CSEC

Swedish Certification Body for IT Security

007 Quality Manual

Issue: 49.0, 2021-Nov-03

Authorisation: Sofia Sandin, Quality Manager , CSEC

Table of Contents

1 Introduction

1 This document is the Quality Manual for the Swedish Certification Body for IT Security (CSEC).

2 For general information on the Swedish Certification Body for IT Security see the publication EP-001 *Certification and Evaluation - Overview* where you also find lists of abbreviations commonly used by CSEC.

3 This document provides a detailed description of the organisation and processes within the Certification Body (CB). It is primarily intended for the Certification Body personnel, but may also be of interest to evaluators, sponsors, developers and other parties who want to gain a better understanding of the operations of the Certification Body.

1.1 Background

4 CSEC is an entity within the Swedish Defence Materiel Administration (FMV) acting as certification body and conformance assessment body within the Cybersecurity Act.

5 In the *Ordinance with instructions for the Swedish Defence Materiel Administration* (SFS 2007:854) the Swedish government has stated that at the FMV there is a Certification Body for security in IT-products and systems. FMV should act to obtain and maintain international recognition for issued certificates.

6 In the *Ordinance with Supplementary Directions to the EU Cybersecurity Act* (SFS 2120:555), the Swedish Government has stated that FMV is the Swedish authority for cybersecurity certification, and that at FMV there is an accredited conformity assessment body according to Article 60.2 of the Cybersecurity Act.

7 In the *Appropriation Directions for the Swedish Defence Materiel Administration,* the Swedish Department of Defence has stated that the budget allocation may be applied to operating a national certification scheme for security in IT products and systems. This includes operating as a national certification body, performing certifications, and acting as a signatory body and representative within the international Common Criteria Recognition Arrangement (CCRA) and the corresponding European agreement (SOGIS-MRA).

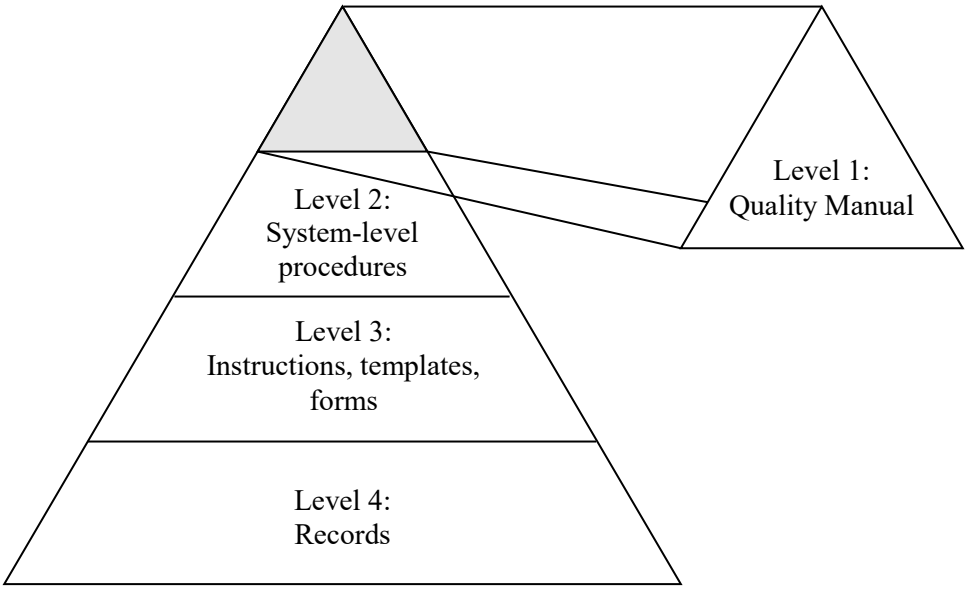
8 The mission of the Certification Body is documented in VB-140 *Verksamhetsbeskrivning* (in Swedish) and in related documents within FMV.

1.2 Documentation

1.2.1 Structure of the Quality Management System

9 The policies and procedures of the Certification Body are documented in the Quality Management system. The documents in the Quality Management System are arranged in a structure with four levels, each representing a more detailed level of abstraction, as follows.

- Quality Manual
- System-level procedures
- Instructions, templates, forms
- Records



Quality Manual (this document)

10 The Quality Manual is the top-level document in the Quality Management System as required by ISO/IEC 17065:2012.

11 The Quality Manual states the policy and strategies of the Certification Body and describes the overall Quality Management System including management and organisation.

12 The Quality Manual defines obligations and responsibilities and refers to the procedures of the Quality Management System.

System-Level Procedures

13 System-level procedures are high-level instructions that describe procedures, functions, and processes in terms of "why", "what", "how", and "when". They are cross-functional in the sense that they clearly identify the responsibilities of different organisations and departments.

14 System-level procedures may reference other documentation, such as specific instructions.

Instructions, Templates, and Forms

15 Instructions are the most detailed description level. They contain information about "how" the different tasks actually are performed. Instructions consist of the following types of documentation.

- Descriptive documents
  These documents contain detailed controlling descriptions. Examples of documents in this category are procedures, definitions of roles, job descriptions, definitions and abbreviations, policies, and declarations.
- Plans and detailed descriptions
  These documents describe the instantiation of the overall policies and procedures for specific projects or tasks.
- Temporary Quality Management Notes
  Notes issued by the Quality Manager clarifying aspects about using the Quality Management System or, after decision by the Change Control Board, describing a deviation from an authorised version of the Quality Management System.

- Process web
  Most common FMV-Instructions are defined as processes, activities, and activity steps in *FMV VHL*. Currently no instructions of the Certification Body are described in this way.
- Other documents
  Everything else, such as forms, templates, or checklists, which are a part of the Quality Management System.

Records

16 Records are the documentation evidence of activities performed or results achieved. Records provide evidence of conformity to requirements and of the effective operation of the Quality Management System.

1.2.2 Requirements

17 The Quality Management System of the Certification Body is designed to meet the requirements of the following national and international standards and regulations.

- EUCC, the European Cybersecurity Certification scheme for ICT products based on the Common Criteria. EUCC will be established thru an EU Implementing Act sometime during 2022.
- International Organisation for Standardisation/International Electrotechnical Commission (ISO/IEC) – ISO/IEC 17065:2012
  Conformity assessment – Requirements for bodies certifying products, processes and services
- Common Criteria Recognition Arrangement (CCRA)
  Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security
- Senior Officials Group Information Systems Security (SOGIS)
  Mutual Recognition Agreement of Information Technology Security Evaluation Certificates

18 The following document contains requirements and conditions for accreditation for the Certification Body. These requirements apply to the accreditation process and set up conditions for accredited bodies and are not traced within the Quality Management System.

- STAFS 2020:1 Styrelsen för ackreditering och teknisk kontrolls föreskrifter och allmänna råd om ackreditering
  (English: *Swedac´s Regulations and General Guidelines on Accreditation*)

1.2.3 Version Description Documents

19 The purpose of a version description document (VDD) is to identify all documents and versions of these documents that constitute a specific version of the Quality Management System. There may be different version description documents for different parts of the Quality Management System. A new version of a version description document is created each time a new version of a document referenced in the version description document is approved. A new version of the version description document is approved each time a new version of the referred part of the Quality Management System is to be published.

1.2.4 Valid Versions of the Quality Management System

20 It is always the current version of the Quality Management System that is used by the Certification Body.

21 When the Quality Management System is updated, the Quality Manager is responsible for ensuring that transition guidelines are established to the extent required to fulfil the Quality Objectives of the Certification Body and to maintain the effectiveness and efficiency of the Certification Body's activities.

22 The version of the Quality Management System used for a specific review, or oversight activity, will be documented in the technical oversight report (TOR) together with the impact of changes made to the Quality Management System.

23 All versions of the Quality Management System used during a Certification will be listed in the Certification Report, together with an analysis of the impact of all changes made to the Quality Management System during the Certification.

1.3 Publications

24 Parts of the Quality Management System which contain information, guidelines and requirements of interest to external interested parties, are published on the external website of the Certification Body. Such documents are divided into two subcategories:

- External publications (EP)
- Scheme Notes (SN)

25 It should be noted that the distinction between External publications and Scheme Notes may, in some cases, be subtle and may depend on the time frame in which the description is valid or the occasion on which it is issued.

26 Policies and procedures for these documents may be found in section 7.1, *The Quality Management System*.

1.4 Definitions

27 For the purposes of this manual, the relevant definitions given in ISO/IEC Guide 2 and ISO 9000 and ISO/IEC 17065 apply.

2 Mutual Recognition

28 Certificates issued by the Certification Body may be subject for mutual recognition according to the following arrangements and regulations:

- EUCC, the European Cybersecurity Certification scheme for ICT products based on the Common Criteria.
- Common Criteria Recognition Arrangement (CCRA)
- European co-operation for Accreditation Multilateral Agreement (EA MLA)
- Senior Officials Group - Information Security Mutual Recognition Agreement (SOGIS-MRA) of Information Technology Security Evaluation Certificates

29 A customer who applies for certification will be able to choose which mutual recognition agreement the certificate should be covered by. If the customer requires a product to be covered by more than one agreement, different certificates will be issued for each agreement.

30 A customer may also choose not to have a certification covered by any mutual recognition agreement. A certificate resulting from such a certification will be called a National Certificate.

2.1 EUCC

31 EUCC, the European Cybersecurity Certification scheme for ICT products based on the Common Criteria. EUCC will be established thru an EU Implementing Act sometime during 2022.

2.2 Common Criteria Recognition Arrangement (CCRA)

32 Certification bodies accepted by the participants of CCRA as compliant may issue certificates that are recognised, under the conditions of the arrangement, by all participants of CCRA.

33 Regulations for mutual recognition are documented in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security and in corresponding documents issued within CCRA.

34 FMV/CSEC is accepted as an Associated Certification Body by the members of CCRA.

2.3 European Accreditation Multilateral Agreement (EA MLA)

35 Certification bodies accredited by an approved accreditation body within the EA may issue certificates that are recognised, under the conditions of the stipulated by EA regulations, by all signatories of the EA MLA for the scope of product certification.

36 The Swedish Board for Accreditation and Conformity Assessment (Swedac) has issued regulations for bodies that certify IT security. These regulations specify conditions for accreditation and are documented in Swedac STAFS 2020:1.

37 FMV/CSEC is accredited by Swedac according to these regulations.

2.4 Senior Officials Group - Information Security Mutual Recognition Agreement (SOGIS-MRA)

38 Certification bodies accepted by the participants of SOGIS-MRA as compliant may issue certificates that are recognised, under the conditions of the agreement, by all participants of SOGIS-MRA.

39 Regulations for mutual recognition are documented in the SOGIS - Mutual Recognition Agreement of Information Technology Security Evaluation Certificates and in corresponding documents issued within the SOGIS-MRA.

40 FMV/CSEC is accepted as a Certification Body, up to evaluation assurance level 4 (EAL4), by the participants in the agreement.

2.5 National Certificates

41 Performing a certification resulting in a National Certificate may be relevant in Certifications where the requirements for mutual recognition could not be met, but where the customer would want to perform a certification according to the same principles.

42 Conditions leading to a National Certificate may be, for example, that the security classification of the Security Target or the certification report means that they cannot be published according to the requirements for mutual recognition.

43 Such certifications will be performed according to the applicable parts of the Quality Management System. Any deviations will be addressed in the certification report.

3 Policy

3.1 Objectives for Quality

44 The quality objectives for the Certification Body are as follows.

- To fulfil the requirements for accreditation as stated by the accreditation body
- To fulfil the requirements as conformity assessment body as stated in the Cybersecurity Act.
- To fulfil the requirements for recognition as a compliant Certification Body as stated within the CCRA
- To fulfil the requirements for recognition as a compliant Certification Body as stated within SOGIS-MRA
- To improve the availability of evaluated, security-enhanced IT products and protection profiles (PP)
- To perform certifications in a cost-effective way where efforts are concentrated to the areas where most benefit is gained with respect to national, as well as commercial, needs for secure products
- To continuously improve the efficiency and cost-effectiveness of the evaluation and certification process for IT products and protection profiles by participating in international technical communities regarding CCRA
- To ensure that evaluations and certifications are performed to high and consistent standards and will promote confidence in the security of IT products certified under this Scheme
- To fulfil the expectations from customers, as well as other interested parties, regarding level of judgement in an equivalent manner in certification reviews
- All assignments shall be executed within the time limits agreed with the customers to the Certification Body, especially the following:
  - Reports received in certification assignments shall be reviewed and answered within the time frame agreed with the customer.
- To continuously improve the efficiency and cost-effectiveness of the evaluation and certification process for IT products and protection profiles by participation in continuous improvements by all employees at CSEC

Comments to the objectives for quality

45 The following comments will help understanding the background to the objectives for quality.

- The standards according to which the Certification Body operates are set out by the regulations for accreditation and for approval within the CCRA. The objective to fulfil these requirements implies high standards for qualities such as impartiality and confidentiality and also for a defined level of operation for management and organisation, procedures for document management, well-structured procedures for change management, and for how the certification service shall be organised and performed.
- It is of vital importance for the trust and the confidence in the services of the Certification Body that it meets all time agreements made with its customers. Although the Certification Body cannot control in detail when reports are received from the evaluation facilities it is an obvious objective for the service quality to always respond within the time agreed with the customer.

- The requirement on the certification service is that it is repeatable and reproducible, independent of who is performing the certification. It is important that the level of judgement is aligned with the market expectations for secure products as well as with the requirements from authorities and from customers of such products. Through proper information and benchmarking it is the objective of the Certification Body to set the level of judgement neither below nor beyond the level of expectations from customers and other parties with significant interest in the operations of the Certification Body
- Evaluations and certifications are performed with financial resources provided by the customers. It is important that time and money is spent in an effective way in respect of identified vulnerabilities while creating and preserving confidence in the certification system.

3.2 Policy for Quality

46 The quality policy defines the overall intentions with respect to quality and is established by the management of the Certification Body.

47 The quality policy of the Certification Body is as follows.

- The Certification Body operates a documented Quality Management System that complies with:
  - the EUCC Certification scheme
  - the CCRA arrangement
  - the SOGIS mutual recognition agreement
  - the regulations for accreditation issued by Swedac.
- The Certification Body operates structured and effective procedures for change management, safeguarding continuous improvement of the Quality Management System with respect to identified nonconformities and changes in internal, as well as external, requirements and conditions.
- The Certification Body constantly evaluates its procedures for certification and uses international benchmarking to ensure that resources and efforts for certification are effectively and efficiently applied with respect to IT security benefits.
- The Certification Body plans its assignments based on its staff resources and estimated work-load in such a way that agreements about time limits are always met.
- The Certification Body provides its services in an impartial and non-discriminatory manner to all applicants whose activities fall within its field of operation by strict adherence to the regulations documented in the Quality Management System, regardless of the status of the potential Sponsor of a certification.
- The Certification Body provides its services at prices adapted to market conditions to all applicants whose activities fall within its field of operation, with no undue financial or other conditions.
- The procedures under which the Certification Body operates are administered in a non-discriminatory manner.
- The Certification Body takes complete responsibility for all decisions relating to granting, maintaining and withdrawing certification.
- The Certification Body has established a Scheme Advisory Committee (SAC) to enable the participation of all significant interested parties in the development of policies and principles regarding the content and functioning of the certification system.

3.3 Applicable Legislation

48 A description of the national laws, subsidiary legislation, administrative regulations, and official obligations that apply to and affect the certification activities and the recognition of CC certificates is provided in CB-136 *Legal Dependencies*.

4 Independence and Impartiality

49 The Certification Body is impartial in the sense that it is free from any influence by anyone having commercial or financial interest in the outcome of the certifications.

50 The Certification Body is organised as an independent entity within the FMV, which is a civil Government authority.

51 A public authority is by law established to be independent and impartial towards any commercial or financial interest.

52 Since the Certification Body is a part of a public authority the permanent personnel of the Certification Body are Swedish civil servants for which the *Swedish law on public employment* applies.

53 The law requires a civil servant not to engage in situations or actions where his impartiality may be questioned or that may harm the confidence in the authority. The law also stipulates how such situations shall be handled.

54 The organisation of the Certification Body is implemented to safeguard impartiality in every aspect of its operations and is described in section 6, *Management and Organisation*.

55 The characteristics of the Senior Executive are described in section 6.2.1, *Management Roles*.

56 The participation of all parties significantly concerned in the development of policies and principles regarding the content and functioning of the certification system is enabled through the Scheme Advisory Committee, which is described in section 6.3.1, *Scheme Advisory Committee*.

57 The Certification Body forms a part of the legal entity The FMV. The relationship with FMV is described in section 4.3, *Separate Legal Entity*.

58 An overall description of the organisation for independence of the Certification Body is found in VB-140 *Verksamhetsbeskrivning* (in Swedish).

4.1 Policy for Independence and Impartiality

4.1.1 Background

59 The Certification Body is to ensure impartiality and independence at the following three levels.

- Strategy and policy
- Decisions on certification
- Evaluation

4.1.2 Policy

60 Independence and impartiality towards FMV is safeguarded as follows.

- Policies issued by FMV's Board apply also to the Certification Body.
- The Certification Body has a Quality Management System of its own which is described in the Quality Manual (this document).
- The operational management of the Certification Body has the exclusive authority to issue CSEC policies for the Certification Body to the extent necessary to maintain impartiality and independence in the sense described above.
- Policies for the Certification Body are issued by the Head of the Certification Body after consulting with the Senior Executive.

- The Scheme Advisory Committee shall review these rules and the observance of the rules and shall recommend actions based on any nonconformity.
- Personnel may not be used to review or make a certification decision for a product for which they have provided consultancy within the last two years.
- Any nonconformity regarding the observance of these rules shall be reported to the Scheme Advisory Committee.

61 Further information about the organisation and the management functions may be found in VB-140 *Verksamhetsbeskrivning* (in Swedish).

4.2 No Compromising Activities

62 The main purpose of the Certification Body is to provide certification services according to:

- the EUCC Scheme
- the CCRA arrangement
- the SOG-IS agreement

63 The Certification Body does not manufacture or trade in any products or systems certified under these Schemes.

64 On some occasions, the Certification Body may be involved in providing advisory services in its area of competence. Such activities will be performed according to specific policies and procedures clearly distinguished from the product certification. The Certification Body does not give prescriptive advice or consultancy as part of an ongoing certification.

4.3 Separate Legal Entity

65 The Certification Body is organised as an independent entity within the FMV, which is a civil government authority. The Certification Body is an integrated part of FMV and will make use of the overall Quality Management System of FMV and will adhere to FMV's overall policies as long as impartiality and independence is not compromised.

66 Further information about the organisation and the management functions may be found in CB-101 *Roller - Specifikation*.

67 The legal status of the Certification Body is described in detail in VB-140 *Verksamhetsbeskrivning*. (in Swedish).

68 The Certification Body has investigated and documented its relationship to the FMV and has concluded that policies and procedures established within the Certification Body eliminate any risk that would affect confidentiality, objectivity, or impartiality. The details are documented in CB-078 *CSEC Relations with The Swedish Defence Materiel Administration*.

4.4 Risk Analysis

4.4.1 Risk Imposing Situations

69 Situations that, according to ISO/IEC 17065:2012, might impose a risk include:

- self-interest (e.g. overdependence on a contract for service or the fees, or fear of losing the customer or fear of becoming unemployed, to an extent that adversely affects impartiality in carrying out conformity assessment activities);

- self-review (e.g. performing a conformity assessment activity in which the Certification Body evaluates the results of other services it has already provided, such as consultancy);
- advocacy (e.g. a Certification Body or its personnel acting in support of, or in opposition to, a given company which is at the same time its customer);
- over-familiarity, i.e. risks that arise from a Certification Body or its personnel being overly familiar or too trusting, instead of seeking evidence of conformity (in the product certification context, this risk is more difficult to manage because the need for personnel with very specific expertise often limits the availability of qualified personnel);
- intimidation (e.g. the Certification Body or its personnel can be deterred from acting impartiality by risks from, or fear of, a customer or other interested party); and
- competition (e.g. between the customer and a contracted person).

70 Such situations will be analysed during the risk analysis.

4.4.2 Yearly Risk Analysis

71 The Certification Body will perform a risk analysis regarding impartiality and independence. The analysis will cover, but not be limited to, all aspects listed in section 4.4.1 *Risk Imposing Situations*.

72 This risk analysis will be updated yearly in conjunction with the Management Review. The procedure for risk analysis is described in VB-186 *CSEC Ledning* (in Swedish). The Management Review is described in CB-117 *Quality and Change Management*.

73 During the risk analysis the relations with the FMV, described in CB-078 *CSEC Relations with The Swedish Defence Materiel Administration*, will be analysed. Any change in this relationship will lead to an update to the document, together with the necessary actions to prevent any risk identified.

4.4.3 Risk Analysis when Staffing

74 When staffing a Certification or Licensing project any risk to the impartiality and independence of the assignment will be analysed.

75 The analysis will cover the relevant aspects of section 4.4.1, *Risk Imposing Situations*. Details about such analysis are described in CB-111 *Certifiering* and in CB-110 *ITSEF Management*.

4.4.4 Continuous Risk Analysis

76 As a complement to the Yearly risk analysis and the Risk analysis when staffing projects, the Certification Body will address risks continuously at management and personnel meetings.

77 Meetings within the Certification Body are described in VB-186 CSEC *Ledning* (In Swedish)

4.4.5 Reporting to the Scheme Advisory Committee (SAC)

78 The Quality Manager is responsible for making information about any identified risk to impartiality, including actions taken to eliminate or minimise the risk, available to the Scheme Advisory Committee (see section 6.3.1, *Scheme Advisory Committee*).

5 Confidentiality

79 The Certification Body shall, to the extent permitted by the national laws, statutes, executive orders, or regulations of the participants, have adequate arrangements to ensure confidentiality of the information obtained in the course of its certification activities at all levels of its organisation and is not to make an unauthorised disclosure of protected information obtained in the course of its certification activities.

80 Documents received by, or drawn up by, the Certification Body are by definition official documents, which means that they may be kept secret only in order to protect the interests listed in The Freedom of Press Act and by referring to the correct article in The Swedish Law on Publicity and Secrecy.

81 Details on how to send documents and make the Certification Body aware of confidentiality claims and procedures for exchanging confidential information are described in EP-001 *Certification and Evaluation - Overview*.

82 The Certification Body has established procedures and arrangements consistent with applicable laws to safeguard confidentiality of the information obtained in the course of its certification activities. These are described in more detail in section 8, *Personnel Management*, and in section 15, *Security*.

83 Where the law requires information to be disclosed to a third party, the supplier will be informed of the information provided as permitted by the law.

84 All persons that take part in certifications or come into contact with information gathered during certifications are required to sign an agreement whereby they assure that they understand and will comply with the confidentiality policy described above. This applies to all personnel and contractors.

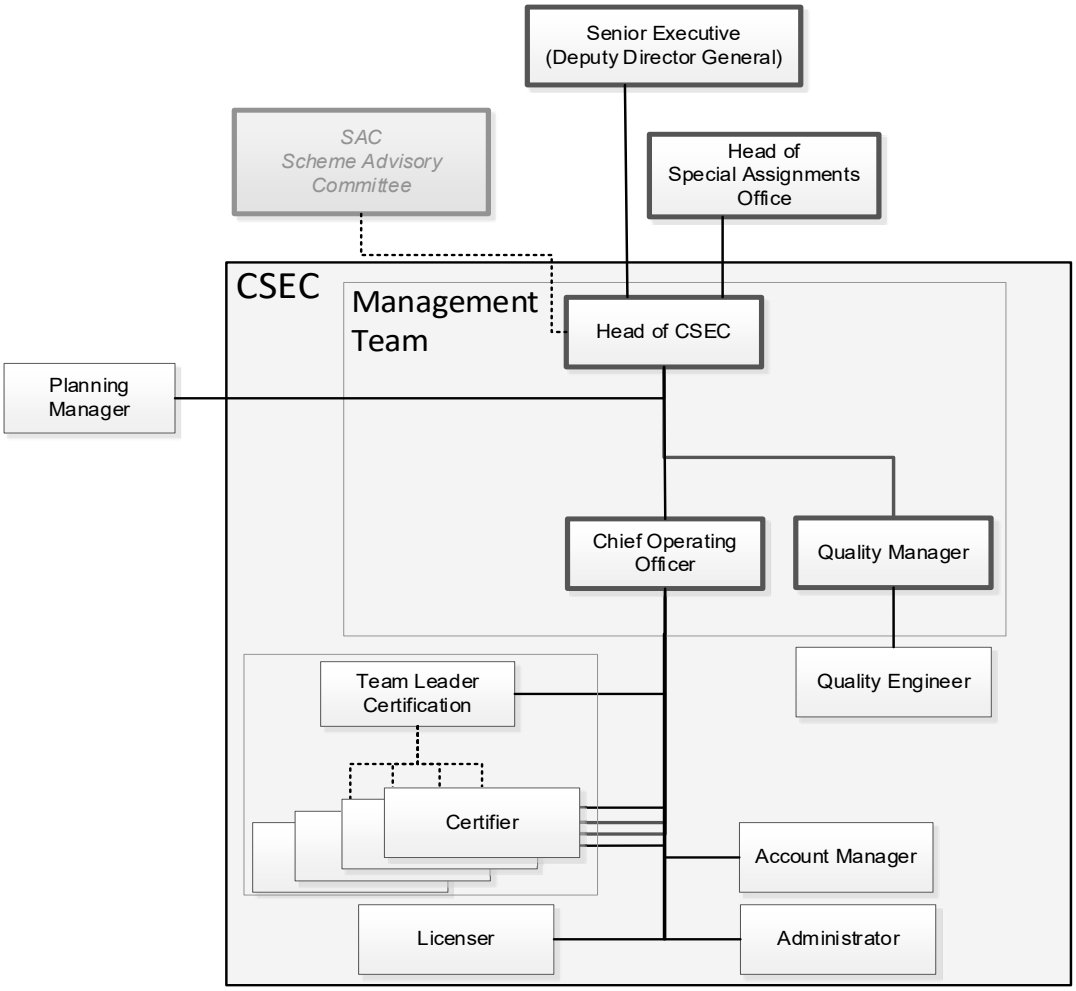
6 Management and Organisation

6.1 Organisation

85 The purpose of the organisation description is to identify the management that has overall responsibility for all of the following.

- Performance of testing, inspection, evaluation, and certification as defined in the Quality Management System
- Formulation of policy matters relating to the operation of the Certification Body
- Decisions on certification
- Supervision of the implementation of its policies
- Supervision of the finances of the Certification Body
- Delegation of authority to committees or individuals as required to undertake defined activities on its behalf
- Technical basis for granting certification

Figure: CSEC Roles



6.1.1 Organisation Description

86 Further information about the organisation and the management functions may be found in VB-140 *Verksamhetsbeskrivning* (in Swedish).

6.2 Roles

87 This section gives a brief introduction to the different roles in the Certification Body and to each role's responsibilities with the purpose of describing how the requirements from ISO/IEC 17065:2012 and CCRA are fulfilled.

88 For a full description of the roles and the organisation, see CB-101 *Roller - Specifikation* and VB-140 *Verksamhetsbeskrivning* (in Swedish).

89 Personnel Management is described in section 8, *Personnel Management*.

90 Assignment of roles within the Certification Body is made through a Staffing Decision[1] made by the Head of CSEC.

6.2.1 Management Roles

91 The following roles are part of the overall management of the Certification Body. They are described in more detail in CB-101 *Roller - Specifikation.*

Senior Executive

92 The Senior Executive is responsible for enabling day-to-day operations and setting objectives for the Certification Body.

93 The Senior Executive reports to FMV's Board.

Head of the Certification Body

94 The Head of the Certification Body, also called Head of CSEC, is responsible for the day-to-day operations within the Certification Body. The Head of the Certification Body reports to the Senior Executive.

95 The Head of the Certification Body also has the overall responsibility for Scheme changes and the handling of complaints and appeals.

96 The Head of the Certification Body may not take part in evaluation activities.

Chief Operating Officer

97 The Chief Operating Officer is responsible for managing the day-to-day operations within the Certification Body, including certification and licensing activities, in cooperation with the Head of the Certification Body.

98 The Chief Operating Officer has the responsibility and authority to evolve and improve all aspects of the services and documentation of the Certification Body.

99 The Chief Operating Officer reports to the Head of the Certification Body.

Quality Manager

100 The Quality Manager is responsible for establishing, implementing, maintaining, and operating the Quality Management System according to ISO/IEC 17065:2012 and other relevant requirements by CCRA, Swedac and FMV. The Quality Manager is also responsible for reporting on the performance of the Quality Management System to the Head of the Certification Body for review and as a basis for continuous improvement.

[1] "Bemanningsbeslut" in Swedish.

6.2.2 Other Roles

101 Other roles of vital importance in running the Certification Body are described in more detail in CB-101 *Roller - Specifikation*

102 *Process roles* may be defined in the process where they operate.

6.3 Boards and Committees

6.3.1 Scheme Advisory Committee (SAC)

103 The Scheme Advisory Committee is established to enable the participation of all parties significantly concerned in the development of policies and principles regarding the content and functioning of the certification system.

104 The main purpose of the Scheme Advisory Committee is to ensure the impartiality of the operations of the Certification Body.

105 The Scheme Advisory Committee is described in the publication EP-103 *Terms of Reference for the Scheme Advisory Committee*.

6.3.2 Management Team

106 The Management Team is established to handle strategic and overall management of the Certification Body.

107 The participants of the Management Team are as follows.

- Head of CSEC (Chairman)
- Chief Operating Officer
- Quality Manager

6.3.3 Change Control Board (CCB)

108 The Change Control Board is established to manage and control the procedures for change management and handling of nonconformities.

109 The Quality Manager, or a person appointed by the Quality Manager, is responsible for conducting the meeting.

110 All personnel at CSEC are invited to the CCB.

111 Further information about the Change Control Board is found in CB-117 *Quality & Change Management*.

6.4 Financing

112 CSEC is a non-profit organisation. The Swedish Government will provide appropriation for the operation of the Certification Body. The yearly amount will be described in the *Appropriation directions for the Swedish Defence Materiel Administration*. The Certification Body will charge fees adjusted to market conditions for its services. For further information about charges and fees, see the publication EP-008 *Charges and Fees*. The procedures for management of finances are described in VB-140 *Verksamhetsbeskrivning* (in Swedish).

6.5 Liabilities

113 As part of a civil government authority, all liabilities arising from the operations of the Certification Body will be handled according to *The Swedish Ordinance on the handling of claims for damages against the State*. The relationships between CSEC and its associated IT Security Evaluation Facilities (ITSEF), Sponsors, and Developers will be regulated in agreements that will cover liability aspects.

6.6 Project Management

114 All licensing and certification assignments are organised and managed as separate projects. Management of such projects are described in CB-110 *ITSEF Management* and CB-111 *Certifiering*.

115 The procedures for project management are based upon the procedures described in *FMV VHL*.

6.7 Management Procedures

116 Procedures for overall management of projects, tasks and other assignments are described in CB-186 *CSEC Ledning*.

7 Quality and Change Management

7.1 The Quality Management System

7.1.1 Use and Deviation

117 The policies and procedures of the Quality Management System are intended to be the best known practice to support the purpose and objectives of the Certification Body. The level of detail may vary substantially between different types of descriptions, all depending on the needs the procedure is to fulfil.

118 All work covered by the Quality Management System is to comply with these policies and procedures at the defined level of detail. If a need to deviate from the documented procedures arises, this is allowed only after consultation with the Quality Manager and a decision by authorised management or permanent personnel. Such decisions are to be properly documented, motivated, and traceable.

119 If a deviation is compelled by an error or nonconformity in the Quality Management System, or if the procedure is regarded as inefficient, a deviation shall always be preceded by a change request describing the problem leading to the need for a deviation.

120 If the deviation is caused by the circumstances for a specific task or project a change request is not required but the reason for the deviation must be clearly stated when the decision is documented.

7.1.2 Document Categories

121 The Quality Management System consists of the documentation described in section 1.2, *Documentation*.

122 The Quality Management System consists of documents internal to the Certification Body as well as publications briefly described in section 1.3, *Publications*. The main categories are distinguished by the prefix in the document identity. There are three categories of documents in the Quality Management System as follows.

Type	Description	Prefix
CB Documents	Internal documents related to Evaluation and Certification	CB
Unit documents	Internal documents relevant to CSEC as a unit within the FMV	VB
Public documents	Documents published on the external web providing information, guidelines and regulations to external interested parties	EP[2]

123 For simplicity, all documents are based on the same template which is issued in Word, and Excel versions. However there are some documents, mostly forms, which are based on a template adapted for forms.

[2] These documents are complemented by Scheme Notes.

7.1.3 Publications

124 The public part of the documentation is divided into two subcategories as follows.

External publications	External publications are the part of the Quality Management System that describes, to external interested parties, the procedures for licensing of evaluation facilities, for evaluation and certification and finally for granting certification. External publications could contain regulations as well as guidelines for the parties involved in licensing and in evaluation and certification. External publications are issued on the CSEC standard template.
Scheme Notes	Scheme Notes are short descriptions of how to interpret the rules and regulations of the scheme. Scheme Notes may be issued as a result of a Request for Interpretation or as a result of an internal decision within the Certification Body. Scheme Notes are published on the Scheme Note form and are limited to one, or at most two, pages. If there is need for more extensive documentation the Scheme Note should not be used and an External publication should be considered.

7.2 Maintenance of the Quality Management System

125 The Quality Management System is maintained through the policies and procedures for quality and change management described in this section.

126 The effectiveness and efficiency of the Quality Management System are assessed on a yearly basis through internal audits, described in section 7.4, *Internal Audits*, and the management review, described in section 7.5, *Management Review*.

127 The Certification Body has procedures, described in CB-117 *Quality & Change Management*, for change management used to implement and follow up solutions for any nonconformity and any suggestion for improvement.

128 The Quality Manager is responsible for the maintenance of the Quality Management System.

7.3 Change Control

129 The purpose of the policies and procedures for change control is to ensure that:

- the views of all significant interested parties are taken into account when the change is implemented,
- no change is introduced without authorisation from the proper management representative, and
- all interested parties are promptly informed and are in a position to take prompt and effective action.

130 This is accomplished by the following rules.

- All changes are handled in a controlled manner according to the procedures in the Quality Management System.
- All changes must be approved by the Change Control Board before implementation.
- All changes with major impact on the operation of the Certification Body are announced to the Scheme Advisory Committee and on the official website in advance of implementation of the change.

- The effectiveness and efficiency of all changes are continuously analysed by the Quality Manager and reported to the Head of the Certification Body.
- The effectiveness and efficiency of the procedures for change management are continuously analysed by the Quality Manager and reported to the Head of the Certification Body.

131 The procedures for change management, including procedures for analysis of the impact of the changes on ongoing Certifications are found in CB-117 *Quality and Change Management*.

7.4 Internal Audits

132 Internal audits are conducted according to a yearly schedule covering all procedures of the Quality Management System.

133 The internal audits are performed according to the procedures for internal audits described in CB-117 *Quality & Change Management*.

134 The Quality Manager is responsible for the planning of such audits and for the appointment of the audit team.

135 Each audit is documented in an audit report that is presented to the Head of the Certification Body and the Senior Executive.

136 All nonconformities are classified according to the classification guide found in Appendix A, *Classification of Nonconformities*, and are handled according to the procedures described in section 7.6, *Handling Nonconformities*.

7.5 Management Review

137 The management of the Certification Body conducts a Certification Body management review on a yearly basis.

138 The management review is performed according to the procedures for management reviews described in CB-117 *Quality & Change Management*.

139 The Quality Manager is responsible for scheduling and planning the management review. The Quality Manager is also responsible for all preparations and material needed.

7.6 Handling Nonconformities

140 Any suggestion for improvement and all findings that may represent a problem, defect or nonconformity shall be documented (as a change request) and reported to the Quality Manager.

141 The resolution may be a correction, a corrective action, a preventive action or a combination thereof.

142 A preventive action is an action to eliminate the cause of a potential nonconformity or other undesirable potential situation.

143 A corrective action is an action to eliminate the cause of a detected nonconformity or other undesirable situation.

144 A correction is an action to eliminate a detected nonconformity.

145 Nonconformities with major impact on the ability to fulfil the requirements for mutual recognition are reported to the Senior Executive and the Scheme Advisory Committee.

146 The decisions about corrections, corrective actions and preventive actions are made at the Change Control Board (CCB).

147 Nonconformities are handled according the procedures described in CB-117 *Quality & Change Management*. The details of the change control process are described in CB-139 *Ändringsstyrning* (in Swedish).

7.7 Configuration Management

148 The Certification Body will introduce new versions of the Quality Management System at regular intervals or when necessary.

149 The procedures for configuration management are used to establish a complete version of the Quality Management System.

150 The Version Description Documents described in section 1.2.3, *Version Description Documents*, will identify the versions of each document or process that constitute the version of the Quality Management System.

151 Release notes that describe the changes since the previous version of the Quality Management System will accompany each new version of the Quality Management System.

152 The procedures for configuration management are described in CB-149 *Releasehantering. (Eng: Release Management)*

7.8 Changes in Requirements for Certification

7.8.1 Requirements from the Standards

153 The requirements for certification consist of the standards described in section 11.4, Relevant Standards.

154 Changes to the standards will be introduced according to the regulations issued by the organisation responsible for the standard.

155 The standards, and the versions of these standards, used in a certification will be documented in the Certificate and in the certification report.

7.8.2 Requirements in the Quality Management System

156 The Quality Management System mainly consists of procedural regulations but may impose requirements for certification.

157 A change to the requirements for certification issued by the Certification Body, will be handled as follows.

- The change will be managed according to the procedures for change control described in section 7.3, *Change Control*.
- All parties affected by the change will be informed according to the procedures described in section 7.9, *Information about Changes*.

158 Changed requirements for certification, introduced through changes to the Quality Management System, are not mandatory if they were not made known to the customer before the Application for Certification was made.

159 If such changes are introduced, and not applied to an ongoing certification, this will be described in the certification report.

7.8.3 Introducing Changed Requirements

160 If a customer wants a certification to be performed according to updated requirements the following actions will be taken.

- An analysis, identifying all parts of the evaluation and certification that are affected by the change, will be performed.

- A detailed analysis of how the evaluation and certification is affected will be performed.

161 If the customer wants to complete the change based on the result of the analysis, all parts of the evaluation and certification affected by the change will be updated.

162 These actions are performed under the responsibility of the Lead Certifier in each certification.

7.9 Information about Changes

163 The Certification Body is to ensure that changes are promulgated in such way that those who need to know are promptly informed and are in a position to take prompt and effective action. This is done through the procedures for information management described in section 10, *Information Management*.

164 The policy for information about changes is as follows.

- All changes to CSEC:s External Publications are published on the official website.
- All changes with major impact on the operation of the Certification Body are announced to the Scheme Advisory Committee and on the official website in advance of implementation of the change.
- All interested parties may subscribe to information about changes. Such information will be distributed by e-mail.

7.10 Accreditation

165 The Quality Manager is responsible for ensuring that the Certification Body, at all times, fulfils the requirements for accreditation as defined in relevant instructions from Swedac.

166 The Quality Manager is responsible for notifying the accreditation body of any changes that might affect the Certification Body's ability to fulfil the conditions for accreditation, as defined in section 10.4, *Information Related to Accreditation*.

167 If the Certification Body should wish to have its accreditation withdrawn, the Senior Executive is responsible for notifying the accreditation body of this, in writing.

168 If the Certification Body has had its accreditation withdrawn, the Head of the Certification Body is responsible for taking steps to ensure that no reference is made to the accreditation.

8 Personnel Management

169 The Certification Body, through FMV, employs permanent personnel and has access to consultants to cover its operations.

170 The personnel include those working for the Certification Body, as well as persons working under a formal agreement that places them within the management control and systems/procedures of the Certification Body.

- Permanent personnel or employees, as used in the Quality Management System, only include personnel employed by the Certification Body.
- Consultants, as used in the Quality Management System, work under a formal agreement.
- Personnel or staff, as used in the Quality Management System, include both permanent personnel/employees and consultants.

8.1 Personnel Resources Administration

171 The Certification Body is formally organised within a unit at FMV. More information about the organisation is found in VB-140 *Verksamhetsbeskrivning* (in Swedish).

172 The Head of the Certification Body is responsible for ensuring that the Certification Body has a sufficient number of personnel for the type, range, and volume of work performed.

173 The Head of the Certification Body will report needs for competence and personnel to the Senior Executive and to the manager of the unit, in which the Certification Body is organised. According to FMV's procedures it is the unit manager that is responsible for assisting the Certification Body in providing sufficient resources.

174 Personnel involved in licensing and certification are assigned to work according to the Quality Management System of the Certification Body.

175 The permanent personnel is ensured by the Senior Executive. The number of permanent personnel cannot be changed without approval by the Head of the Certification Body and authorisation from the Senior Executive. The details of these procedures are documented in VB-140 *Verksamhetsbeskrivning* (in Swedish).

8.2 Financially and Commercially Independent Personnel

176 According to the requirements from ISO/IEC 17065:2012 and CCRA and according to the policy of the Certification Body, the personnel of the Certification Body shall be free from any commercial, financial, or other pressures that might influence the results of the certification process.

177 Because the Certification Body is a part of a public authority, the permanent personnel of the Certification Body are Swedish civil servants for which the *Swedish law on public employment* applies.

178 The Head of the Certification Body is responsible for ensuring that all permanent personnel are informed about this law and in which situations it may be applicable.

179 The Head of the Certification Body is responsible for requesting all permanent personnel to report any condition necessary for the Certification Body to make judgement on any complementary occupation on behalf of the employee.

180 For subcontractors and personnel working under a formal agreement see section 8.5 Agreement.

8.3 Competence Development

181 Competence development is performed according to the procedures for competence development described in CB-202 *CSEC Kompetensledning* (in Swedish), and in *FMV VHL*.

182 The manager of the FMV unit is responsible for competence development common to all FMV permanent personnel and for maintaining plans for this competence development.

183 The Head of the Certification Body has overall responsibility for competence development that falls into the field of operation of the Certification Body.

184 The Chief Operating Officer has overall responsibility for any necessary supplementary competence development needed within a project or a specific assignment.

8.4 Recruitment

185 Recruitment is performed according to the procedures described in *FMV VHL*.

186 During the recruitment process, the Head of the Certification Body is responsible for the following.

- Ensuring that the permanent personnel is informed about the *law on public employment* and its impact
- Requesting the permanent personnel to report any condition necessary for the Certification Body to make judgement on any complementary occupation on behalf of the employee

8.5 Agreement

187 When entering the Certification Body, all personnel, including those acting in a managerial capacity, and each subcontractor who will be involved in the certification process will be required to sign the CB-057 *CSEC Impartiality agreement - Form* stating that they will:

- comply with the rules defined by the Certification Body, including those relating to confidentiality and independence from commercial and other interests;
- declare any prior and/or present association on their own part, or on the part of their employer, with a supplier or designer of products relevant to the evaluation or certification to which they are to be assigned; and
- reveal any situation known to them that may present them or the Certification Body with a conflict of interest.

188 The Head of the Certification Body is responsible for ensuring that these agreements are signed and saved in the personnel file.

189 The Head of the Certification Body is responsible for using the information as input into identifying risks to impartiality raised by the activities of such personnel, or by the organisations that employ them.

8.6 Personnel File

190 The Certification Body maintains information on the relevant qualifications, training, and experience of all personnel involved in the certification process.

191 All records relevant for ensuring that the personnel involved in the certification process have the necessary education, training, technical knowledge, and experience for performing certification work are kept in individual personnel files.

192 The personnel files are described in CB-202 *CSEC Kompetensledning (in Swedish)*.

8.7 Performance Monitoring

193 The management in charge of the operations of the Certification Body continuously monitors the performance of its personnel. Performance monitoring of the permanent personnel is described in CB-202 *CSEC Kompetensledning (in Swedish)*. Consultants are monitored through continuos discussions with the permanent personnel that is supported by the work of the consultant.

8.8 Individual Job Description

194 The roles in the organisation of the Certification Body are described in detail in CB-*101 Roller - Specifikation*. The document contains description of the duties and responsibilities for each role. The roles of Senior Executive, Head of the Certification Body, Chief Operating Officer and Quality Manager are considered to be of special importance to the quality of the Certification Body's services and are described in section 6.2, Roles, of this Quality Manual.

195 Each permanent personnel is appointed to one or more roles, by which the duties and responsibilities are uniquely identified.

8.9 Qualifications

8.9.1 Certifiers

196 Permanent personnel involved in certification activities will be designated as certifiers. Although higher evaluation levels require considerably more certification experience, no classification of certifiers is made based on specific evaluation assurance levels (EAL).

197 Certifiers should fulfil at least the following competence requirements.

- Bachelor or Master of Science in Engineering, or corresponding qualifications acquired in another manner
- At least 5 years of qualified technical experience in the field of IT security
- Completion of the CSEC Certifiers Training Course
- Participation in at least one evaluation effort
- Introduction to the Quality Management System of the Certification Body

198 Contracted personnel may be appointed as certifiers if they fulfil the requirements to become certifiers.

199 Decisions about appointments as certifiers are made by the Head of the Certification Body. Decisions shall be documented.

200 A diploma, signed by the Head of CSEC, is issued to each appointed certifier using CB-189 *Certifier Diploma - Form*.

8.9.2 Certifier Assistants

201 Personnel involved in certification activities may be designated as Certifier Assistants. Such personnel may perform certification tasks under close supervision of a Certifier.

202 Certifier Assistants should fulfil at least the following competence requirements.

- Post-secondary education in Engineering, or corresponding qualifications acquired in another manner
- Valid technical experience in the field of IT security
- Completion of the CSEC Certifiers Training Course, or education deemed equivalent by the Certification Body
- Introduction to the Quality Management System of the Certification Body

203 Decisions about appointments as Certifier Assistants are made by the Head of the Certification Body and is documented.

8.9.3 Other Permanent Personnel

204 Permanent personnel other than Certifiers are appointed based on competence requirements documented in CB-101 *Roller - Specifikation*. The appointments are made by the Head of CSEC and shall be documented. See also CB-202 *CSEC Kompetensledning* (in Swedish).

8.10 Assignments and Projects

205 The Chief Operating Officer is responsible for the assignments of the Certification Body and assigns personnel for the necessary work.

206 Assignment of certification projects is described in CB-111 *Certifiering.* The Lead Certifier acts as project manager for the certification project.

207 Assignment of licensing projects is described in CB-110 *ITSEF Management*. The Licenser acts as project manager for the licensing project.

208 The Chief Operating Officer assigns the roles of the project. The Chief Operating Officer is responsible for ensuring that all personnel assigned to a project have relevant competence for the tasks they are to undertake.

209 When assigning Certifiers to a certification project, the criteria for minimum relevant competence described in section 8.9.1, Certifiers, must be taken into account.

210 The Head of the Certification Body is responsible for ensuring that neither the project manager nor any other personnel assigned to the project have been involved in any of the activities listed below with regard to the applicant or supplier in question or anybody related to the supplier within the last two years.

211 The following activities or situations may present individuals involved in any part of the certification process with a conflict of interest.

- Provision or design of products of the type that is to be certified
- Provision of advice or consultancy services to the applicant on methods of dealing with matters that are barriers to the certification requested
- Present or previous involvement with the supplier of the product being evaluated

212 The Head of the Certification Body is responsible for investigating any such situation and for taking appropriate actions.

213 The details of the FMV procedures are described in *FMV VHL*.

8.11 Reporting Conflicts of Interest

214 Each individual involved in certification activities is required to report to the management of the Certification Body any situation which may present the individual with a conflict of interest.

215 The Head of the Certification Body decides how to handle each reported situation. The decision shall be documented.

9 Document Management

9.1 Handling of Documents

216 Documents created within the Certification Body are produced, approved, registered, and archived according to the procedures for creating and updating documents in CB-173 *Dokumenthantering* (in Swedish).

217 Incoming documents are registered and archived according to the procedures for managing incoming documents in CB-173 *Dokumenthantering* (in Swedish).

9.2 Confidentiality

218 Because the Certification Body is a public authority, special rules regarding confidentiality of information and documents apply. The confidentiality policy for the Certification Body can be found in section 4.4.4, Continuous Risk Analysis. By definition, documents received by or drawn up by the Certification Body are official documents to which the principle of public access to official documents is applicable.

9.2.1 Background Information

Official documents

219 A *document* is a presentation in writing or images or recording that can be read, listened to, or comprehended in another way, for example: using technical aids.

220 A document is *official* if it is:

- held by a public authority and
- according to special rules, regarded as having been received or drawn up by a public authority.

The principle of public access to official documents

221 The principle of public access to information means that the public and the mass media are entitled to receive information about state and municipal activities. The principle of public access to information is expressed in various ways. Those of importance to the Certification Body are as follows.

- Anybody whosoever may read the documents of authorities: *Access to official documents.*
- Civil servants and others who work for the state or municipalities are entitled to say what they know to outsiders: *Freedom of expression for civil servants and others.*
- Civil servants and others in the service of the state or municipalities have special powers to disclose information to newspapers, radio, and television: *Communication freedom for civil servants and others*.

9.2.2 Rules for Confidentiality within the Certification Body

222 Official documents within the Certification Body may be kept confidential according to the following articles in The Swedish Law on Publicity and Secrecy.

15 Chap. Art. 1, 2	Regarding the security of the realm or its relationships with another state or international organisation
17 Chap. Art. 1, 4	Regarding inspection, control, or other superviso-

	ry activities of a public authority
18 Chap. Art. 2, 8	Regarding the interest of preventing or prosecuting crime
19 Chap. Art. 1, 3	Regarding the economic interests of the public institutions
21 Chap. Art. 7 31 Chap. Art. 12, 16, 17, 20-23 39 Chap. Art. 1, 2, 3, and 5	Regarding the protection of the personal or economic circumstances of private subjects

223 Further details about the rules for confidentiality are documented in VB-132 *Sekretessregler CSEC* (English: *Rules for Confidentiality within CSEC*).

224 All personnel involved in licensing and certification are educated in the meaning of these rules and how the procedures for confidentiality within the Certification Body are implemented.

225 The procedures for confidentiality are described in VB-102 *Lokal säkerhetsskyddsföreskrift* (English: *Local Security Regulation*).

9.3 Superseded Documents

226 The valid versions of all working documents are published either at the internal or the external website of the Certification Body according to the procedures described in section 10, *Information Management*. Such documents are marked with the following text.

Uncontrolled copy when printed

227 If documents are printed or copied from the website, they are no longer controlled and may not be used in licensing or certification unless the user can verify the correctness of the document.

228 Documents or versions of documents which are superseded or for any other reason no longer valid, are immediately withdrawn from the websites. Relevant interested parties are informed about the withdrawal and if applicable, about the new document or version.

9.4 Records

229 Since the Certification Body is part of a public authority the principle of public access to official records apply. This means that every document sent to the Certification Body, and every document drawn up within the Certification Body, will be registered in the diary and archived according to Swedish law. This applies to records as well as to any other document. Confidentiality is safeguarded by the policies and procedures described in section 5, *Confidentiality*, and in section 15, *Security*. Applicable legislation is listed in CB-136 *Legal Dependencies*.

230 The details of which records are produced and handled within the Certification Body are found in the description of the procedure in which the record is produced.

231 Records drawn up within the Certification Body are handled according to the procedures for document management described in this section and in CB-173 *Dokumenthantering* (in Swedish).

232 Incoming records, such as information gained within the Licensing and Certification processes are, handled according to the procedures for document management described in this section and in CB-173 *Dokumenthantering* (in Swedish).

233 Since records are official documents, they are stored in public archives according to the procedures for archiving described in section 9.1, *Handling of Documents*.

10 Information Management

234 The purpose of the procedures for information management is to ensure that all significant interested parties always have information about and access to the relevant documentation and information about the operations of the Certification Body. The primary channel for spreading information to external parties is the website of the Certification Body.

235 The website of the Certification Body shall be updated when:

- a new version of the Quality Management System has been issued,
- a certificate has been issued or withdrawn,
- an interpretation has been issued or withdrawn, or
- information about a licensed ITSEF has changed. (e.g., licensing status, address)

236 Interested parties shall be notified by e-mail through predefined send lists.

237 Changes or prospective changes to Swedish laws, administrative regulations, or official obligations, or evaluation and certification operations or procedures that may affect the ability of the Certification Body to act consistently with the terms of the CCRA shall be distributed by the Certification Body through the Swedish CCRA Member to participants.

238 New Certificates and certification reports will be made available on the website of the Certification Body and to CCRA participants.

239 All documents published electronically will be made available in PDF format except for forms that will be published in MS Word format.

10.1 Distribution

240 The Certification Body will maintain a list of all appropriate documents including information about issue and/or amendment status.

241 Distribution of all such documents is controlled to ensure that the appropriate documentation is made available to personnel of the Certification Body and to all relevant interested parties, depending on the contents of the document.

- The Administrator is responsible for keeping the website of the Certification Body updated about the general documentation maintained by CSEC.
- The Administrator is responsible for providing notifications to external requestors whenever the document is changed, according to instructions in CB-124 *Informationsledning.*.
- The Administrator is responsible for the publication of all new versions of public documents on the CSEC website.
- The Certification Body documentation, including the lists of certified products and protection profiles, is published on the CSEC website and may also be requested through contact with the Administrator or the Certification Body.
- All documentation produced by the Certification Body is stored and archived according to the procedures in section 9, *Document Management*.
- The Administrator is responsible for ensuring that all documentation that needs to be available to the personnel of the Certification Body, including its subcontractors, is published in proper format on the internal web of the Certification Body.
- The Administrator is responsible for the information to be provided to the participants of the CCRA according to the description in section 10.3, *Information to Participants*.

- The Administrator is responsible for the document list, including amendments, according to the procedures in section 9, *Document Management*..

242 Details about distribution of documents are described in CB-124 *Informationsledning.*

10.2 Publishing

243 The table below indicates which information is to be published and in which document the information is originally found. These documents are published at the CSEC website.

Information	Source document
Information about the authority under which the Certification Body operates	EP-007 Quality Manual
Documented statement of the product certification system, including the rules and procedures for granting, maintaining, extending, suspending, and withdrawing certification	EP-007 Quality Manual EP-002 Evaluation and Certification
Description of the means by which the organisation obtains financial support	EP-007 Quality Manual
General information on the fees charged to applicants and to suppliers of certified products	EP-008 Charges and Fees
Description of the rights and duties of applicants and suppliers of certified products	EP-002 Evaluation and Certification
Requirements, restrictions, or limitations on the use of the Certification Body's logo and on claims related to the certification granted	EP-001 Certification and Evaluation - Overview
Information about procedures for handling complaints and appeals	EP-007 Quality Manual
Information about withdrawn CC Certificates	N/A
Directory of certified products and their suppliers	N/A
Directory of interpretations	N/A
Directory of explanations	N/A

244 The Head of the Certification Body is responsible for ensuring that all of this information is published and that all published documents are up to date.

245 The Administrator is responsible for the actual publishing.

246 Details about the publishing activities are described in CB-124 *Informationsledning.*

10.3 Information to Participants

247 The Administrator is responsible for providing the CCRA Participants with copies of certain documents concerning the Certification Body.

248 The Administrator is also responsible for providing the CCRA Participants with copies of the amendments or the new versions whenever changes are made to the documents or new versions are issued.

249 The table below indicates which information is to be provided and in which document the information is originally found.

250 Details about the procedures for providing information to the CCRA participants are described in CB-124 *Informationsledning*.

Information	Document/Source
The national set of rules and regulations for evaluation and certification/validation in accordance with mutually-agreed IT security evaluation criteria and methods	EP-002 Evaluation and Certification
The organisational structure of the Certification Body	EP-007 Quality Manual
The Quality Manual of the Certification Body	EP-007 Quality Manual
The accreditation or licensing/approval policy of the Certification Body	EP-004 Licensing of Evaluation Facilities
The titles and addresses of the ITSEFs licensed by the Certification Body and their status (e.g., governmental or commercial)	Licensing decisions from CSEC document archive
The national interpretation of ISO/IEC 17025: General requirements for the competence of testing and calibration laboratories.	SS-EN ISO/IEC 17025

10.4 Information Related to Accreditation

251 The Quality Manager is responsible for notifying the accreditation body, in writing, of any changes that might affect the Certification Body's ability to fulfil the conditions for accreditation. This includes the following.

- Change of key persons or key functions
- Organisational changes
- Physical moving of the whole or parts of the business to new premises, establishing new business premises, or closing down business at existing premises
- Loss of essential equipment
- Change of name of the certification body
- Change of ownership
- Substantial change in the number of persons involved in work within the scope of the accreditation
- Use of subcontractors for work within the scope of the accreditation

11 Schemes and regulations

11.1 Schemes

252 The certification body operates within several different schemes corresponding to the arrangements of mutual recognition described in chapter 2 Mutual Recognition.

11.2 Regulations of the Certification Body

253 The regulations of the Certification Body are documented in the following documents.

EP-001 Certification and Evaluation - Overview

254 This document contains a general description of certification and evaluation under the CCRA and SOG-IS agreements. It is the public top document of the CSEC CCRA/SOG-IS certification regulations. The document contains a brief description about the operations of the Certification Body and describes roles, definitions, and abbreviations important for the understanding of the information.

255 This is an informative document and is not to be regarded as controlling. It does not contain any information or specifications that are not declared or defined elsewhere.

EP-301 Certification and Evaluation - EUCC - Overview

256 This document contains a general description of certification and evaluation under EUCC. It is the public top document of the CSEC EUCC certification regulations.

257 The document contains a brief description about the operations of the Certification Body and describes roles, definitions, and abbreviations important for the understanding of the information.

258 This is an informative document and is not to be regarded as controlling. It does not contain any information or specifications that are not declared or defined elsewhere.

EP-002 Evaluation and Certification

259 This document describes the policy and procedures for evaluations and certifications performed by the Certification Body It provides sufficient information to each party in the evaluation and certification process; defining their responsibilities for maintaining a consistent and high quality and for cost effectiveness.

EP-003 Assurance Continuity

260 This document references the requirements and procedures for the

261 continuous maintenance of certifications.

EP-004 Licensing of Evaluation Facilities

262 This document describes the requirements and procedures for licensing and for the maintenance of licenses of evaluation facilities.

11.3 Scheme Owners

11.3.1 CCRA and SOG-IS

263 According to the *A R R A N G E M E N T on the Recognition of Common Criteria Certificates In the field of Information Technology Security* and the SOG-IS *Mutual Recognition Agreement of Information Technology Security Evaluation Certificates* each compliant Certification Body manages an Evaluation and Certification/Validation Scheme.

264 In that respect CSEC is the owner of the scheme for evaluation and certification within CCRA and SOG-IS.

265 The regulations for these schemes are owned by the members of the arrangements.

11.3.2 EUCC

266 *The COMMISSION IMPLEMENTING REGULATION (EU) .../... of XXX establishing the Common Criteria-based European cybersecurity certification scheme (EUCC)* is owned by the EU Commission.

11.4 Relevant Standards

267 The Certification Body performs certification according to the official versions of the standards below. The details of the operations of the Certification Body are described in the documents referred to in section 11.2 Regulations of the Certification Body.

11.4.1 CCRA

268 The standard for how certification is performed is *Common Criteria for Information Technology Security Evaluation*, which includes the following documents.

- CC Part 1: Introduction and general model
- CC Part 2: Security functional requirements
- CC Part 3: Security assurance requirements

269 The methods for evaluations and certifications are described in *Common Methodology for Information Technology Security Evaluation (CEM).*

270 The versions used are the latest versions approved by the CCRA.

11.4.2 ISO/IEC

271 The standard for how certification is performed is ISO/IEC 15408 *Information technology — Security techniques — Evaluation criteria for IT security*, which includes the following documents.

- ISO/IEC 15408 Part 1: Introduction and general model
- ISO/IEC 15408 Part 2: Security functional requirements
- ISO/IEC 15408 Part 3: Security assurance requirements

272 The methods for evaluations and certifications are described in ISO/IEC 18045 *Information technology — Security techniques — Methodology for IT security evaluation*

273 The versions used are the latest versions issued by ISO/IEC.

11.5 Certification Management

11.5.1 Information about Certification

274 The Certification Body provides information on the external web about the evaluation and certification procedures and the documents containing the requirements for certification, applicants' rights, as well as duties of suppliers of certified products (including fees to be paid by applicants or suppliers of certified products).

275 Information needed by the Certification Body personnel involved in certification can be found in the publication EP-002 *Evaluation and Certification* and in the process description CB-111 *Certifiering*.

276 For Evaluation and Certification of target of evaluations with cryptographic functionality, the Certification Body has a specific Policy described in EP-188 *Scheme Crypto Policy*.

11.5.2 Pre-evaluation

277 During pre-evaluation, the Certification Body shall:

- review the formal application for certification,
- ensure the ITSEF's ability to perform the certification,
- approve evaluator assignments,
- plan the certification project and assign personnel, and
- handle re-evaluations.

278 Details about the pre-evaluation activities are described in the procedures for *pre-evaluation* in the publication EP-002 *Evaluation and Certification* and in the process description CB-111 *Certifiering*.

11.5.3 Applications to be considered related to national security

279 CSEC is obliged to take national safety interests into account in its operations.

280 Procedures describing how to handle applications where national safety interests must be taken into account are described in CB-012 *Specialhantering av ansökningar - Nationell säkerhet*.

11.5.4 Extending or Reducing the Scope of a Certification

281 Procedures for handling extending or reducing the scope of certification are described in the publication EP-002 *Evaluation and Certification* and in the process description CB-111 *Certifiering*.

11.5.5 Conduct of Evaluation

282 During the conduct of evaluation phase, the certifier shall:

- monitor the evaluation and
- review evaluation reports.

283 Details about conduct of evaluation activities are described in the procedures for *Conduct of evaluation* in the publication EP-002 *Evaluation and Certification* and in the process description CB-111 *Certifiering*.

11.5.6 Conclusion of Evaluation

284 During the conclusion of evaluation phase, the Certification Body shall:

- verify that non-conformances are resolved,
- decide whether or not to certify a product,
- issue certificates,
- publish certificates and certification reports, and
- update the certified product list or certified protection profile list.

285 Details about conclusion of evaluation activities are described in the procedures for *Conclusion of Evaluation* in the publication EP-002 *Evaluation and Certification* and in the process description CB-111 *Certifiering.*

11.5.7 Assurance Continuity

286 During Assurance Continuity, the Certification Body shall:

- maintain certification.

287 Details about Assurance Continuity activities are described in the procedures for *Assurance Continuity* in EP-003 *Assurance Continuity* and in the process description CB-112 *Rutiner för tillsyn och underhåll av certifikat.*

11.5.8 Certificate Surveillance

288 The Certification Body shall perform certificate surveillance, including:

- monitoring the use of certificates and marks,
- monitoring the supplier's handling of complaints, and
- handling misuse of certificates and marks.

289 Details about certificate surveillance activities are described in the procedures for *Certificate Surveillance* in the publication EP-002 *Evaluation and Certification* and in the process description CB-112 *Rutiner för tillsyn och underhåll av certifikat*.

11.5.9 Withdrawal/Suspension of Certificates

290 The Certification Body shall withdraw certificates when appropriate.

291 Details about withdrawal of certificates are described in the procedures for *withdrawal of certificates* in the publication EP-002 *Evaluation and Certification* and in the process description CB-112 *Rutiner för tillsyn och underhåll av certifikat*.

11.5.10 Certificate/Marking

292 The use of certification marks shall follow the requirements stated in the publication EP-001 *Certification and Evaluation - Overview*.

293 Conditions for the use of trademarks applicable to the certification and licensing processes are listed in EP-070 *Conditions for the Use of Trademarks*.

11.6 ITSEF Management

294 The Certification Body shall:

- perform licensing of ITSEFs,
- provide a documented agreement between the Certification Body and the ITSEF consisting of the ITSEF application for licensing and the Certification Body acceptance of the application,
- publish a list of ITSEFs,
- perform audit and review of evaluation facilities, and
- provide guidance and technical support to evaluation facilities.

295 The procedures for Licensing of Evaluation Facilities are described in the publication EP-004 *Licensing of Evaluation Facilities* and in the process description CB-110 *ITSEF Management*.

296 The Policy for licensing of Evaluation Facilities, and performing evaluations, outside Sweden is described in EP-191 *Cross Frontier Evaluation*.

297 Details about the publishing activities are described in CB-124 *Informationsledning.*

11.7 Mutual Recognition and International Liaisons

11.7.1 CCRA

298 Sweden has signed the Common Criteria Arrangement on the Mutual Recognition of Common Criteria Certificates in the field of Information Technology Security (CCRA), thus accepting CC certificates issued in other countries.

299 CCRA compliance ensures mutual recognition of CC certificates at EALs up to and including EAL 4, possibly augmented by Flaw Remediation, among the CCRA participants.

300 CSEC intends to follow, participate in, initiate, and lead activities aiming to promote IT security in general, and IT security evaluation in particular, both within and outside the CCRA framework.

301 As a CCRA-compliant Certification Body, CSEC must undergo a voluntary periodic assessment (VPA) at least once every five years, as requested by the CCRA Management Committee. During these assessments, it is CSEC's responsibility to support the assessment team to the greatest possible extent, sharing internal scheme documentation and evaluation documents, in accordance with the requirements of CCRA Annex D.

302 If Sweden is recognised as a Qualified Participant in CCRA, and CSEC achieves the status of an Associated Certification Body, CSEC will share the responsibility for performing voluntary periodic assessments with any other Associated Certification Bodies.

303 When sharing protected information with other CCRA participants, for example during a voluntary periodic assessment, CSEC will follow the special rules described in CCRA Annex F.4, regarding the marking, storing, and safeguarding of such information.

11.7.2 EA MLA

304 Sweden participates through Swedac in the EA.

305 For further information about mutual recognition within EA see section 2.3, *European Accreditation* Multilateral Agreement (EA MLA).

11.8 Interpretations

306 The uniform application of the requirements of the CC and the Common Methodology (CEM) over time s assured through the use of interpretations.

307 Whenever a situation occurs in the context of an evaluation the Certification Body will have to choose a course of action, possibly based upon subjective judgement. Such choices must be documented as Scheme Notes.

308 A request for clarification of the certification regulations is called a request for interpretation. The use of the publication EP-094 *Request for Interpretation -Form* is recommended, but not mandatory. If an Interpretations request is rejected the person filing the request shall be informed about this by the Chief Operating Officer.

309 Scheme Notes relevant to the current version of the certification regulations must always be considered in subsequent certifications.

310 Scheme Notes shall be processed in accordance with the procedures for change management.

311 Descriptions of the CSEC procedures for handling changes is found in EP-007 *Quality Manual* and more detailed descriptions in CB-117 *Quality and Change Management.*

12 Customer Satisfaction

312 Feedback of any kind, from customers and other interested parties, regarding a project or any other matter concerning the activities of the Certification Body, should be handled based upon judgement from the person responsible for the matter.

313 Follow-ups will be performed during or after feedback originating from any of the following.

- Licensing
- Certification
- Spontaneous reactions

314 The Quality Manager is responsible for performing customer satisfaction surveys, using the questions in the form *Kundnöjdhetsundersökning – Blankett*. Customer satisfaction surveys are planned to be performed yearly. The Administrator is responsible for providing the list of customers for customer surveys. If there has been no progress in a project since the last answered survey that customer may be excluded from the list of customers for customer surveys that year.

315 If the survey is performed during a meeting the result should be documented in *Kundnöjdhetsundersökning – Blankett* or in minutes or a protocol from the meeting. All non-conformances are documented as change requests according to the procedures described in CB-117 *Quality & Change Management.*

316 The result from customer satisfaction surveys are reported to the Scheme Advisory Committee.

317 Spontaneous customer reactions are registered as change requests according to the procedures described in CB-117 *Quality & Change Management* Complaints are handled according to the procedures for handling complaints, described in section 13, *Complaints and Appeals*.

13 Complaints and Appeals

318 The purpose of the procedures for management of complaints and appeals is to ensure that:

- the Certification Body has suitable policies and procedures for the resolution of complaints and appeals,
- details of the procedures for handling complaints and appeals are documented and published according to applicable standards,
- the Certification Body has procedures to correct decisions that are not made according to the Quality Management System, and
- the Certification Body has procedures to learn from any complaints or appeals and to update the Quality Management System accordingly.

319 A detailed description of the procedures for management of complaints and appeals are found in this section.

320 Only complaints and appeals that apply to the certification activities of the Certification Body will be addressed using the procedure below. Other complaints or appeals may, if deemed relevant, be handled as change requests but without any formal status.

13.1 Complaints

321 The Certification Body will document and investigate any complaint directed towards it that applies to the certification activities for which it is responsible.

322 All such complaints will be registered as change requests that will be handled according to the procedures described in CB-117 *Quality & Change Management*. To separate Complaints from other change requests the title will begin with the keyword *Complaint.*

323 All identified nonconformities will be handled according to the procedures for handling nonconformities described in section 7.4, *Internal Audits*.

324 The Quality Manager is responsible for:

- confirming whether the complaint relates to the certification activities,
- informing the complainant that the complaint has been received and that it will be treated as a complaint,
- documenting and recording the complaint as a change request and presenting it to the Change Control Board for further handling,
- ensuring that the complaint is investigated and handled at the proper level of authorisation within the Certification Body, and
- ensuring that all nonconformities are handled accordingly.

325 The person to whom the complaint is assigned is responsible for:

- investigating the complaint and if necessary seeking the aid of impartial and independent technical experts;
- determining whether the decision made or action performed has been made on false grounds, in conflict with the scheme regulations (ISO/IEC 17065:2012, CC, CEM, scheme specific documents), or for any other reason is found to be incorrect;
- establishing a plan for implementation of corrective actions; and
- documenting the corrective actions taken in the change request, and reporting to the Change Control Board.

326 The resolution of the Complaint is handled according to the normal procedures for change requests.

327 The Head of the Certification Body is responsible for the decision, at the Change Control Board, about a complaint.

328 When the Complaint has been closed, the Quality Manager will:

- ensure that the complainant is informed about the outcome of the complaint,
- inform the complainant of his/her right to appeal,
- report the complaint and the corrective actions to the Head of the Certification Body and ensure that further identified nonconformities are reported and handled, and
- ensure that relevant documentation is placed under document control.

329 The Head of the Certification Body will:

- make the complaint available to the Scheme Advisory Committee upon request.

330 Forms for complaints can be found on the CSEC website: http://www.csec.se. The use of these forms is not mandatory.

13.2 Appeals

331 A complainant that is not satisfied with a decision, or with the outcome of a complaint, that applies to the certification activities for which the Certification Body is responsible may file an appeal.

332 The appeal shall be made within 30 days of the original decision, it shall be made in writing, and it shall contain the following information:

- the decision that is appealed;
- the requested change; and
- the name, address, and telephone number of the appellant.

333 To preserve the impartiality of the appeals process, appeals are handled by personnel not involved in the decision appealed.

334 The appeal is handled by the Quality Manager and is registered as a change request for reference.

335 The decision about the outcome of the appeal is made by the Head of the Certification Body.

336 The decision about the outcome of the appeal shall be approved by the Senior Executive.

337 The Quality Manager is responsible for:

- confirming whether the appeal relates to the certification activities;
- documenting the appeal as a change request;
- checking that the appeal has arrived in time and contains all necessary information;
- informing the appellant that the appeal has been received and that it will be treated as an appeal;
- investigating and handling the appeal, and proposing consequent actions (if necessary, the aid of impartial and independent technical experts shall be used);
- determining whether the decision under investigation has been made on false grounds, in conflict with ISO/IEC 17065:2012, CC, CEM, and/or the Quality Management System, or if it contains errors; and

- presenting the appeal, and the investigation, to the Head of the Certification Body who is responsible for the decision about the appeal.

338 The Head of the Certification Body is responsible for:

- making the decision about the appeal; and
- presenting the appeal, the investigation, and the decision about the appeal to the Senior Executive who is responsible for approval of the decision.

339 When the decisions about the appeal are made and approved, the Quality Manager is responsible for:

- ensuring that the appellant is informed about the outcome of the appeal,
- making the appeal and the final conclusion available to the Scheme Advisory Committee,
- ensuring that documentation relevant to the resolution of the appeal and all subsequent actions are placed under document and record control as change requests according to the procedures described in CB-117 *Quality & Change Management* ensuring that all identified nonconformities are reported and handled.

340 Forms for appeals can be found on the CSEC website: http://www.csec.se. The use of these forms is not mandatory.

14 Subcontractor Management

341 Detailed descriptions of the procedures for handling subcontractors can be found in *FMV VHL*.

342 In addition to these instructions, some specific rules and procedures are applicable to the Certification Body.

14.1 Evaluation and Purchasing

343 In addition to the FMV processes for subcontractor evaluation and purchasing, the Head of the Certification Body is responsible for:

- ensuring that all necessary means are available for the activities for which the subcontractor is contracted;
- establishing a strategy, together with the appointed administrator of commercial dealings at FMV, for purchasing including stipulate requirements so that all subcontractors are informed about the applicable requirements of ISO/IEC 17065:2012;
- together with the appointed PL, approving any subcontractor according to their compliance with the related requirements of ISO/IEC 17065:2012;
- ensuring that the subcontracted body or person is competent and is not involved either directly or through the person's employer with the design or production of any product under evaluation in such a way that impartiality would be compromised; and
- ensuring that the subcontracted body or person gives undertakings regarding marketing of their services in line with the requirements on the Certification Body.

344 Since *the Public Procurement Act* (2016:1145) applies to the Certification Body, no list of approved subcontractors is maintained within the Certification Body. In some cases FMV will have general agreements with a number of subcontractors. In these cases all subcontractors with which FMV has signed general agreements will be regarded as approved according to the conditions of the procurement.

345 The Head of the Certification Body is responsible for documenting the criteria for selection of subcontractors involved in testing or inspection.

14.2 Agreement

346 The Head of the Certification Body is responsible for obtaining the applicant's consent in any case where the Certification Body decides to subcontract work related to certification.

347 Together with the appointed administrator of commercial dealings at FMV, the Head of the Certification Body has to establish a contractual agreement on each occasion when a subcontractor performs work for the Certification Body that is related to certification.

14.3 Conflict of interests

348 If a subcontractor will be involved in certification activities, the agreement shall be complemented with the CB-057 *CSEC Impartiality agreement – Form*, as described in section 8.5, *Agreement*.

349 Any situation which may present the subcontractor with a conflict of interests shall be reported to the management of the Certification Body.

14.4 Operations

350 After a subcontractor is contracted, the Head of the Certification Body is responsible for:

- specifying the requirements for any tests or inspections performed by the subcontracted body after input from Chief Operating Officer and Lead Certifier
- taking full responsibility for all subcontracted work and for ensuring that the Certification Body maintain its responsibility for granting, maintaining, extending, suspending, or withdrawing certification; and
- ensuring that the subcontracted body or person is competent and is not involved either directly or through the person's employer with the design or production of any product under evaluation in such a way that impartiality would be compromised.

351 The Quality Manager is responsible for implementing appropriate corrective action in the event that subcontractors operate in breach of the undertakings that they have given.

14.5 Surveillance

352 The Head of the Certification Body is responsible for ensuring that subcontractors never operate in breach of the undertakings that they have given.

353 The Quality Manager is responsible for assessing, monitoring, and recording the performance of any subcontractor performing work for the Certification Body that is related to certification to ensure that any work carried out by a subcontracted body gives the same confidence as work carried out by the Certification Body itself.

15 Security

354 To protect confidential information from unauthorised disclosure, the Certification Body has policies and procedures for information security complemented by procedures for physical security.

355 The procedures for physical security also serve purposes of protection against theft, fire, and personal injury.

356 Security procedures have been established and adopted for use by the Certification Body in the following areas.

- Security organisation
- Personnel regulations
- Logical access control
- Physical access control
- Information classification
- Handling confidential information
- Security planning
- Security analysis
- Incident reporting
- Visitor control
- Mechanical burglary protection
- Alarm protection
- Alarm distribution
- Guard duty

357 The procedures are described in detail in VB-102 *Lokal Säkerhetsskyddsföreskrift* (English: Local Security Regulation).

358 The local procedures are complements to and specialisations of the overall security regulations and procedures of FMV. Those regulations cover a wide range of areas and are based on the requirements of ISO/IEC 27001, where this has been applicable.

Appendix A Classification of Nonconformities

A.1 General Classification

359 Findings from, for example, Internal Audits are classified according to definitions in the table below.

360 It should be noted that a non-conformity, by definition, implies that a requirement isn't met or that a task is not performed as decided.

361 All findings should be stated relative to documented requirements or criteria prescribed by the Quality Management System or by the standards or agreements upon which the Quality Management System is based.

Major	A finding that implies: - a vital function does not exist, or - the total breakdown of a vital function in such a way that a requirement is not fulfilled. *Explanation* This classification is used when a procedure important to fulfil a requirement does not exist in the quality management system and when the requirement subsequently is not fulfilled in the actual work. This classification may also be used when the requirement is addressed in a satisfactory manner in the documentation but where the actual work does not conform to the documentation. For a non-conformity to be classified as major the requirement that is not fulfilled should be relevant to the Certification Body.
Minor	Finding that implies that a function does not completely fulfil a requirement. *Explanation* This classification is used for non-conformities in actual work resulting in a requirement not being fulfilled but where the requirement would be fulfilled if the documented procedures were followed. For such a non-conformity to be classified as minor there should be proof that there are only single occurrences of the non-conformity and that the requirement is normally fulfilled. This classification may also be used when the documented procedure would not fulfil a requirement but where the requirement is fulfilled in the actual work.
Observation	Finding that has no or limited effect on the possibility to fulfil a requirement. *Explanation* This classification is used when the actual work does not conform to what is documented but where it is judged that the requirements are still satisfactorily fulfilled. It may also be used in similar cases when a documented procedure is judged unnecessary to fulfil requirements. Both of these cases would indicate that a change to the Quality Management System would be suitable.

Improvement	Suggestion for improvement of documentation or procedures. *Explanation* This is a classification that may be used for any proposal that is aimed at improving our way of work to make it more effective or efficient. A suggested improvement is not related to a non-conformity.

362 This classification may also be used in the process of licensing, or license surveillance, of Evaluation Facilities.

A.2 Findings in Document Reviews

363 The general classification primarily aims at the implementation of a function or a requirement, rather than defects in single documents. When used in document reviews, the following definitions may be used.

Major	A procedure to resolve a vital requirement allocated to the document is missing.
Minor	A requirement allocated to the document is not completely resolved by the described procedures.
Observation	A finding that is not related to the ability to fulfil requirements.

Appendix B References

364 These references are common to all documents in the Quality Management System

Identity	In Swedish	Title
Certification Body Documents		
CB-012	X	Specialhantering av ansökningar - Nationell säkerhet
CB-017	X	Checklista för årlig licenstillsyn
CB-023		ITSEF Licensing Assessment - Checklist
CB-057		CSEC Impartiality agreement - Form
CB-065		Certificate - Form
CB-078		CSEC Relations with the Swedish Defence Materiel Administration
CB-101	X	Roller - Specifikation
CB-110	X	ITSEF Management
CB-111	X	Certifiering
CB-112	X	Rutiner för tillsyn och underhåll av certifikat
CB-117		Quality & Change Management
CB-124	X	Informationsledning
CB-136		Legal Dependencies
CB-139	X	Ändringsstyrning
CB-149	X	Releasehantering
CB-170	X	Administration och ekonomisk hantering
CB-173	X	Dokumenthantering
CB-189		Certifier Diploma - Form
CB-202	X	Kompetensledning
External publications		
EP-001		Certification and Evaluation - Overview
EP-002		Evaluation and Certification
EP-003		Assurance Continuity
EP-004		Licensing of Evaluation Facilities
EP-007		Quality Manual
EP-008		Charges and Fees
EP-016		License Report - Form
EP-022		Evaluator Status Change Application – Form
EP-024		IT Security Competence – Form
EP-070		Conditions for the Use of Trademarks

Identity	In Swedish	Title
EP-092		Appeal Report – Form
EP-094		Request for Interpretation – Form
EP-103		Terms of Reference for the Scheme Advisory Committee
EP-184		Policy for Certification Queues
EP-188		Scheme Crypto Policy
EP-191		Cross Frontier Evaluation
EP-195		License Application - Form
EP-196		Certification Application with Terms - Form
EP-199		Certification Application with Terms (FMV) - Form
EP-301		Certification and Evaluation - EUCC - Overview
CSEC general documentation		
VB-055	X	Skrivregler
VB-102	X	Lokal säkerhetsskyddsföreskrift
VB-130	X	Säkerhetsskyddsanvisning
VB-132	X	Sekretessregler CSEC
VB-140	X	Verksamhetsbeskrivning
VB-145	X	Granskningsprocedur
VB-146	X	Erinran och kvittens - CSEC sekretessregler
VB-167		CSEC Training Plan - Template
VB-186	X	CSEC Ledning
Agreements		
CCRA		Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, July 2 2014
SOG-IS MRA		Senior Officials Group Information Systems Security - Mutual Recognition Agreement, Jan. 8 2010.
Standards		
ISO/IEC 15408		Information technology — Security techniques — Evaluation criteria for IT security Comment: ISO/IEC-version of the Common Criteria for Information Technology Security Evaluation
ISO/IEC 18045		Information technology — Security techniques — Methodology for IT security evaluation

Identity	In Swedish	Title
		Comment: The ISO/IEC-version of the Common Evaluation Methodology
ISO/IEC 17025		General requirements for the competence of testing and calibration laboratories. The most recent version is ISO/IEC 17025:2018
ISO/IEC 17065		Conformity assessment — Requirements for bodies certifying products, processes and services. The most recent version is ISO/IEC 17065:2012
ISO/IEC 27001		Information technology -- Security techniques -- Information security management systems -- Requirements. The most recent version is ISO/IEC 27001:2013
ISO/IEC 27002		Information technology -- Security techniques -- Code of practice for information security management. The most recent version is ISO/IEC 27002:2013
National administrative regulations		
STAFS 2020:1	X	Styrelsen för ackreditering och teknisk kontrolls föreskrifter och allmänna råd om ackreditering
External Guidelines		
CSC		Conducting Shadow Certifications
VPA		Voluntary Periodic Assessment
Common Criteria		
CC		Common Criteria for Information Technology Security Evaluation
CC Part 1		Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model
CC Part 2		Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements
CC Part 3		Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements
CEM		Common Methodology for Information Technology Security Evaluation
FMV Regulations		
ArbO	X	Arbetsordning Försvarets materielverk Rule of Procedure for the Swedish Defence Materiel

Identity	In Swedish	Title
		Administration
FMV VHL	X	FMV Verksamhetsledningssystem