Swedish Certification Body for IT Security

004 Licensing of Evaluation Facilities

Issue: 28.0, 2020-Nov-02

Authorisation: Mats Engquist, Chief Operating Officer , CSEC

Template: CSEC_mall_doc, 7.0

Table of Contents

1 Preface 3
1.1 Purpose 3
1.2 Terminology 3

2 Introduction 4
2.1 Overview 4
2.2 Licensing Agreement and Licensing Fees 4
2.3 Management of Confidential Information 4

3 Procedures and Requirements for ITSEF Licensing 6
3.1 ITSEF Licensing Procedures 6
3.2 ITSEF Requirements 9
3.3 ITSEF License Maintenance 15
3.4 License Extension 15
3.5 Termination of License 16

4 Evaluator Qualification 18
4.1 Three Levels of Evaluator Status 18
4.2 Limitations 18
4.3 Application Procedure 18
4.4 Competence Requirements 19
4.5 Maintenance of Evaluator Status 22

1 Preface

1 This document is part of the description of the Swedish Common Criteria Evaluation and Certification Scheme ("the Scheme").

2 This document is part of a series of documents that provide a description of aspects of the Scheme and procedures applied under it. This document is of value to all participants under the Scheme, i.e., to anyone concerned with the development, procurement, or accreditation of IT products for which security is a consideration, as well as those already involved in the Scheme, i.e., employees at the Certification Body, Evaluators, current customers, contractors, and security consultants.

3 The Scheme documents and further information can be obtained from the Swedish Certification Body for IT Security. Complete contact information is provided in the following box.

Swedish Certification Body for IT Security
FMV / CSEC
Postal address: SE-115 88 Stockholm, Sweden
Visiting address: Banérgatan 62

Telephone: +46-8-782 4000 E-mail: csec@fmv.se
Web: www.csec.se

1.1 Purpose

4 This document describes the requirements and procedures for licensing and license maintenance of Evaluation Facilities under the Scheme.

5 The document is primarily intended for organisations planning to set up an Evaluation Facility and operate it under the Scheme.

1.2 Terminology

6 Abbreviations commonly used by CSEC are described in SP-001 *Certification and Evaluation - Scheme Overview*

7 The following terms are used to specify requirements:

SHALL	Within normative text, “SHALL” indicates “requirements strictly to be followed in order to conform to the document and from which no deviation is permitted.” (ISO/IEC).
SHOULD	Within normative text, “SHOULD” indicates “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.” (ISO/IEC) The CC interprets 'not necessarily required' to mean that the choice of another possibility requires a justification of why the preferred option was not chosen.
MAY	Within normative text, “MAY” indicates “a course of action permissible within the limits of the document.” (ISO/IEC).
CAN	Within normative text, “CAN” indicates “statements of possibility and capability, whether material, physical or causal.” (ISO/IEC).

2 Introduction

2.1 Overview

8 The Scheme allows certificates to be awarded to IT products or protection profiles which have been successfully evaluated by an IT Security Evaluation Facility (ITSEF) licensed by the Certification Body.

9 The licensing process ensures that the ITSEF has sufficiently demonstrated that it is technically competent in the specific field of IT security evaluation and that it is in a position to comply in full with the rules of the Scheme.

10 The licensing process includes demonstrating that the ITSEF has the ability to apply *the Common Criteria for Information Technology Security Evaluation* (the Common Criteria or CC), and the corresponding *Common Methodology for Information Technology Security Evaluation* (the Common Methodology or CEM), correctly and consistently, satisfying the Scheme's following universal principles of evaluation.

- Appropriateness
- Impartiality
- Objectivity
- Repeatability
- Reproducibility
- Generation of sound results
- Cost effectiveness
- Confidentiality

11 An ITSEF may be managed and staffed by commercial or governmental organisations.

2.2 Licensing Agreement and Licensing Fees

12 A licensing agreement is established as follows.

1. The applicant signs and submits a licensing application form (SP-195 *License Application - Form*) to the Certification Body, thereby accepting the responsibility to comply with the requirements defined in this document and the charges associated with licensing as defined in the application form and in Scheme publication SP-008 *Charges and Fees*.
2. The Certification Body determines the licensing fees depending on the scope of the licensing application, and sends a Tender to the applicant.
3. The applicant sends a written and signed acceptance of the Tender to the Certification Body.

13 These three documents together form the Licensing Agreement.

2.3 Management of Confidential Information

14 Documents received or drawn up by the Certification Body are official documents ("*allmän handling*") and may be kept secret by the Certification Body only when it is required to protect the interests covered by articles in The Swedish Law on Publicity and Secrecy regarding:

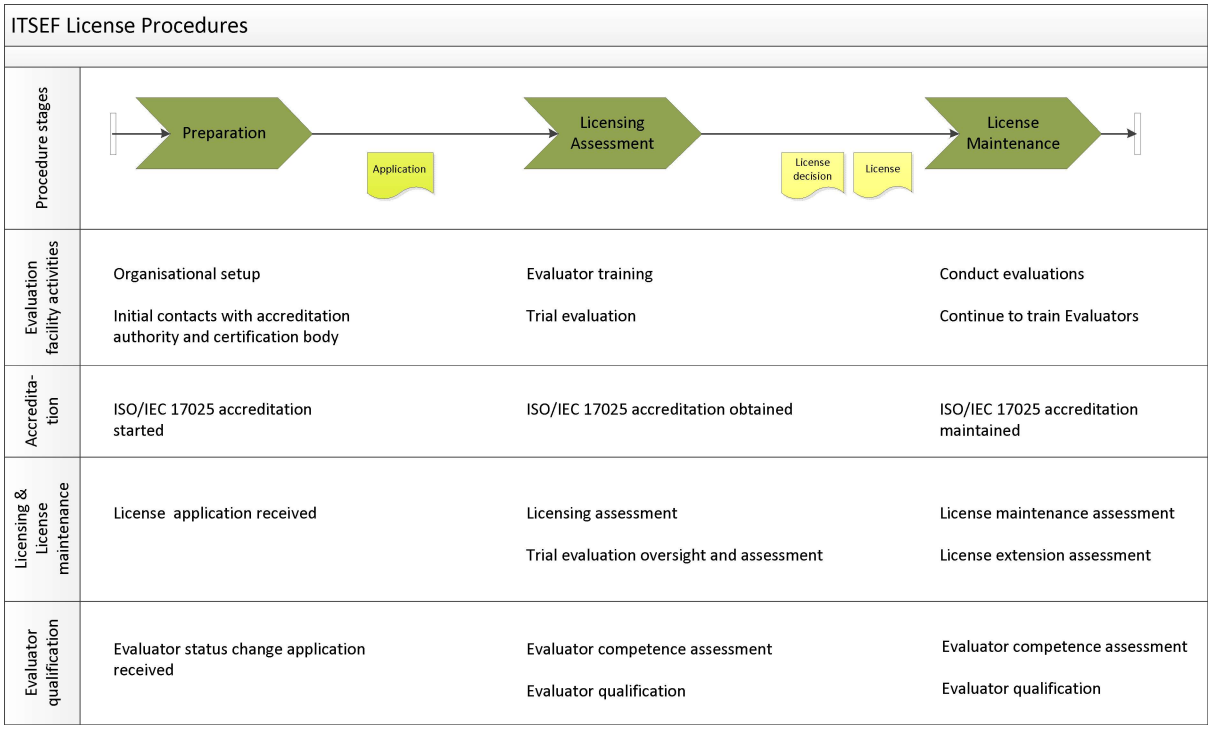
- the security of the realm or its relationships with another state or international organisation;
- inspection, control, or other supervisory activities of a public authority;
- the prevention or prosecution of crime;

- the economic interests of the public institutions; and
- the protection of the personal or economic circumstances of private subjects.

15 For further details on legal protection of confidential information, how to make the Certification Body aware of confidentiality claims and procedures for exchanging confidential information with the Certification Body please contact the Certification Body.

3 Procedures and Requirements for ITSEF Licensing

3.1 ITSEF Licensing Procedures



ITSEF Licensing procedures can be described by defining three stages:

- Preparation stage, wherein the ITSEF prepares for, and applies for, ISO/IEC 17025-accreditation and ITSEF licensing;
- Licensing Assessment stage, wherein ISO/IEC 17025-accreditation and ITSEF license are obtained and Evaluators are trained; and
- License Maintenance stage, wherein the ITSEF license is maintained by regular assessments.

3.1.1 Preparation and Application

16 Some amount of preparation by the ITSEF is needed in order to meet the Scheme requirements for an ITSEF. See section 3.2 *ITSEF Requirements*.

17 In addition to preparing the organisation and management systems of the ITSEF to meet the ITSEF requirements, procedures for ISO 17025 Accreditation and for Evaluator qualification should be started. The Evaluator qualification procedures are described in section 4 *Evaluator Qualification*.

18 The ITSEF is advised to contact the Certification Body before starting the preparations.

License application

19 The ITSEF should apply in writing to the Certification Body, using SP-195 *License Application - Form*. The application should be signed by the applicant and accompanied by the ITSEF's Quality Manual, its Security Instructions and documented Evaluation procedures.

20 The Certification Body will acknowledge the receipt of the license application and will propose a time for a meeting to be held with representatives of the ITSEF.

Licensing Start-Up Meeting

21 The purpose of the Licensing Start-Up meeting is to inform the ITSEF about the licensing procedures and to inform the Certification Body about the status of the ITSEF regarding licensing issues. The meeting also includes discussion of a preliminary plan for the licensing procedures.

3.1.2 Licensing Assessment

22 The Certification Body will review documents provided by the ITSEF to ensure that the requirements stated in section 3.2, *ITSEF Requirements*, are met. Documents to be reviewed are those provided with the license application as well as any other relevant documents requested by the Certification Body during the assessment, such as the following.

- Accreditation assessments, if applicable
- Internal audit reports
- Management review reports
- Risk assessment reports
- The ITSEF's Quality management system
- Evaluator Curriculum Vitae (CV) see section 4.5 Maintenance of Evaluator Status

23 The assessment involves one or more visits at the ITSEF ("site visits") and interviews with ITSEF staff.

24 Each location to be covered by the ITSEF license will be assessed and may be the subject of a site visit.

25 Full co-operation from the ITSEF is essential during the initial assessment, including supplying information, making personnel available for questions and discussions, and permitting reasonable inspections for the purpose of assessment on an agreed time schedule.

26 The Certification Body will report the outcome of the assessment to the ITSEF, stating which issues were found during the assessment and a time limit within which they must be resolved by the ITSEF if the licensing is to continue.

3.1.3 Trial Evaluation

27 In a trial evaluation, the ITSEF will demonstrate that it has appropriate organisational structure, processes, and infrastructure for performing evaluations.

28 The trial evaluation will also demonstrate that the ITSEF staff is competent in all aspects of the organisation and management of an evaluation task, including relationships with the other organisations that are involved in the evaluation process.

29 The Certification Body will monitor the performance of the ITSEF in those aspects.

30 Trial evaluations performed within the Scheme may be excluded from mutual recognition if ISO/IEC 17025 accreditation has not yet been granted to the ITSEF.

Trial Evaluation Preparations

31 The ITSEF is responsible for selecting a suitable product to become the Target of Evaluation (TOE) for the Trial Evaluation.

- The evaluation should be financed by a Sponsor.

- The evaluation should be performed at Evaluation Assurance Level (EAL) 3 or 4, possibly augmented.
- The evaluation should be ongoing, i.e. not already completed.
- The fact that the evaluation is a trial must be communicated and accepted in advance by the Sponsor.

32 The ITSEF is responsible for appointing an evaluator team with appropriate technical competence for the suggested target of evaluation.

- One candidate Evaluator/Qualified Evaluator should be appointed to the team, in order to be able to meet the requirements for Qualified Evaluator. See section 4, *Evaluator Qualification*.
- The team may be augmented by internal or external technical experts as needed to ensure the necessary technical competence. See section 4.4 *Competence Requirements*.

Trial Evaluation Assessment

33 During the trial evaluation, the Certification Body will pay particular attention to the performance of the ITSEF in the following areas.

- The choice of Target of Evaluation (TOE) for the trial evaluation
- The appointment of an Evaluator team with regard to technical competence
- The planning of the evaluation
- The conduct of the evaluation to ensure conformance with the Scheme, and the extent to which the test methods employed meet the requirements of objectivity, repeatability, reproducibility, and impartiality
- The reporting of the evaluation, both in terms of quality and level of detail
- Procedures to ensure that confidentiality requirements are observed

34 Granting an ITSEF license does not require granting a certificate to the evaluated product. ITSEF licensing may succeed even if the evaluation does not end with the granting of a certificate to the evaluated product.

35 The outcome of the trial evaluation assessment will be reported to the ITSEF.

3.1.4 Granting of an ITSEF Licence

36 The Evaluation Facility will be granted an ITSEF license when the following conditions are met.

- The trial evaluation has been assessed and the requirements in section 3.1.3, *Trial Evaluation,* have been met
- No unresolved findings from the licensing assessment remain
- The ITSEF has been accredited according to ISO/IEC 17025 (unless established by the Swedish Government)
- The ITSEF has at least one Qualified Evaluator on its staff

37 The License Decision is taken by the Head of CSEC and will be documented, stating the scope and locations covered by the License. The License may be extended, see section 3.4, *License Extension*.

3.2 ITSEF Requirements

38 To achieve and maintain an ITSEF license, the ITSEF must comply with the requirements defined in this section. Evaluation Facilities planning to perform evaluation activities outside Sweden must also comply with the requirements in Scheme publication SP-191 *Cross Frontier Evaluation*.

39 The requirements are divided into the following areas.

- Initial requirements are requirements that have to be met in order for a license application to be considered.
- Management requirements are requirements on the ITSEF organisation and procedures.
- Security requirements are requirements on security procedures as well as on the actual security maintained during evaluation assignments.
- Staff qualification requirements are requirements on the qualifications and number of Evaluators.

3.2.1 Initial Requirements

40 IT security evaluations within the Scheme in which it is licensed SHOULD be one of the business objectives of an ITSEF.

41 An ITSEF licensed in the Scheme SHALL also be accredited as a testing laboratory by an accreditation body in accordance with the ISO/IEC 17025 standard, unless established under a law or statutory instrument by the Swedish government.

42 An ITSEF thus not required to be accredited SHALL fulfil the requirements of ISO/IEC 17025 in addition to the requirements in this document.

43 Regardless of accreditation status, fulfilment of ISO/IEC 17025 requirements may be subject to review during license assessments / re-assessments.

3.2.2 Management Requirements

General

44 The ITSEF SHALL comply with the requirements of the Scheme, including rules and procedures for evaluations and certifications stated in Scheme publication SP-002 *Evaluation and Certification*.

45 The ITSEF SHALL co-operate with the Certification Body at evaluations and certifications, including supplying information, making personnel available for questions and discussions, and permitting reasonable inspections for the purpose of assessment by the Certification Body.

46 The ITSEF SHALL keep the Certification Body informed of all Scheme evaluation work in progress.

47 The ITSEF SHALL have documented procedures to ensure that it does not:

- jeopardise the reputation of the Scheme or the Certification Body;
- make use of its, or its Evaluators', status within the Scheme when promoting services or other professional activities performed outside the scope of the Scheme; or
- give misleading information about its status or about its Evaluators' status within the Scheme.

Organisation

48 In addition to the requirements of ISO/IEC 17025, the following roles and responsibilities concerning ITSEF organisation SHALL be appointed and documented and communicated to the Certification Body.

49 *Head of the ITSEF*

- The Head of the ITSEF SHALL have overall responsibility for the ITSEF operation within the Scheme.
- The Head of the ITSEF SHOULD have a thorough understanding of the Scheme.
- The Head of the ITSEF SHOULD be authorised to sign agreements in the name of the ITSEF organisation.
- The Head of the ITSEF SHOULD sign the ITSEF's application to become a licensed ITSEF.

50 *Point of Contact*

- In matters concerning the ITSEF as an organisation, the point of contact responsible for liaison with the Certification Body SHOULD be the Head of the ITSEF.
- From time to time, the Head of the ITSEF MAY appoint a different point of contact with the Certification Body.
- For individual projects, the point of contact with the Certification Body SHOULD be the Lead Evaluator.

51 *Security Manager*

- The Security Manager SHALL be responsible for the physical and information security aspects of ITSEF operation.
- The Security Manager SHALL report to the Head of ITSEF.

Impartiality

52 The ITSEF SHALL have documented procedures for identifying conflicts of interest which may pose a risk to its impartiality, and for ensuring that such conflicts of interest do not adversely influence the quality of the evaluations.

53 The procedures SHOULD ensure that no ITSEF personnel that has been involved with the supplier of a product under evaluation within the preceding two years, either in design of the product or consultancy services to the supplier regarding methods of dealing with matters that are barriers to the product being certified, can be assigned to an evaluation.

Quality

54 The ITSEF SHALL maintain a Quality Manual according to the requirements in ISO/IEC 17025.

55 The ITSEF SHALL have documented procedures to ensure that the current versions of all documents related to the ITSEF operation are used. This includes, at least, the Common Criteria, the Common Methodology, the Scheme documentation, internal checklists, and procedures.

56 The ITSEF SHALL have documented procedures to ensure that all records and documents related to evaluations under the Scheme will be kept and handled in a secure manner during a sufficiently long period. These procedures SHALL include the following.

- Archiving routines
- Rules for retrieving objects from an archive
- Backup routines

- Restoring of data from backups
- Destruction of backups

57 The ITSEF SHALL have documented procedures to ensure that periodic audits of the quality management system are held.

58 The ITSEF SHALL have mapping for how ISO/IEC 17025 requirements are met in the ITSEF management system.

59 The ITSEF SHALL have mapping for how the requirements in the CSEC Scheme Publications (SP) are met in the ITSEF management system, at a minimum for the "SHALL" requirements.

Locations

60 Licensed ITSEFs SHALL identify those physical locations where evaluation activities are conducted or controlled that determine or demonstrate the effectiveness of the ITSEFs in accordance with the Scheme. Such locations are referred to as "Critical Locations".

61 Critical Location(s) SHALL be situated within Sweden and be subject to the licensing procedures of the Scheme.

62 FMV/CSEC may approve that evaluation activities/processes which are not reserved for Critical Location are performed at a location outside Sweden (referred to as a "Foreign Location").

63 In such cases the following restrictions apply.

- The scope of evaluation activities performed at Foreign Locations SHALL be documented in the ITSEF quality system.
- The ITSEF and associated Foreign Location SHALL fulfil the requirements for evaluation facilities licensed under the Scheme.
- The licensed ITSEF SHALL provide documentation that demonstrate that the ITSEF and Foreign Locations (within the claimed scope of operation) fulfil all requirements, including general requirements, quality requirements, security requirements and competence requirements defined in this section.
- Such documentation SHALL be up-to-date and subject to configuration management.

64 The ITSEF Critical Location SHALL check and document their fulfillment of the restrictions above

65 Such documentation MAY be included in the Management review report.

66 Both Critical and Foreign locations are subject to the regulations in Scheme publication SP-191 *Cross Frontier Evaluation*.

67

Use of Logotypes and Trademarks

68 The ITSEF SHALL follow the rules for using logotypes stated in Scheme publication SP-070 *Conditions for the Use of Trademarks*.

Subcontracting

69 The ITSEF SHALL have documented procedures to ensure that when a subcontractor is used to perform evaluation activities, the following restrictions apply.

- The Certification Body is notified in advance about the subcontractor activities.

- The subcontractor has signed necessary confidentiality agreements with the ITSEF and, if necessary, the Sponsor, to handle the information necessary for the subcontractor's activities.

70 The ITSEF is responsible to the Sponsor and the Certification Body for the subcontractor's work.

3.2.3 Staff Requirements

71 The ITSEF SHALL have sufficient personnel to perform adequate quality assurance on its evaluations.

Evaluators

72 The Scheme recognises three levels of Evaluator qualification as follows.

- Trainee Evaluator
- Evaluator
- Qualified Evaluator

73 The ITSEF SHALL be able to demonstrate the Evaluator's competence in the Quality and the Security Management System of the ITSEF.

74 The ITSEF SHALL have at least one Qualified Evaluator. At least one Qualified Evaluator SHALL be involved in each evaluation that is not a trial evaluation. All of the Qualified Evaluators SHALL comply with the general requirements for acting as Lead Evaluators (see Scheme publication SP-002 *Evaluation and Certification)*.

75 The qualification requirements for Evaluators, Qualified Evaluators and Trainee Evaluators are given in section 4 *Evaluator Qualification*.

76 The Evaluation reports SHALL contain information about any technical experts, other experts or Evaluator assistants who have contributed to the evaluation and it SHOULD be clarified in the report which parts they have contributed with.

3.2.4 Security Requirements

77 An ITSEF SHALL operate an effective Security Management System in order to preserve confidentiality when handling confidential information and equipment. When handling classified governmental information, additional safeguards may be required which are beyond the scope of this document. The ITSEF SHALL be able to provide evidence that confidentiality requirements are being met.

78 The ITSEF SHALL perform risk analysis identifying assets needing protection, possible threats, and appropriate countermeasures. The risk analysis SHOULD be made available to the Certification Body if requested.

79 At a minimum, the ITSEF security system SHOULD include countermeasures derived from the risk analysis to deal with the following areas.

- Physical Security
- Information Security

80 All ITSEF staff SHALL be trained in the application of the safeguards defined in the Security Instructions (see below).

81 The rules defined for ITSEF staff SHALL be applied not only to employees but also to contractors and other temporary staff engaged by the ITSEF. See the section on Subcontracting in section 3.2.2, *Management Requirements*, for additional information.

Security Instructions

82 The Security Management System of the ITSEF SHALL be documented in Security Instructions either in a separate document or integrated into the Quality Management System. The Security Instructions SHALL govern the handling of confidential data and other preventative security activities in the ITSEF.

83 In addition to physical and information security, the instructions SHOULD address the following.

- Periodic audit of the procedures
- Keeping the ITSEF staff trained in the procedures
- Dealing with security violations

84 The ITSEF SHOULD maintain records so that adherence to the Security Instructions can be audited.

85 The Security Instructions and associated records SHALL be kept up to date and in accordance with the requirements in this document and with other applicable requirements.

Confidentiality Agreement

86 All staff SHALL sign a confidentiality agreement with the ITSEF. In the process of evaluation, additional individual confidentiality agreements MAY be required.

Physical Security

87 The ITSEF SHALL use appropriate premises and physical security safeguards to be able to protect information and equipment used in evaluations.

88 The premises SHALL be appropriately secured to ensure that evaluation material can only be accessed by authorised staff of the ITSEF. This MAY include locks and keys, alarms, and other safeguards.

89 At a minimum, the Security Instructions SHOULD address the following.

- Physical protection of facilities (locks, alarms)
- Identifying and registering staff and visitors
- Access control to the premises of the ITSEF and its individual rooms, as well as to equipment, cabinets and information
- Ensuring that unauthorised staff and visitors of the ITSEF only have supervised access to controlled areas

90 The above measures contribute to maintaining confidentiality. An ITSEF MAY propose other arrangements that preserve confidentiality. Such proposals SHALL also be acceptable to any Sponsor whose evaluation projects are involved.

Information Security

91 To uphold the Scheme requirements on confidentiality of information entrusted to the ITSEF for evaluation purposes, the ITSEF SHALL be operated in a way that preserves information security. This SHOULD include at least the following.

- Access control, such as identification and authentication
- Security audit (logging of events, penetration detection, etc.)
- Security of data access (separation of data, penetration resistance, etc.)
- Security of communication (with Sponsor, Developer, Certification Body, etc.)
- Cryptographic key management (creation, distribution, storage, and destruction of keys, etc.)

- Incident management
- Protection of data (registration, safe archiving, backup and restore, secure destruction, etc.)
- Distribution of confidential material (mail, couriers, etc.).

92 With regard to information security, the security manual SHALL cover the handling of sensitive information in whatever form it is held.

3.3 ITSEF License Maintenance

3.3.1 Principles for License Maintenance

93 The ITSEF license is automatically renewed annually unless withdrawn, and an annual fee is charged (see SP-008 *Charges and Fees*).

94 In order to keep its license, the ITSEF SHALL comply with the requirements stated in section 3.2, *ITSEF Requirements*, as well as with the requirements defined in this section.

95 In addition to yearly assessments (see section 3.3.3, *License Report*) and the continuous certification oversight, the Certifications Body maintains contact with the ITSEFs through regular meetings with the Heads of ITSEF and a yearly conference (called "*ITSEF-dagen"*).

3.3.2 Information Requirements

96 The ITSEF SHALL inform the Certification Body without delay of any significant changes that may impact its Quality Management System or Security Management System or the ITSEF's competence level.

97 In such cases, the license will be reviewed with respect to the ITSEF's continuing ability to meet the requirements stated in section 3.2, *ITSEF Requirements*.

98 The ITSEF SHALL inform the Certification Body about accreditation assessments and it SHALL send copies of reports from assessments performed by the Accreditation Body to the Certification Body together with descriptions of the planned, and executed, actions resulting from such assessments.

99 Failure to retain ISO/IEC 17025 accreditation for an ITSEF licensed in the Scheme will result in withdrawal of the license and removal from the list of licensed Evaluation Facilities as described in section 3.5, *Termination of License*.

3.3.3 License Report

100 The ITSEF SHALL upon request by the Certification Body submit a license report, using SP-016 *License Report - Form*, together with required documentation, or reference to previously submitted documentation.

101 The required documentation includes e.g reports from accreditation assessments and internal audits, current mapping between ISO17025 requirements and how they are met in the ITSEF´s management system, current mapping between CSEC requirement in SP-documentation and how they are met in the ITSEF´s management system. It also includes management reviews and the follow-up of Foreign Locations.

102 For all current Evaluators and Qualified Evaluators this includes current CVs detailing any CC-related activities for the past year (see section 4.5 Maintenance of Evaluator Status).

103 The Certification Body may request further information if deemed necessary, and may also perform an on-site inspection of any licensed site.

104 After completed maintenance assessment, the Certification Body will issue a report stating the conclusions of the assessment.

3.4 License Extension

105 A licensed ITSEF may wish to extend its license, e.g. to include locations or types of evaluations not covered by the current License.

106 The Head of ITSEF SHOULD apply in writing to the Certification Body, stating the nature of the requested extension.

107 An assessment of the extension and, if needed, a partial re-assessment will be made, and a new License Decision will be taken.

108 For licenses including locations outside Sweden, see also Scheme publication SP-191 *Cross Frontier Evaluation.*

109 For charges and fees associated with license extension, see Scheme publication SP-008 *Charges and Fees.*

3.5 Termination of License

110 If the Certification Body determines that the ITSEF does not comply with all Scheme requirements, the ITSEF's license MAY be suspended or withdrawn.

111 The license MAY also be withdrawn at the request of the ITSEF.

112 Decision about suspension or withdrawal is taken by the Head of the Certification Body and will be documented.

3.5.1 Suspension

113 The ITSEF's license MAY be subject to suspension if both of the following circumstances are true.

- A condition not compliant with the requirements of the Scheme exists
- The condition is likely to be resolved with reasonable efforts within six months (or within another period specified by the Certification Body)

114 If such a condition is identified, the Certification Body will immediately, in writing, inform the ITSEF about this. The Certification Body will also inform the ITSEF that the ITSEF Licence may be suspended or withdrawn if the condition is not resolved within a specified time period.

115 If the condition that caused the suspension is not resolved within the specified time period, the ITSEF license MAY be withdrawn according to the rules in section 3.5.2, *Withdrawal*.

116 If the ITSEF's license is suspended, the Certification Body will determine whether, and in what way, on-going Scheme evaluation work is to be allowed to continue.

117 Work performed during suspension will be closely monitored by the Certification Body. Evaluations will not be allowed to continue if continuation could bring the Scheme into disrepute or if the interests of the Sponsor are not supported.

3.5.2 Withdrawal

118 The Certification Body reserves the right to withdraw the license without any foregoing suspension period if the ITSEF is found to be in serious breach of the conditions of license, i.e., for any the following reasons.

- The ITSEF's ISO/IEC 17025 accreditation lapses, if such accreditation is required. (no notification time by the Certification Body is required)
- The ITSEF has been declared bankrupt. (no notification time by the Certification Body is required)
- The conditions causing a suspension have not been resolved within the agreed time period. (no notification time by the Certification Body is required)
- The Scheme is to be terminated.

119 If the ITSEF license is withdrawn, the ITSEF SHALL immediately cease all Scheme evaluation activities. The Certification Body will consult with the affected Sponsors to decide how to handle any on-going Scheme evaluation activities to minimise the harm to the affected Sponsors and Developers.

120 The ITSEF will be removed from the list of licensed Evaluation Facilities.

3.5.3 Withdrawal at ITSEF's Request

121 The license MAY be withdrawn at the ITSEF's own request for whatever reason.

122 The ITSEF SHOULD apply for withdrawal in writing to the Certification Body, at least one month before the annual renewal, stating the circumstances.

123 The time schedule and possible actions to be undertaken before the license can be withdrawn will then be agreed between the ITSEF and the Certification Body.

4 Evaluator Qualification

124 This section describes the meaning of status as Evaluator, Qualified Evaluator or Trainee Evaluator, the qualifications needed for achieving the status and the qualification procedures. The section also describes the requirements for maintenance of different Evaluator statuses.

4.1 Three Levels of Evaluator Status

125 An Evaluator working within the Scheme is licensed as such by the Certification Body according to the procedures described here. There are three levels of Evaluator Status: Evaluator, Qualified Evaluator or Trainee Evaluator.

126 The Certification Body maintains records of all Evaluators, Qualified Evaluators and Trainee Evaluators.

- Evaluators
  - An Evaluator is allowed to perform evaluation work and write evaluation reports.
- Qualified Evaluators
  - An Evaluator who have been assessed by the Certification Body and meet the requirements for becoming Qualified Evaluator, are awarded the Qualified Evaluator status.
  - A Qualified Evaluator may act as Lead Evaluators.
  - Qualified Evaluators up to EAL 2 or 3 may only lead evaluations up to the evaluation assurance level they have been qualified for.
- Trainee Evaluators
  - A Trainee Evaluator SHALL have a Trainee Supervisor, who is an Evaluator or a Qualified Evaluator, appointed by the ITSEF.
  - The Trainee Supervisor SHALL take full responsibility for the work of the Trainee.
  - A Trainee Evaluator may perform evaluation work and to write evaluation reports under the supervision of the Trainee Supervisor.

4.2 Limitations

127 The Evaluator's status is limited to the context of the Scheme.

- An Evaluator SHALL not claim his or her Evaluator status to perform work outside the Scheme. If this happens, the Certification Body may withdraw the Evaluator's status.

128 The Evaluator's status is specific to the ITSEF, since knowledge of matters specific to the ITSEF is a significant component of the Evaluator's competence.

- If a new member of the ITSEF staff achieved Evaluator, Qualified Evaluator or Trainee Evaluator status within the Swedish Scheme in a previous position, before joining the ITSEF, an application for the re-award of this status SHALL be submitted to the Certification Body.

4.3 Application Procedure

129 The Head of ITSEF SHALL apply in writing to the Certification Body for a staff member to be awarded or re-awarded Evaluator, Qualified Evaluator or Trainee Evaluator status, for instance using Scheme publication SP-022 *Evaluator Status Change Application – Form*.

130 The application SHALL be accompanied by the following documents:

- When applying for Evaluator or Trainee Evaluator status; a declaration of IT security competence using Scheme publication form SP-024 *IT Security Competence - Form ,* which states the candidate's background, knowledge and experience in the fields of IT security evaluation, IT security in general, IT in general, and other relevant areas.
- If the Evaluator previously had achieved Trainee Evaluator Status, the application SHALL also be accompanied by the completed and by the Head of ITSEF signed training plan.
- When applying for Trainee Evaluator status; the application SHALL also include an individually established training plan for the Trainee Evaluator to achieve Evaluator status with regard to previous education and experience. The training plan SHALL identify and address the competencies that constituted an obstacle for the individual to not apply for Evaluator status directly.
- When applying for re-award of Evaluator, Qualified Evaluator or Trainee Evaluator status the application SHALL be accompanied by a description of how the new ITSEF staff member has received sufficient training and guidance in the ITSEF's Quality and Security Management Systems.
- When applying for Qualified Evaluator see additional requirements in chapter 4.4.2 *Qualified Evaluator Competence Requirements.*

4.4 Competence Requirements

131 Evaluators, irrespective of status and level, shall be able to demonstrate relevant knowledge in the tasks they are assigned.

132 Evaluators and Qualified Evaluators working within the Scheme are expected to:

- understand the principles and methods used in the CC, the CEM, and the Scheme;
- understand the relationship between supporting documents used in the CC or in different types of Protection Profiles (PP:s) in the field of ITSEF operation;
- be able to demonstrate understanding of the Quality and Security Management Systems of the ITSEF;
- be able to apply the CC, the CEM, and the Scheme in real evaluations at any assurance level accepted for mutual recognition;
- demonstrate understanding of the overall evaluation planning process;
- be able to independently document the evaluation results of his or her work objectively, precisely, correctly, unambiguously, and at the level of detail required by the CC, the CEM, and the Scheme.

133 In addition to the general competence described in this section, the Evaluators also SHALL have sufficient technical competence for the tasks they perform.

- It is the ITSEF’s responsibility to determine the competence needed in the Evaluator team for each evaluation, to appoint evaluators accordingly, and, if necessary, to augment the Evaluator team with internal or external technical experts.
- The Certification Body will independently determine the competence needed in the Evaluator team and assess the appointments made by the ITSEF.
- The Certification Body will report the assessment results, and may request justification from the ITSEF for the appointment decisions, with regard to the overall technical competence of the Evaluator team.
- See Scheme publication SP-002 *Evaluation and Certification*.

134 The Certification Body may decide upon specific competence requirements for specific tasks. Such requirements will be published by the Certification Body.

4.4.1 Evaluator Competence Requirements

135 In this section the education and experience needed for achieving Evaluator status is described.

Initial Education and Experience for an Evaluator

136 The Evaluator SHOULD meet the following minimum education and experience requirements.

- Three years of university studies followed by two years' IT security work experience

or

- Upper secondary school followed by five years of work experience including two years' IT security work experience.

137 If the Evaluator previously had achieved Trainee Evaluator Status, the completed and by the Head of ITSEF signed training plan has to be provided by the ITSEF.

Requirements for Achieving Evaluator Status

138 The candidate SHALL:

- demonstrate acceptable common IT security knowledge and former IT security experience by filling in form SP-024 *IT Security Competence – Form,* and by taking part in a personal interview;
- participate in CC/Scheme training
- pass the CC/Scheme examination.

139 In addition to the assessment performed during the evaluation oversight, the Certification Body will monitor the progress of the Evaluator as necessary to determine the readiness to become a Qualified Evaluator.

140 A candidate who meets the Evaluator competence requirements can be assigned status as Evaluator directly, without first having to work as a Trainee.

4.4.2 Qualified Evaluator Competence Requirements

141 A Qualified Evaluator SHALL, (in addition to the Evaluator competence requirements in the previous section*)* meet the following qualifications.

- The Qualified Evaluator SHALL demonstrate experience in:
  - planning and conduct of vulnerability analysis and penetration tests
  - planning and conduct of site visits
- The Qualified Evaluator SHALL have understanding and experience of using supporting documents used in the CC or in different types of Protection Profiles (PP:s) in the field of ITSEF operation;
- The Qualified Evaluator SHALL, at least once, have independently written Evaluator results for all Evaluator actions in each assurance family at evaluation assurance level 4 (EAL 4) and above.
- If appropriate EAL 4 projects not have been available the ITSEF may apply for status as Qualified Evaluator up to EAL 2 or Qualified Evaluator up to EAL 3. Qualified Evaluators up to EAL 2 or 3 may only lead evaluations up to that EAL.

- The Qualified Evaluator up to EAL 2 or 3 SHALL, at least once, have independently written Evaluator results for all Evaluator actions in each assurance family at the chosen evaluation assurance level and below.

142 To achieve any Qualified Evaluator status the candidate must first achieve Evaluator status.

4.4.3 Trainee Evaluator Competence Requirements

143 In this section the education and experience needed for achieving Trainee Evaluator status is described.

Initial Education and Experience for a Trainee Evaluator

144 The Trainee Evaluator SHOULD meet the following minimum education and experience requirements.

- Three years of university studies in the field of IT- or Information security

or

- Upper secondary school followed by five years of work experience including two years' IT security work experience.

Requirements for achieving Trainee Evaluator Status

145 The candidate SHALL:

- demonstrate common IT security knowledge and former IT security experience by filling in form SP-024 *IT Security Competence – Form*;

146 The ITSEF SHALL:

- have a Trainee Supervisor for each Trainee Evaluator
- maintain records on who is appointed to each Trainee Evaluator
- provide an individually established training plan for the Trainee Evaluator to achieve Evaluator status with regard to previous education and experience
- in the training plan identify and address the competencies that constituted an obstacle for the individual to not apply for Evaluator status directly

During the Trainee period

147 Special rules apply during the Trainee period.

148 In all evaluation tasks the Trainee Evaluator SHALL be supported by the rest of the evaluation team under supervision by the Trainee Supervisor.

149 The trainee SHOULD:

- complete the CC/Scheme training according to the training plan
- pass the CC/Scheme examination within a maximum of two years as Trainee Evaluator.

150 The ITSEF SHALL:

- maintain records of who is appointed as Trainee Supervisor (Evaluator or Qualified Evaluator) to every Trainee Evaluator
- monitor the progress of the Trainee until the Trainee status is changed for Evaluator status

4.5 Maintenance of Evaluator Status

151 The status of Evaluator, Qualified Evaluator or Trainee Evaluator is to be maintained by continuously practising as an Evaluator. Evaluator status will be reviewed by the Certification Body in conjunction with the regular maintenance of the ITSEF's license (see section 3.3, *ITSEF License Maintenance*). The Certification Body will also monitor the performance of each Evaluator during certifications.

152 Evaluator completed and planned competence development SHALL be documented in an Evaluator CV. The completion SHOULD be recorded with date and year or/and planned competence development SHOULD be recorded with planned year in the following:

- CC Evaluations (within or outside of the Scheme) specifying areas of competence involved
- Formal training in the field of CC / IT Security
- Other relevant experience in the field of CC / IT Security, gained or planned

153 For a Trainee Evaluator the individually established training plan SHALL be updated with performed actions with date and year.

154 The efficiency of the competence development SHOULD be monitored and documented in the management review both for critical location and foreign locations.