D R A F T

Common Evaluation Methodology for Information Technology Security

CEM-97/017

Part 1 :
Introduction and general model

Version 0.6

97/01/11

D R A F T

Foreword

Following publication of the Common Criteria for Information Technology Security Evaluation version 1.0, this document provides the first version of the principles and model of the Common Evaluation Methodology, needed to apply the Common Criteria.

This document is issued for review by the international security community. All the comments received will be considered for further development of the Common Evaluation Methodology

Any observation reports should be communicated to the CEM point of contact (cem@cse.dnd.ca) or to one or more of the following points of contact at the sponsoring organisations, using the template for reporting observations included in annex B of this document :

National Institute of Standards and Technology
Computer Security Division
NIST North Building, Room 426
Gaithersburg, Maryland 20899
U.S.A.
Tel: (+1)(301)975-2934, Fax:(+1)(301)926-2733
E-mail:csd@nist.gov
http://csrc.ncsl.nist.gov

National Security Agency
Attn: V2, Common Criteria Technical Advisor
Fort George G. Meade, Maryland 21122
U.S.A.
Tel: (+1)(410)859-4458, Fax:(+1)(410)684-7512
E-mail: common_criteria@radium.ncsc.mil

Communications Security Establishment
Criteria Coordinator
R2B IT Security Standards and Initiatives
P.O. Box 9703, Terminal
Ottawa, Canada K1G 3Z4
Tel:(+1)(613)991-7409, Fax:(+1)(613)991-7411
E-mail:criteria@cse.dnd.ca
ftp:ftp.cse.dnd.ca
http://www.cse.dnd.ca

UK IT Security and Certification Scheme
Senior Executive
P.O. Box 152
Cheltenham GL52 5UF
United Kingdom
Tel: (+44) 1242 235739, Fax:(+44)1242 235233
E-mail: ccv1.0@itsec.gov.uk
ftp: ftp.itsec.gov.uk
http://www.itsec.gov.uk

Bundesamt für Sicherheit in der Informationstechnik
Abteilung V
Postfach 20 03 63
D-53133 Bonn
Germany
Tel: (+49)228 9582 300, Fax:(+49)228 9582 427
E-mail:cc@bsi.de

Service Central de la Sécurité des Systèmes d'Information
Bureau Normalisation, Critères Communs
18 rue du docteur Zamenhof
92131 Issy les Moulineaux
France
Tel: (+33)(1)41463784, Fax:(+33)(1)41463701
E-mail:106174.1363@compuserve.com

Netherlands National Communications Security Agency
P.O. Box 20061
NL 2500 EB The Hague
The Netherlands
Tel: (+31) 70 3485637, Fax:(+31).70.3486503
E-mail: criteria@nlncsa.minbuza.nl

This document is paginated from i to iv and from 1 to 24

D R A F T

Table of contents

Chapter 1
Introduction 1

1.1 Objective 1
1.2 Target audience 1
1.3 Interested parties and expected benefits 1
1.4 Scope 3
1.5 Document organisation 3
1.6 Document conventions and terminology 4

Chapter 2
Universal principles of evaluation 5

2.1 Statement and discussion of universal principles 5
2.1.1 Appropriateness 5
2.1.2 Impartiality 5
2.1.3 Objectivity 5
2.1.4 Repeatability and reproducibility 6
2.1.5 Soundness of results 6
2.2 Assumptions 6
2.2.1 Cost-effectiveness 6
2.2.2 Methodology evolution 6
2.2.3 Re-usability 6
2.2.4 Terminology 7

Chapter 3
General model 9

3.1 Responsibilities of the roles 9
3.1.1 Sponsor 9
3.1.2 Developer 9
3.1.3 Evaluator 10
3.1.4 Overseer 10
3.1.5 Relationship of the roles 10
3.2 Evaluation process overview 12
3.2.1 Preparation 12
3.2.2 Conduct 14
3.2.3 Conclusion 16

Annex A
Glossary 19

A.1 Abbreviations and acronyms 19
A.2 Vocabulary 19
A.3 References 22

D R A F T

Annex B
CEM observation report (CEMOR) 23

B.1 Introduction 23
B.2 Forwarding a CEMOR 23
B.3 Format of a CEMOR 23
B.3.1 Example observations: 24

D R A F T

List of figures

Figure 1.1 - Key parties to the security evaluation process 2
Figure 1.2 - Evaluation framework 3
Figure 3.1 - Responsibilities and relationships of the roles 11
Figure 3.2 - Preparation stage 13
Figure 3.3 - Conduct stage 15
Figure 3.4 - Conclusion stage 17

D R A F T

List of tables

Table 3.1 - Undue influence permitted between roles during a single evaluation 11

D R A F T

Chapter 1

Introduction

1.1 Objective

1 This document, the Common Evaluation Methodology (CEM), has been prepared in order to develop an agreed **methodology** for conducting evaluations which apply the Common Criteria (CC, [CCREF]). The CEM supports the mutual recognition of security **evaluations**[1].

1.2 Target audience

2 The CEM is aimed primarily at **evaluators**. However, other parties will also gain useful information from the CEM, these include **developers**, **sponsors**, **overseers**, and parties involved in publishing and using evaluation results.

Editor Note : The CEMEB recognises that the term Overseer is awkward and invites suggestions for a better word.

1.3 Interested parties and expected benefits

3 A **Protection Profile** (PP) developer (author) is likely to be a group of user representatives or a vendor of an Information Technology (IT) product. The PP developer will benefit from the application of the CEM in that PP evaluation will be performed consistently and that the PP will be independently validated.

4 A **Target of Evaluation** (TOE) developer may be a vendor of an IT product, a system integrator who incorporates IT products into systems, or any other form of organisational entity which produces IT solutions. A TOE developer will benefit from the application of the CEM in that:

a) the security characteristics documented in the PP and **Security Target** (ST) will have been independently validated and verified;

b) the developer's customers will be more easily convinced that the TOE delivers the security characteristics claimed;

c) evaluated products may be used more effectively in composing secure systems;

d) the CEM contributes to cost-effective and timely evaluations.

1. Vocabulary definitions are provided in Annex A for terms presented in bold face type on first use.

D R A F T

5 A sponsor of an evaluation is the organisational entity that commissions an evaluation. A sponsor can be a developer (e.g. vendor or integrator) or consumer (e.g. user, accreditor, system custodian, system security officer). The sponsor will benefit from the application of the CEM in that the security characteristics of the TOE will have been documented and independently validated and verified, thus enabling comparison between TOEs.

6 An evaluator applies the CC in conformance to the CEM. An evaluator will benefit from the CEM in that it will offer specific guidance on consistent application of the CC.

7 An overseer is the entity that assures that the **evaluation process** is conducted in accordance with the CC and the CEM. The overseer will benefit from the CEM as it defines a consistent set of information to be provided by the evaluator.

8 Figure 1.1 illustrates the key parties to the security evaluation process. All parties will benefit from the CEM in that it supports mutual recognition.

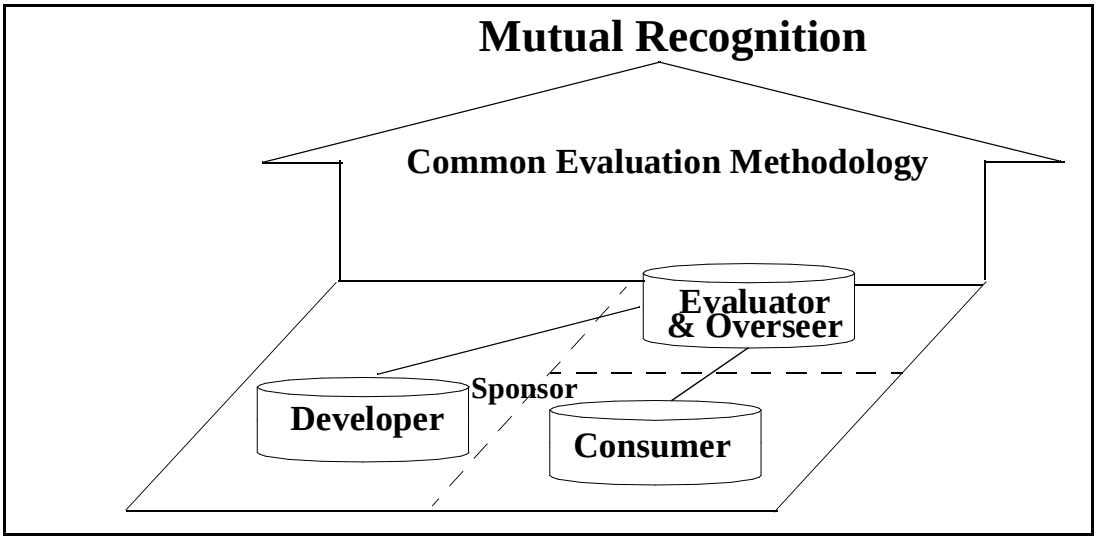

Figure 1.1 - Key parties to the security evaluation process

D R A F T

1.4 Scope

9 The evaluation process consists of the actions to be performed during the evaluation together with those of the development process and the oversight process necessary to comply with the evaluation methodology. There are actions within the development and oversight processes which are outside the scope of both the evaluation process and the CEM. Figure 1.2 illustrates the scope of the evaluation framework which is covered by this document.

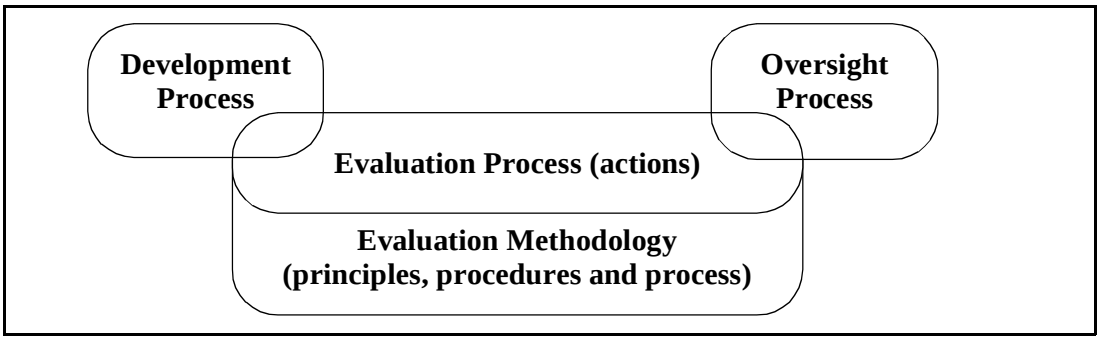

Figure 1.2 - Evaluation framework

10 This document will address the principles, procedures and processes (actions) that apply to IT security evaluation. It will not address the national or local implementation of these rules (i.e. the **scheme**).

1.5 Document organisation

11 This document is structured into three parts. This part, Part 1, introduces the principles and general model of evaluation. The intention is that should an aspect of evaluation not be fully covered by the CEM, reference to the principles of evaluation should provide valuable guidance in determining a course of action.

12 The schemes adopting this methodology will be required to enforce the implementation of the normative **elements** of Part 2. The implementation of the schemes will need to be upheld against the universal principles of evaluation introduced in Part 1.

13 Part 2 describes the evaluation process by refining the actions mandated by Part 3 of the CC. It will address the activities of the different parties involved, and the description of the evaluation process will describe the actions to be performed during the development process and the oversight process to comply with the evaluation methodology.

D R A F T

14 Part 3 describes extensions to the evaluation methodology in order to make full use of evaluation results. For instance, Part 3 includes guidance on content of **evaluation deliverables** and requirements definition.

1.6 Document conventions and terminology

15 Abbreviations and acronyms, presented in Annex A.1 of this part, are introduced on first use. References to sections of text and figures are made as required. References to other documents are provided using abbreviations to identify the referenced material. A full reference list is presented in Annex A.3 of this part.

16 Glossary definitions are presented in bold face type when introduced in this document. The Glossary definitions, presented in Annex A.2 of this part, are provided for only those terms which are used in a specialised way within this document. The majority of terms are used according to their accepted definitions.

17 The verbal forms *shall* and *shall not* are used to indicate requirements that must be followed strictly in order to conform to the CEM.

18 The verbal forms *must* and *must not* are used within requirements to describe an unavoidable situation.

19 The verbal forms *should* and *will* are used to indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required; or that (in the negative form *should not*) a certain possibility or course of action is deprecated but not prohibited within the CEM.

20 The verbal forms *may* and *need not* are used to indicate a course of action permissible within the limits of the CEM. The verbal forms *can* and *cannot* are used for CEM statements of possibility and capability, whether material, physical or causal.

D R A F T

Chapter 2

Universal principles of evaluation

21 The universal principles of evaluation are introduced in this chapter. These principles are the foundation for evaluation. Evaluation methodology alone does not enforce the principles. Assumptions on the parties involved in evaluation and the scheme managing the application of this methodology must also contribute to the enforcement of the principles.

2.1 Statement and discussion of universal principles

22 This section states the universal principles of evaluation. In each subsection, the principle is stated and is followed by a brief discussion.

2.1.1 Appropriateness

23 Principle: The evaluation activities employed in achieving an intended level of assurance *shall be appropriate*.

24 All parties involved in an evaluation shall perform their required tasks to a degree of rigor consistent with the guidance and requirements of the target **Evaluation Assurance Level** (EAL).

2.1.2 Impartiality

25 Principle: All evaluations *shall be free from bias*.

26 No party involved in evaluation shall have bias toward/against any Target of Evaluation (TOE) or Protection Profile (PP) being evaluated. Proper technical oversight coupled with a scheme that eliminates conflicts of interest should reduce to a nominal level any residual bias. Mutual recognition and the scheme must address in detail the concept of unacceptable conflict of interest.

2.1.3 Objectivity

27 Principle: Evaluation results *shall be obtained* with a minimum of subjective judgement or opinion.

28 Individuals cannot be totally free of opinion or judgements. Proper technical oversight based on well defined methodology and **interpretations** should reduce opinions and judgments to an acceptable level.

D R A F T

2.1.4 Repeatability and reproducibility

29 Principle: The repeated evaluation of the same TOE or PP to the same requirements with the same **evaluation evidence** *shall yield the same results*.

30 The results of each **evaluator action element** should yield the same result regardless of who performs the evaluation. Requirements should be interpreted in a consistent manner across evaluations. Reproducibility differs from repeatability in that the former is concerned with consistency across evaluators, and the latter is concerned with the consistency of results by the same evaluators.

2.1.5 Soundness of results

31 Principle: The results of evaluation *shall be complete* and technically correct.

32 The output of evaluation shall demonstrate good judgement and an accurate technical assessment of the TOE or PP. The evaluation process and results should be subject to technical oversight to ensure that the requirements of the CC, CEM, and scheme are met.

2.2 Assumptions

33 Underlying the universal principles are a number of assumptions with respect to the environment of the evaluation and the activities of all parties involved. The principles depend on the validity of these assumptions.

2.2.1 Cost-effectiveness

34 Assumption: The value of an evaluation should offset the time, resources, and money expended by all interested parties.

35 A balance must continually be maintained between value, and expenditure of time and resources in the evaluation of TOEs and PPs.

2.2.2 Methodology evolution

36 Assumption: The impact of changing environmental and technical factors on evaluations should be reflected into the evaluation methodology in a well-considered and consistent manner.

37 Changing environments and evolving technology may impact the effectiveness of the techniques that are used to evaluate a TOE or PP. Additionally, the evaluation methodology must take the environment into account and be applicable to evolving technology to ensure the fitness for purpose of the evaluated TOE or PP.

2.2.3 Re-usability

38 Assumption: Evaluations should make effective use of previous evaluation results.

39 The results of evaluating a TOE or PP, and the interpretations that arise in the course of the evaluation, are useful in subsequent evaluations if the same conditions apply. Re-usability is especially useful for evaluations where the evaluated TOE or PP is incorporated into another TOE or PP. The content and structure of evaluation results and the evaluation methodology should support re-usability.

2.2.4 Terminology

40 Assumption: A common nomenclature should be used by all parties involved in evaluation.

41 To ensure consistent technical quality of evaluation results and to provide a consistent basis of understanding and communication across evaluations, all interested parties must share a common nomenclature and a common understanding of what terms mean in practice.

D R A F T

D R A F T

Chapter 3

General model

42 This chapter presents the general model of the methodology and identifies:

a) roles and responsibilities of the parties involved in the evaluation process;

b) a high-level evaluation process including a high-level characterization of evaluation results.

43 The general model does not prescribe any particular scheme; however, it includes requirements that any scheme should comply with to satisfy mutual recognition of an evaluation.

3.1 Responsibilities of the roles

44 The general model defines the following roles: sponsor, developer, evaluator, and overseer. Each role has responsibilities identified within the methodology. The general model does not preclude an organisation or other entity from assuming one or more roles, subject to adherence to the universal principles, specifically the universal principle of impartiality. A scheme may impose additional requirements to ensure compliance with national laws and regulations.

3.1.1 Sponsor

45 The responsibilities of the sponsor include:

a) establishing the necessary agreements for evaluation (e.g. commissioning the evaluation);

b) assuring that the evaluator is provided with evaluation deliverables (e.g. evaluation evidence, training, and support).

3.1.2 Developer

46 The responsibilities of the developer include:

a) supporting the evaluation;

b) developing and maintaining evaluation evidence.

D R A F T

3.1.3 Evaluator

47 The responsibilities of the evaluator include:

a) receiving the evaluation evidence (e.g. documentation, PP, ST, a copy of the TOE);

b) performing the evaluator actions required by the CC;

c) requesting and receiving evaluation support as needed (e.g. training by the developer, interpretations by the overseer);

d) providing the **oversight deliverables**;

e) documenting and justifying the **overall verdict** and any **interim verdicts** to the overseer;

f) complying with the universal principles and the relevant scheme.

3.1.4 Overseer

48 The responsibilities of the overseer include:

a) monitoring evaluations as required by the scheme;

b) receiving and reviewing oversight deliverables;

c) creating conditions that assure that evaluations conform to the universal principles and implement the CEM;

d) supporting evaluations by providing scheme and criteria interpretation and guidance;

e) approving or disapproving the overall verdict;

f) documenting and justifying the **oversight verdict** to the evaluation authority.

3.1.5 Relationship of the roles

49 This section includes a figure and a table describing the relationship between the roles. Figure 3.1 summarizes the responsibilities of each of the roles and the relationship between the roles.

50 Table 3.1 describes the required separation of the roles from the perspective of undue influence on a single evaluation. Undue influence is defined as a violation of the universal principles by any individual fulfilling a role on a single evaluation. A “No” at the intersection of a row and a column indicates that the role of that row is not permitted to unduly influence the role of that column.

D R A F T

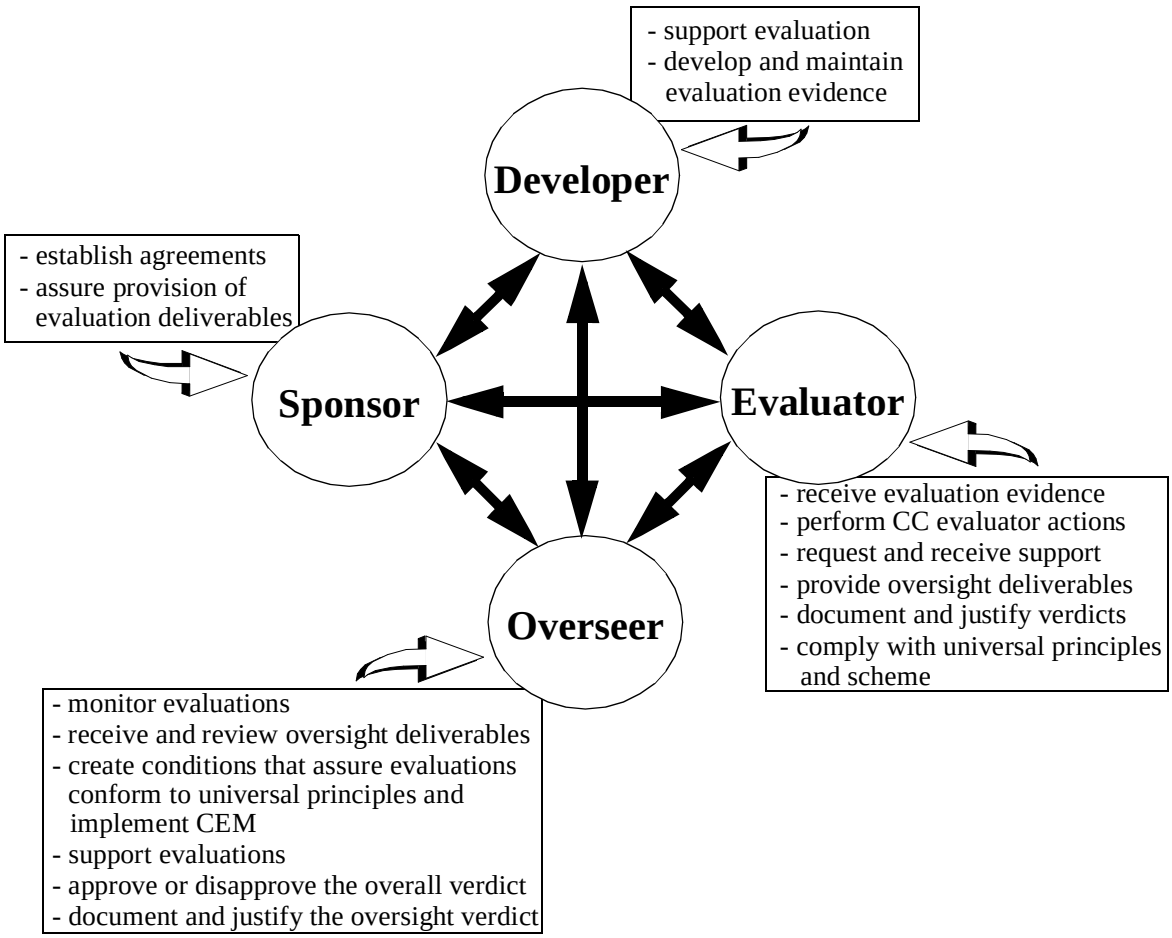

Figure 3.1 - Responsibilities and relationships of the roles

Table 3.1 - Undue influence permitted between roles during a single evaluation

	Developer	Sponsor	Evaluator	Overseer
Developer		Yes	No	No
Sponsor	Yes		No	No
Evaluator	No	No		No
Overseer	No	No	No	

D R A F T

3.2 Evaluation process overview

51 The following is a high-level overview of the evaluation process under the CEM. The evaluation process can be divided into three stages which may overlap:

a) preparation - in this stage initial contact is made between the sponsor and the evaluator;

b) conduct - in this stage the evaluation is performed;

c) conclusion - in this stage the evaluation results are delivered.

52 The interactions between these roles during each stage of evaluation are described in the following sections.

3.2.1 Preparation

53 In the preparation stage (see Figure 3.2), the sponsor approaches the relevant party within the scheme to initiate the evaluation of a PP or a TOE. The sponsor supplies the evaluator with the PP or the ST. The evaluator performs a feasibility analysis to assess the likelihood of a successful evaluation, requesting relevant information from the sponsor. The sponsor or the developer supplies the evaluator with a subset of evaluation deliverables (possibly in draft form). The evaluator may review the PP or the ST and advise the sponsor about changes needed to assure a firm basis for the evaluation. If the scheme requirements for evaluation are satisfied, the evaluation will proceed to the next stage.

54 The feasibility output should include the list of the evaluation deliverables, an ordered list of evaluation activities and information about sampling requirements in the CC will be addressed (e.g. ATE_IND). The feasibility output should be agreed to by all roles. The details of the feasibility output depend on a variety of factors, particularly on whether the evaluation is of a PP or of a TOE. All roles are responsible for identifying and protecting proprietary information.

55 In accordance with the scheme, the sponsor and the evaluator typically sign an agreement during this stage to define the framework of the evaluation. The agreement takes account of constraints imposed by the scheme and of national laws and regulations as applicable.

D R A F T

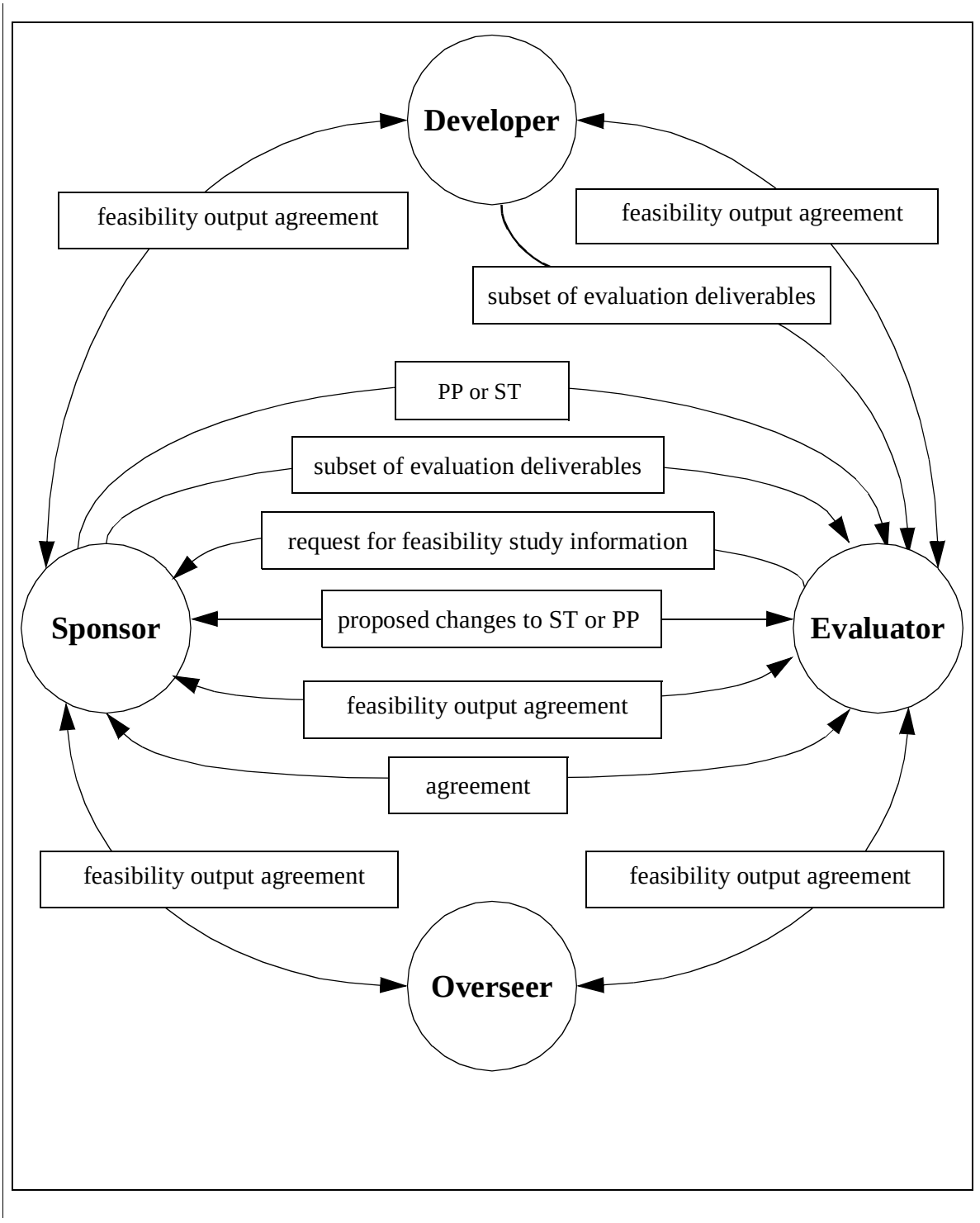

Figure 3.2 - Preparation stage

D R A F T

3.2.2 Conduct

56 The conduct stage is the main part of the evaluation process (see Figure 3.3). During the conduct stage, the evaluator reviews the evaluation deliverables received from the sponsor or developer and performs the evaluator actions required by the assurance criteria.

57 During the evaluation, the evaluator may generate **observation reports**. The evaluator may request clarification on the application of a requirement from the overseer using an observation report. This request could result in an interpretation of a requirement to ensure consistent application of the requirement in future evaluations. The evaluator may also use the observation report to identify a potential vulnerability or deficiency and to request additional information from the sponsor or the developer. The distribution of the observation reports may be further specified in the scheme.

58 The overseer monitors the evaluation as required by the scheme. The evaluator produces the **Evaluation Technical Report** (ETR) which contains the overall verdict and the justification for the verdict.

D R A F T

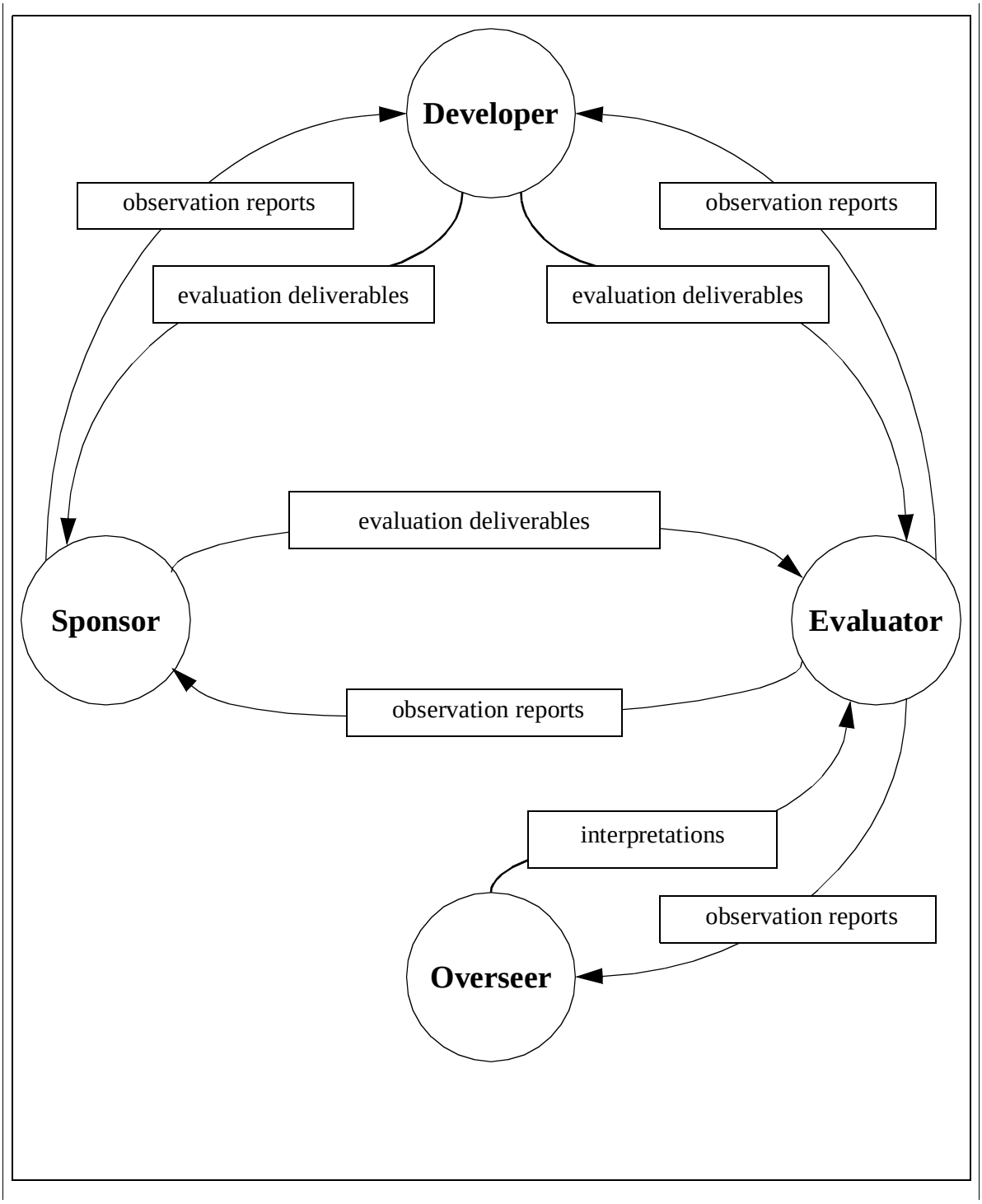

Figure 3.3 - Conduct stage

D R A F T

3.2.3 Conclusion

59 In the conclusion stage (see Figure 3.4), the evaluator delivers the ETR to the overseer. Requirements for controls on handling the ETR are established by the scheme which may include delivery to the sponsor or developer. The ETR may include sensitive or proprietary information and may need to be sanitised before it is given to the sponsor since the sponsor may not have access to developer proprietary data.

60 The overseer reviews and analyses the ETR to assess conformance to the CC, CEM, and scheme requirements. The overseer makes a decision to agree or disagree with the overall verdict in the ETR (oversight verdict), and prepares an **Evaluation Summary Report** (ESR). The overseer uses the ETR as the primary input to the ESR. The evaluator could be required to provide technical support and/ or guidance on nondisclosure requirements to the overseer for the preparation of the ESR.

61 At the end of the conclusion stage, the overseer delivers the ESR to the evaluation authority. The sponsor, developer and the evaluator should have the right to review the ESR to ensure its releasability to the evaluation authority.

D R A F T

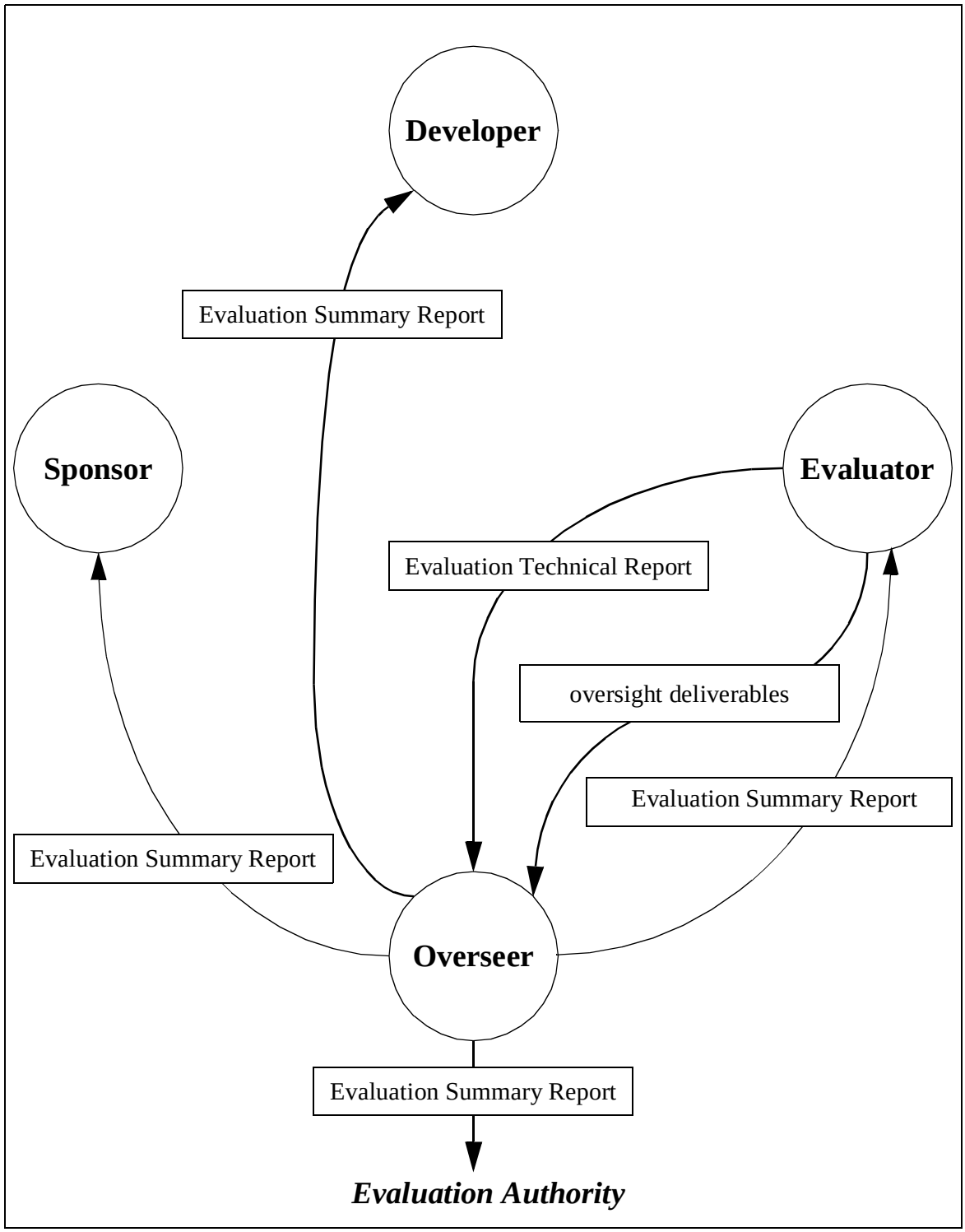

Figure 3.4 - Conclusion stage

D R A F T

Annex A

Glossary

62 In this annex, abbreviations and acronyms, vocabulary and references used in this part are presented.

A.1 Abbreviations and acronyms

63 CC Common Criteria

64 CEM Common Evaluation Methodology

65 EAL Evaluation Assurance Level

66 ESR Evaluation Summary Report

67 ETR Evaluation Technical Report

68 IT Information Technology

69 PP Protection Profile

70 ST Security Target

71 TOE Target of Evaluation

A.2 Vocabulary

72 Vocabulary which are presented in bold faced type are themselves defined in this section. If the vocabulary is defined in another document (e.g., the CC), the definition is quoted verbatim unless otherwise noted, and the source is noted in brackets at the end of the definition.

73 Deliverable:

see **evaluation deliverable** and **oversight deliverable**.

74 Developer:

refer to Chapter 3.1, section 3.1.2.

D R A F T

75 Element:

an indivisible security requirement. [CCREF]

76 Evaluation:

the assessment of a PP or TOE against defined evaluation criteria.

77 Evaluation Assurance Level:

a pre-defined set of assurance components from Part 3 (of the CC) that represent a point on the CC assurance scale. [CCREF]

78 Evaluation Authority:

the body responsible for the business application of the evaluation results. Its activities are outside the scope of the CEM, but include such things as issuing “certificates”, making mutual recognition agreements and defining scheme rules such as “licensing” commercial facilities.

79 Evaluation Deliverable:

any resource required from the **sponsor** or **developer** by the **evaluator** or **overseer** to perform one or more **evaluation** or oversight activities.

80 Evaluation Evidence:

a tangible **evaluation deliverable**.

81 Evaluation Process:

a set of actions performed by the parties in order to conduct an IT security **evaluation**.

82 Evaluation Result:

Editor Note: this term is used in a generic sense only.

83 Evaluation Summary Report:

a report issued by an **overseer** and submitted to an evaluation authority that documents the **oversight verdict** and its justification.

84 Evaluation Technical Report:

a report produced by the **evaluator** and submitted to an **overseer** that documents the **overall verdict** and its justification.

D R A F T

85 Evaluator:

refer to Chapter 3.1, section 3.1.3.

86 Evaluator Action Element:

an assurance requirement stated in the CC that represents a TOE **evaluator**'s responsibilities in verifying the security claims made in the TOE's **security target**. [CCREF]

87 Interim Verdict:

a "pass", "fail" or "inconclusive" statement issued by an **evaluator** with respect to one or more requirements.

88 Interpretation:

a clarification or amplification of a CC, CEM or **scheme** requirement.

89 Methodology:

the system of principles, procedures and processes applied to IT security **evaluations**.

90 Observation Report:

a report written by the **evaluator** requesting a clarification or identifying a problem during the **evaluation**.

91 Overall Verdict:

A "pass" or "fail" statement issued by an **evaluator** with respect to the result of an **evaluation**.

92 Overseer:

refer to Chapter 3.1, section 3.1.4.

93 Oversight Deliverable:

any resource required from the **evaluator** to perform one or more evaluation oversight activities.

94 Oversight Verdict:

a "pass" or "fail" statement issued by an **overseer** confirming or rejecting an **overall verdict** based on the results of evaluation oversight activities.

D R A F T

95 Protection Profile:

a re-usable and complete combination of security objectives, functional and assurance requirements with associated rationale. [CCREF]

96 Role:

Editor Note: this term is used in a generic sense only.

97 Scheme:

set of rules defining the evaluation environment, including criteria and **methodology** required to conduct IT security **evaluations**.

98 Security Target:

a complete combination of security objectives, functional and assurance requirements, summary specifications and rationale to be used as the basis for **evaluation** of an identified TOE. [CCREF]

99 Sponsor:

refer to Chapter 3.1, section 3.1.1.

100 Target of Evaluation:

an IT product or system that is the subject of an **evaluation**. [CCREF]

101 Verdict:

see **overall verdict** and **interim verdict**.

A.3 References

CCREF Common Criteria for Information Technology Security Evaluations, Version 1.0, January 1996.

COD Concise Oxford Dictionary.

D R A F T

Annex B

CEM observation report (CEMOR)

B.1 Introduction

102 This annex details a mechanism by which to comment on the CEM.

103 This mechanism consists of a report format to be used to articulate the observation as well as a mailing address to which a CEMOR should be sent.

B.2 Forwarding a CEMOR

104 A CEMOR may be sent directly to the internet mail address "cem@cse.dnd.ca". The CEMOR may be sent to this internet address directly by the originator or, alternatively, through one of the organisations listed in the foreword of this part. An acknowledgement will normally be sent to the originator of a CEMOR.

B.3 Format of a CEMOR

105 A CEMOR shall be forwarded in a text (ASCII) format only.

106 A separate CEMOR shall be created for each observation. A single CEMOR shall not address two or more unrelated observations.

107 A CEMOR shall contain all of the following fields, although one or more fields may be empty. Each field shall begin with the ASCII character "**$**", followed by an arabic number, followed by the ASCII character "**:**"

$1: Originator's name

108 Full name of the originator.

$2: Originator organisation

109 The originator's organisation/affiliation.

$3: Return address

110 Electronic mail or other address to acknowledge receipt of the CEMOR and request clarification, if necessary.

$4: Date

111 Submission date of observation YY/MM/DD.

D R A F T

$5: Originator's CEMOR identifier

112 This identifier is assigned to the CEMOR by the originator. There are two requirements for this identifier. Firstly, that it be unique to the originator and, secondly, that it be prefixed with "**CEMOR.**".

$6: Title of the CEMOR

113 A short descriptive title for this CEMOR.

$7: CEM document reference

114 Single reference to the affected area of the CEM. This field shall identify the CEM part number and section number and. Additionally, a paragraph number (or, if no paragraph number is relevant, the table or figure number) shall also be identified in this field.

$8: Statement of observation

115 Comprehensive description of the observation. There is no restriction regarding the length of this field. However, it shall contain text only; no figures or tables other than what can be achieved within the realm of ASCII shall be used.

$9: Suggested solution(s)

116 Proposed solution(s) for addressing the observation.

117 ### $$ End of CEMOR

118 Required to mark the end of CEMOR relevant information.

B.3.1 Example observations:

$1: A. N. Other

$2: PPs 'R' US

$3: another@ppsrus.com

$4: 96/01/31

$5: CEMOR.ano.comment.1

$6: Spelling Error

$7: Part 1, Section 3.1.5, Paragraph 49

$8: "Summarizes"

$9: If the intent is to use UK English, use "summarises".$$