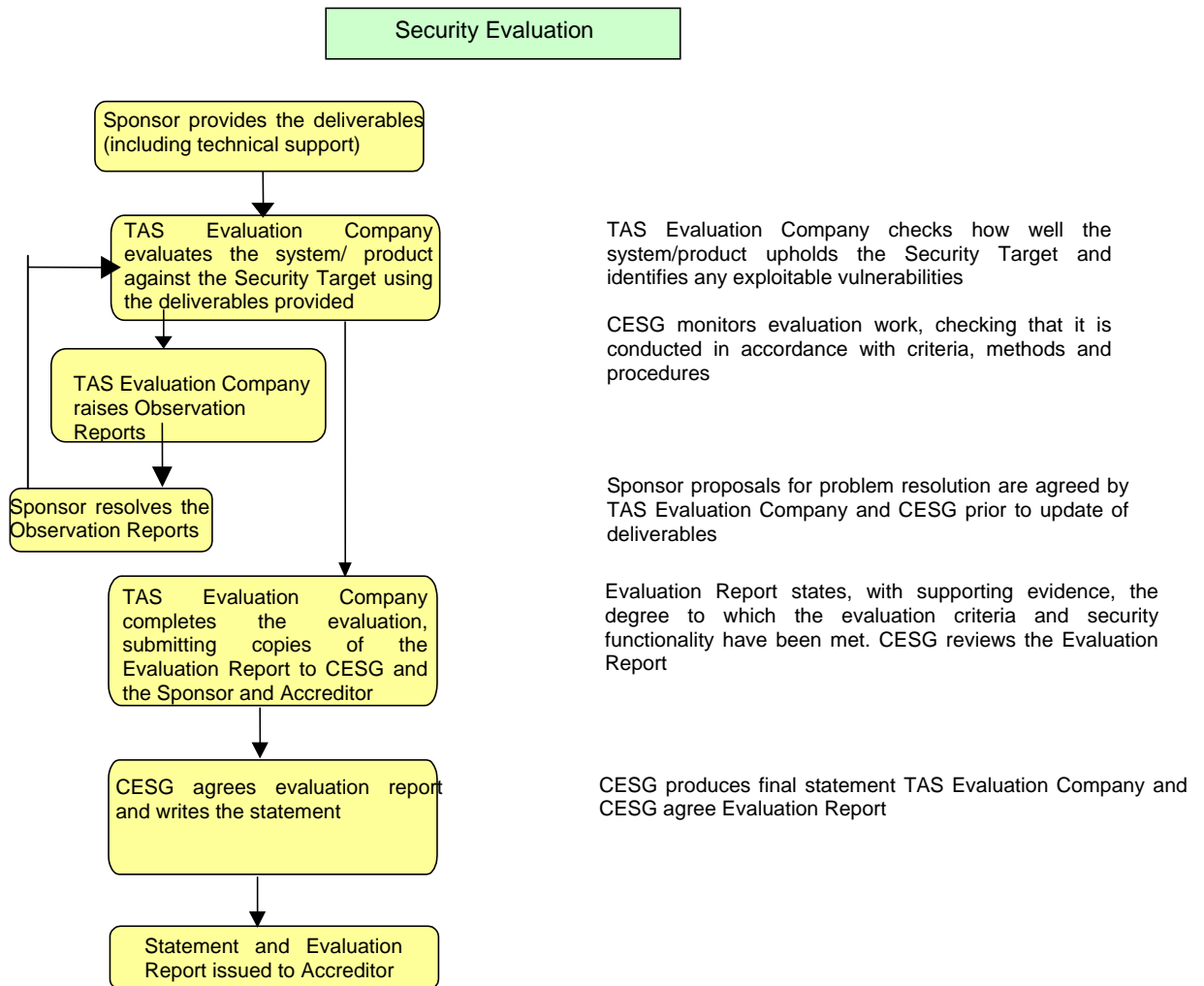


CESG Tailored Assurance Service

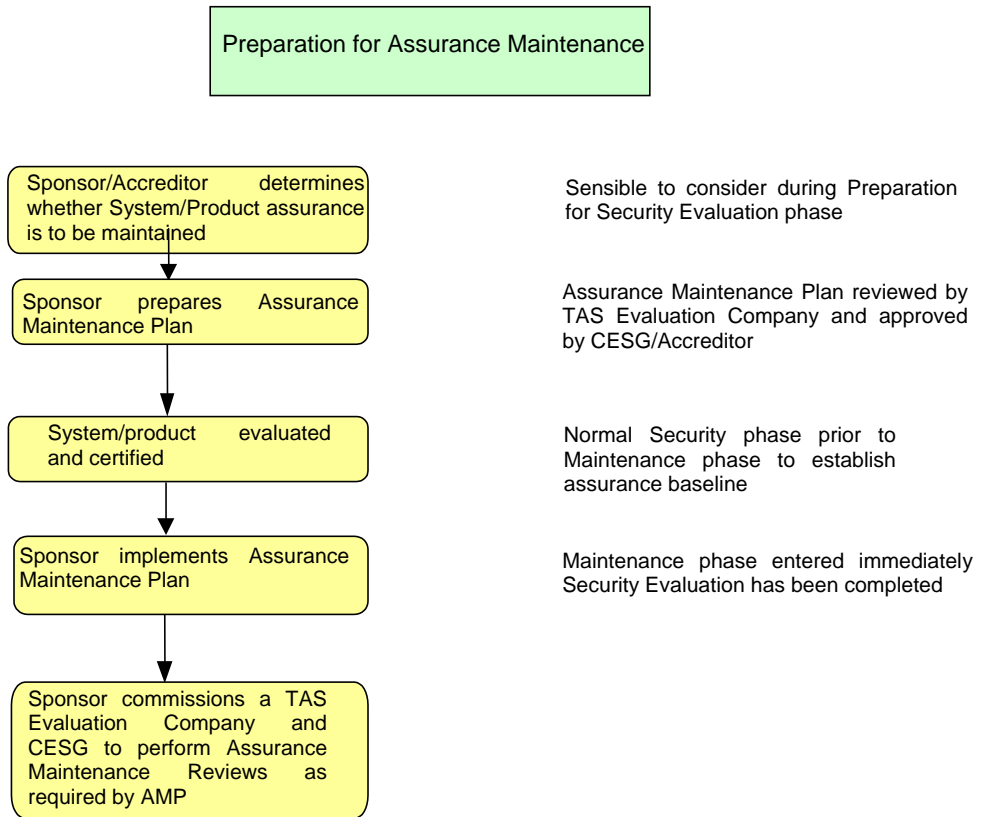
SECURITY EVALUATION ACTIVITIES



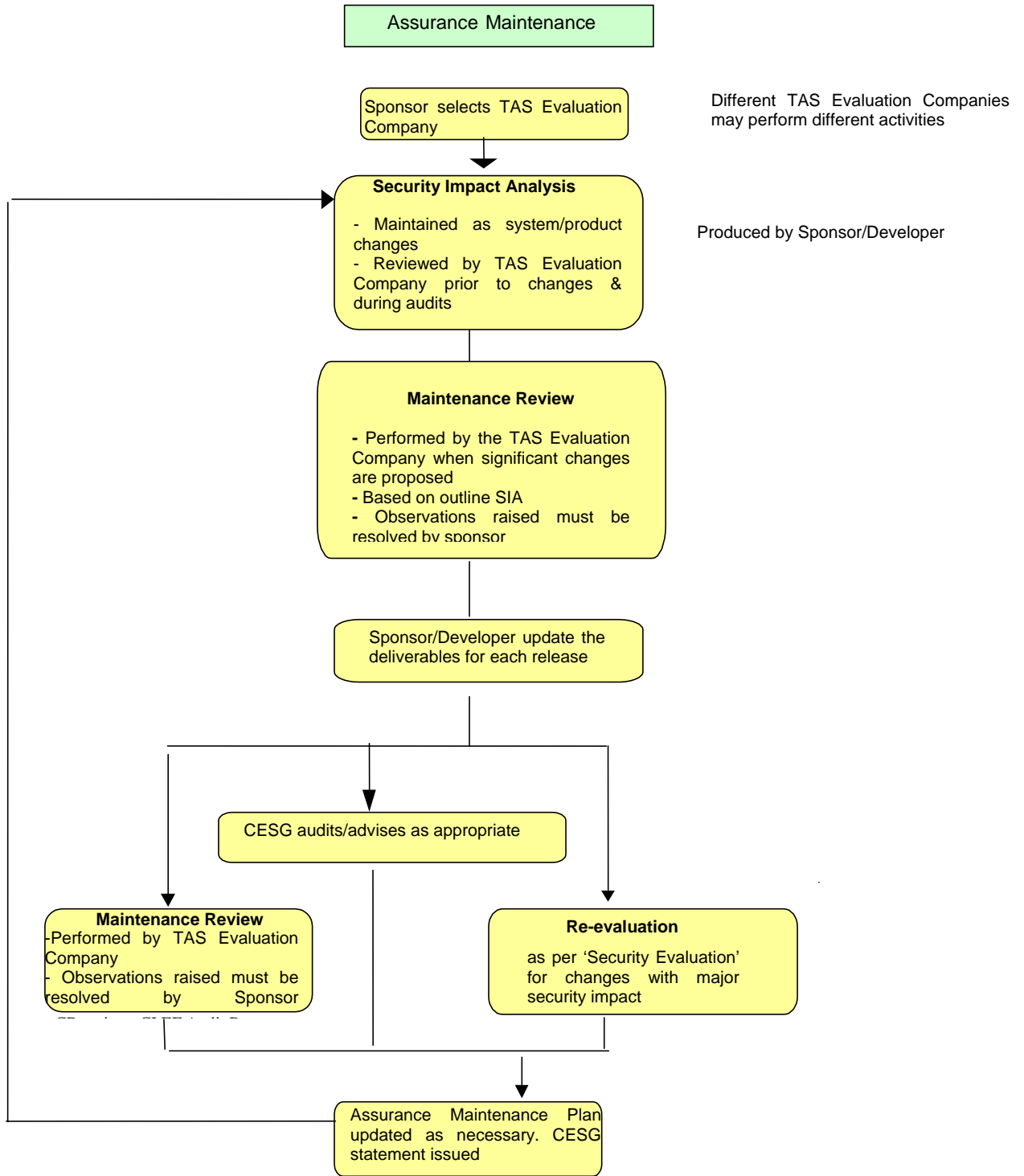
Operating Procedure for Evaluations



CESG Tailored Assurance Service



Operating Procedure for Evaluations



Different TAS Evaluation Companies may perform different activities

Produced by Sponsor/Developer

Maintenance Review usually performed after 6 months then annually

Re-evaluation performed in accordance with AMP schedule or earlier for major security changes

THIS PAGE IS INTENTIONALLY LEFT BLANK

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

Operating Procedures for Evaluations

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 Operating Procedure for Evaluations, Version 1.0
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)