CSEC

Swedish Certification Body for IT Security

007 Quality Manual

Issue: 45.0, 2019-Sep-25

Authorisation: Mats Engquist, 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 Common Criteria Evaluation and Certification Scheme ("the Scheme"), see Scheme publication SP-001 *Certification and Evaluation Scheme - Scheme 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 Quality Management System.

1.1 Background

4 CSEC is an entity within the Swedish Defence Materiel Administration (FMV) responsible for implementing the Scheme.

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 that should establish and operate a Certification Scheme for security in IT-products and systems. FMV should act to obtain and maintain international recognition for issued certificates.

6 In the *Appropriation Directions for the Swedish Defence Materiel Administration,* the Swedish Department of Defence has stated that FMV shall be Certification Body for security in IT-products and systems and should establish and operate a Certification Scheme for security in IT-products and systems. FMV shall act as national Certification Body within the Common Criteria Recognition Arrangement (CCRA) and should act to obtain and maintain international recognition for issued certificates. FMV should co-operate internationally in order to make the methodology for evaluation and certification more effective and should give support and guidance in using Common Criteria (CC) for requirements specification.

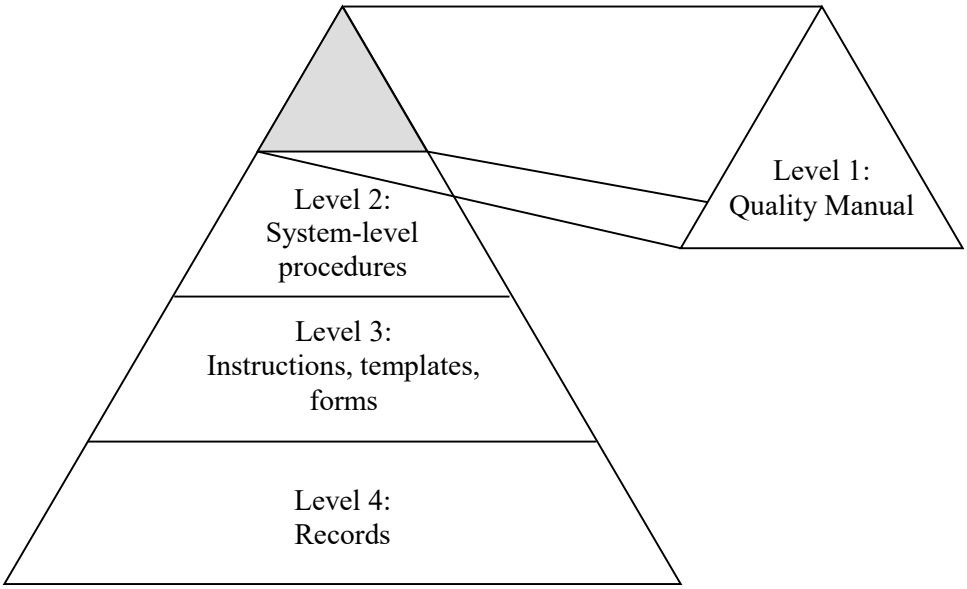
7 The mission of the Certification Body is documented in VB-140 *Verksamhetsbeskrivning* (in Swedish) and in related documents within FMV.

1.2 Documentation

1.2.1 Structure of the Quality Management System

8 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)

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

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

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

System-Level Procedures

12 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.

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

Instructions, Templates, and Forms

14 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

15 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

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

- 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

17 The following documents contain 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 2015:8
  Föreskrifter och allmänna råd om ackreditering
  (English: *Regulations and General Guidelines (STAFS 2015:8) on Accreditation*)
- STAFS 2013:5
  Föreskrifter och allmänna råd om ackreditering av organ som certifierar produkter
  (English: *Regulations and General Guidelines for Accreditation of Bodies that Certify Products*)
- STAFS 2007:21
  Föreskrifter och allmänna råd om organ som certifierar IT-säkerhet
  (English: *Regulations and General Guidelines for Accredited Bodies that Certify IT-security*)

18 In the documents listed below and in some supplementary documentation, there are a number of guidelines on the application of these requirements. Guidelines regarded as especially relevant to the Certification Body are found in the following documents.

- STAFS 2007:20
  Föreskrifter och allmänna råd om evalueringsorganisationer som utvärderar IT-säkerhet
  (English: *Regulations and guidelines for bodies that evaluate IT-security)*

19 These guidelines are not traced within the Quality Management System.

1.2.3 Version Description Documents

20 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 version description document identifies all formal relationships between the documents in the Scheme.

21 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 Scheme is to be published.

1.2.4 Valid Versions of the Scheme

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

23 When the Scheme 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.

24 The version of the Scheme 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 Scheme.

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

1.3 Publications

26 Parts of the Quality Management System and the Scheme, 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 three subcategories:

- Scheme Publications (SP)
- Scheme Policies
- Scheme Notes (SN)

27 It should be noted that the distinction between Scheme Publications, Scheme Policies 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.

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

1.4 Definitions

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

2 Arrangements on Mutual Recognition

30 Certificates issued under the Scheme may be subject for mutual recognition according to the following arrangements:

- 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

31 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.

32 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 Common Criteria Recognition Arrangement (CCRA)

33 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.

34 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.

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

2.2 European Accreditation Multilateral Agreement (EA MLA)

36 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.

37 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 2015:8, 2013:5 and 2007:21.

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

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

39 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.

40 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.

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

2.4 National Certificates

42 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.

43 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.

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

3 Policy

3.1 Objectives for Quality

45 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 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

46 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 scheme.
- 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

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

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

- The Certification Body operates a documented Quality Management System that complies with the CCRA agreement, with the SOGIS mutual recognition agreement, and with 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 our field of operation by strict adherence to Scheme rules, 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 our 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

49 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

50 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.

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

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

53 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.

54 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.

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

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

57 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*.

58 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*.

59 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

60 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

61 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.

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

4.2 No Compromising Activities

63 The main purpose of the Certification Body is to provide certification services according to the Scheme.

64 The Certification Body does not manufacture or trade in any products or systems certified under the Scheme.

65 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

66 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.

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

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

69 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

70 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).

71 Such situations will be analysed during the risk analysis.

4.4.2 Yearly Risk Analysis

72 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*.

73 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*.

74 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

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

76 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

77 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.

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

4.4.5 Reporting to the Scheme Advisory Committee (SAC)

79 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

80 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.

81 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.

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

83 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*.

84 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.

85 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.

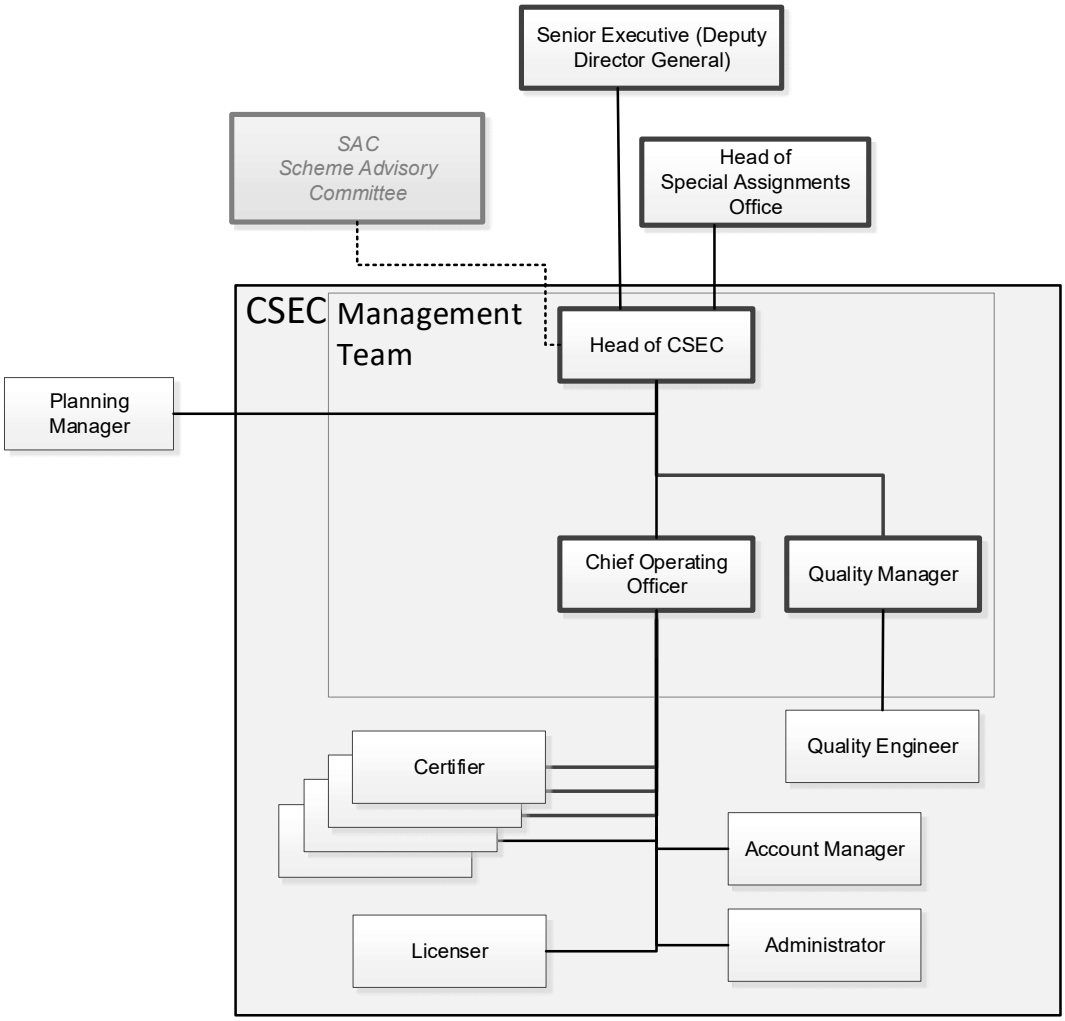
6 Management and Organisation

6.1 Organisation

86 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

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

6.2 Roles

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

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

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

91 Assignment of roles within the Certification Body is made through a Decision to Appoint a person and are made by the Head of CSEC.

6.2.1 Management Roles

92 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

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

94 The Senior Executive reports to FMV's Board.

Head of the Certification Body

95 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.

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

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

Chief Operating Officer

98 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.

99 The Chief Operating Officer has the responsibility and authority to evolve and improve all aspects of the Scheme services and documentation.

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

Quality Manager

101 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.

6.2.2 Other Roles

102 The following roles have responsibilities of vital importance in running the Scheme.

- Certifier
- Licenser
- Quality Engineer
- Administrator
- Account Manager

103 These roles are described in more detail in CB-101 *Roller - Specifikation.*

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

6.3 Boards and Committees

6.3.1 Scheme Advisory Committee (SAC)

105 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.

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

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

6.3.2 Management Team

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

109 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)

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

111 The participants in the Change Control Board are as follows.

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

112 Personnel with other roles may participate, and may be invited, but are not required.

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

6.4 Financing

114 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 Scheme publication SP-008 *Charges and Fees*. The procedures for management of finances are described in VB-140 *Verksamhetsbeskrivning* (in Swedish).

6.5 Liabilities

115 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

116 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*.

117 The procedures for project management are based upon the procedures described in *FMV VHL* (see Appendix C, *FMV VHL*).

6.7 Management Procedures

118 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

119 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.

120 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.

121 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.

122 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

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

124 The Quality Management System and the Scheme consist 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 and the Scheme as follows.

Type	Description	Prefix
CB Documents	Internal documents related to the Evaluation and Certification Scheme	CB
Unit documents	Internal documents not limited to the Scheme but 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	SP[1]

125 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.

[1] These documents are complemented by Scheme Policies and Scheme Notes.

7.1.3 Publications

126 The public part of the documentation is divided into three subcategories as follows.

Scheme Publications	Scheme Publications are the part of the Scheme included in 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. Scheme Publications could contain regulations as well as guidelines for the parties involved in licensing and in evaluation and certification. Scheme Publications are issued on the CSEC standard template.
Scheme Policies	Scheme Policies describe how the Scheme is to be used or applied in different situations and how the Certification Body will act in situations not directly related to the procedures for granting Certification. Scheme Policies 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 a Scheme Policy or a Scheme Publication should be considered.

7.2 Maintenance of the Quality Management System

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

128 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*.

129 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.

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

7.3 Change Control

131 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.

132 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 Scheme 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.

133 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

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

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

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

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

138 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

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

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

141 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

142 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.

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

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

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

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

147 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.

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

149 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

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

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

152 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 Scheme and the Quality Management System.

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

154 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

155 The requirements for certification consist of the standards described in section 11.3, Relevant Standards

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

157 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 Scheme Regulations

158 The Scheme and the Quality Management System mainly consist of procedural regulations but may impose requirements for certification.

159 A change to the Scheme and the Quality Management System that would represent a change to the requirements for certification 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*.

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

161 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

162 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.

163 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.

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

7.9 Information about Changes

165 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*.

166 The policy for information about changes is as follows.

- All changes to the Scheme are published on the official website.
- All changes with major impact on the operation of the Scheme 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

167 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.

168 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*.

169 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.

170 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

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

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

8.1 Personnel Resources Administration

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

174 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.

175 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.

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

177 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

178 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.

179 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.

180 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.

181 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.

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

8.3 Competence Development

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

184 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.

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

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

8.4 Recruitment

187 Recruitment is performed according to the procedures described in *FMV VHL* (see Appendix C, FMV VHL).

188 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

189 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.

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

191 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

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

193 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.

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

8.7 Performance Monitoring

195 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

196 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.

197 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

198 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).

199 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

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

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

202 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

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

204 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

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

8.9.3 Other Permanent Personnel

206 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

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

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

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

210 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.

211 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.

212 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.

213 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

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

215 The details of the FMV procedures are described in *FMV VHL* (see Appendix C, FMV VHL).

8.11 Reporting Conflicts of Interest

216 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.

217 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

218 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).

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

9.2 Confidentiality

220 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* . 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

221 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.

222 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

223 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

224 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

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

226 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.

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

9.3 Superseded Documents

228 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

229 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.

230 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

231 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*.

232 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.

233 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).

234 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).

235 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

236 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 Scheme. The primary channel for spreading information to external parties is the website of the Certification Body.

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

- a new version of the Scheme or 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)

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

239 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.

240 New Certificates and certification reports will be made available on the website of the Certification Body and to CCRA participants through the Swedish CCRA Member.

241 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

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

243 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 ensuring that there is a distribution list for each document that, if relevant, includes the website of the Certification Body.
- The Account Manager supported by the Chief Operating Officer is responsible for providing applicants with information about the appropriate general documentation.
- The Lead Certifier is responsible for providing all applicants with the appropriate project-specific documentation maintained by CSEC.
- The Evaluator is responsible for updating the applicants during the project with changes regarding the general documentation and adding other relevant information during the project.
- The Administrator is responsible for providing notifications to all external requestors on the distribution list for the document whenever the document is changed.
- The Administrator is responsible for the publication of all new versions of public documents on the CSEC website.
- The Scheme 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 8, Personnel 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 8, Personnel Management.

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

10.2 Publishing

245 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	SP-007 Quality Manual
Documented statement of the product certification system, including the rules and procedures for granting, maintaining, extending, suspending, and withdrawing certification	SP-007 Quality Manual SP-002 Evaluation and Certification
Description of the means by which the organisation obtains financial support	SP-007 Quality Manual
General information on the fees charged to applicants and to suppliers of certified products	SP-008 Charges and Fees
Description of the rights and duties of applicants and suppliers of certified products	SP-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	SP-001 Certification and Evaluation Scheme - Scheme Overview
Information about procedures for handling complaints and appeals	SP-007 Quality Manual
Information about withdrawn CC Certificates	
Directory of certified products and their suppliers	
Directory of interpretations	
Directory of explanations	

246 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.

247 The Administrator is responsible for the actual publishing.

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

10.3 Information to Participants

249 The Administrator is responsible for providing the CCRA Participants with copies of documents covering significant aspects of the Scheme.

250 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.

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

252 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	SP-002 Evaluation and Certification
The organisational structure of the Certification Body	SP-007 Quality Manual
The Quality Manual of the Certification Body	SP-007 Quality Manual
The accreditation or licensing/approval policy of the Certification Body	SP-004 Licensing of Evaluation Facilities
The titles and addresses of the ITSEF's associated with the Scheme and their status (e.g., governmental or commercial)	Licensing agreements 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

253 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 legal entity
- 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 Scheme

11.1 Scheme Documentation

254 The general description of the Scheme is documented in the following documents.

SP-001 Certification and Evaluation Scheme - Scheme Overview

255 This document contains a general description of the Scheme. It is the public top document of the Scheme. It is through this document that most external interested parties get information leading them further into the details of the Scheme.

256 The document contains a brief description about the Scheme and describes roles, definitions, and abbreviations important for the understanding of the information.

257 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.

SP-002 Evaluation and Certification

258 This document describes the policy and procedures for evaluations and certifications performed under the Scheme. 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.

SP-003 Assurance Continuity

259 This document describes the scheme for continuous maintenance of certifications.

SP-004 Licensing of Evaluation Facilities

260 This document describes the requirements and procedures for licensing and for the maintenance of licenses of evaluation facilities under the Scheme.

11.2 Scheme Owner

261 CSEC is the owner (Scheme Owner) of the Swedish Common Criteria Evaluation and Certification Scheme.

11.3 Relevant Standards

262 The Certification Body performs certification according to the official versions of the standards below. The details of the Scheme are described in the documents referred to in section 11.1, *Scheme Documentation*.

11.3.1 CCRA

263 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

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

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

11.3.2 ISO/IEC

266 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

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

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

11.4 Certification Management

11.4.1 Information about Certification

269 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).

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

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

11.4.2 Pre-evaluation

272 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.

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

11.4.3 Extending or Reducing the Scope of a Certification

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

11.4.4 Conduct of Evaluation

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

- monitor the evaluation and
- review evaluation reports.

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

11.4.5 Conclusion of Evaluation

277 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.

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

11.4.6 Assurance Continuity

279 During Assurance Continuity, the Certification Body shall:

- maintain certification.

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

11.4.7 Certificate Surveillance

281 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.

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

11.4.8 Withdrawal/Suspension of Certificates

283 The Certification Body shall withdraw certificates when appropriate.

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

11.4.9 Certificate/Marking

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

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

11.5 ITSEF Management

287 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.

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

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

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

11.6 Mutual Recognition and International Liaisons

11.6.1 CCRA

291 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.

292 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.

293 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.

294 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.

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

296 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.

11.6.2 EA MLA

297 Sweden participates through Swedac in the EA.

298 For further information about mutual recognition within EA see section 2.2, *European Accreditation* Multilateral Agreement (EA MLA).

11.7 Interpretations

299 The uniform application of the requirements of the CC and the Common Methodology (CEM) over time, within, and between Schemes, is assured through the use of interpretations. This also applies to any Scheme-specific requirements, within the Scheme in question.

300 Whenever a situation occurs in the context of an evaluation, and where the CC and the CEM does not provide sufficient guidance, the Scheme will have to choose a course of action, possibly based upon subjective judgement. Such choices must be documented as National Interpretations if strictly CC/CEM related, or as Scheme Notes if Scheme related.

301 In the Scheme, a request for clarification of the CC, the CEM, or the Scheme procedures, is called a request for interpretation. The use of Scheme publication SP-094 *Request for Interpretation -Form* is recommended, but not mandatory.

302 Each National Interpretation that may be relevant to other Schemes within CCRA shall be presented to the Common Criteria Maintenance Board (CCIMB), where it may be taken up for international interpretation. Scheme Notes shall be processed in accordance with the procedures for change management.

303 National interpretations relevant to the current version of CC and Scheme Notes relevant to the current version of the Scheme procedures must always be considered in subsequent certifications.

304 A detailed description of the CSEC procedures for handling interpretations is found in CB-122 *Interpretations Management*.

12 Customer Satisfaction

305 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.

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

- Licensing
- Certification
- Spontaneous reactions

307 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.

308 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.*

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

310 Spontaneous customer reactions are registered in the Task Management System by the member of personnel who receives the matter.

311 Complaints are handled according to the procedures for handling complaints, described in section 13, *Complaints and Appeals*.

13 Complaints and Appeals

312 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 rules of the Scheme, and
- the Certification Body has procedures to learn from any complaints or appeals and to update the Scheme accordingly.

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

314 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

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

316 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.*

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

318 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.

319 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.

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

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

322 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.

323 The Head of the Certification Body will:

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

324 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

325 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.

326 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.

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

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

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

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

331 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 the scheme regulations (ISO/IEC 17065:2012, CC, CEM, scheme specific documents), 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.

332 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.

333 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 in the Task Management System, and
- ensuring that all identified nonconformities are reported and handled.

334 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

335 Detailed descriptions of the procedures for handling subcontractors can be found in *FMV VHL* (see Appendix C, *FMV VHL*).

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

14.1 Evaluation and Purchasing

337 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.

338 Since *the Public Procurement Act* (2007:1091) 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.

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

14.2 Agreement

340 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.

341 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 within the Scheme for the Certification Body.

14.3 Conflict of interests

342 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*.

343 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

344 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.

345 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

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

347 The Quality Manager is responsible for assessing, monitoring, and recording the performance of any subcontractor performing work within the Scheme 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

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

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

350 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

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

352 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

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

354 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.

355 All findings should be stated relative to documented requirements or criteria prescribed by the Scheme or by the standards or agreements upon which the Scheme 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.

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

A.2 Findings in Document Reviews

357 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

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

Identity	In Swedish	Title
Certification Body Documents		
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-095		National Interpretation - Form
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-122		Interpretations 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-177		Certificate – Form (Accreditation/EA MLA)
CB-187	X	Hantering av certifieringsköer
CB-189		Certifier Diploma - Form
CB-202	X	Kompetensledning
Scheme Publications		
SP-001		Certification and Evaluation Scheme - Scheme Overview
SP-002		Evaluation and Certification
SP-003		Assurance Continuity
SP-004		Licensing of Evaluation Facilities
SP-007		Quality Manual
SP-008		Charges and Fees

Identity	In Swedish	Title
SP-016	X	Licensrapport - blankett
SP-022		Evaluator Status Change Application – Form
SP-024		IT Security Competence – Form
SP-070		Conditions for the Use of Trademarks
SP-092		Appeal Report – Form
SP-094		Request for Interpretation – Form
SP-103		Terms of Reference for the Scheme Advisory Committee
SP-184		Policy for Certification Queues
SP-188		Scheme Crypto Policy
SP-191		Cross Frontier Evaluation
SP-194	X	Ansökan om licens - Mall
SP-195		License Application - Form
SP-196		Certification Application with Terms - Form
SP-199		Certification Application with Terms (FMV) - Form
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
Standards		
ISO/IEC 15408		Information technology — Security techniques — Evaluation criteria for IT security Comment: ISO/IEC-version of the Common Criteria for Infor-

Identity	In Swedish	Title
		mation Technology Security Evaluation
ISO/IEC 18045		Information technology — Security techniques — Methodology for IT security evaluation 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 2015:8	X	Styrelsens för ackreditering och teknisk kontroll (Swedac) föreskrifter och allmänna råd om ackreditering
STAFS 2013:5	X	Styrelsens för ackreditering och teknisk kontroll (Swedac) föreskrifter och allmänna råd om ackreditering av organ som certifierar produkter
STAFS 2007:20	X	Styrelsens för ackreditering och teknisk kontroll (Swedac) föreskrifter och allmänna råd om evalueringsorganisationer som utvärderar IT-säkerhet
STAFS 2007:21	X	Styrelsens för ackreditering och teknisk kontroll (Swedac) föreskrifter och allmänna råd om organ som certifierar IT-säkerhet
External Guidelines		
CSC		Conducting Shadow Certifications
VPA		Voluntary Periodic Assessment
Common Criteria		
CC		Common Criteria for Information Technology Security Evaluation

Identity	In Swedish	Title
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	
VO	X	Verksamhetsordning FÖR FÖRSVARETS MATERIELVERK Activity regulation for the Swedish Defence Materiel Administration
FMV VHL	X	FMV Verksamhetsledningssystem

Appendix C FMV VHL

359 The Quality Management System at FMV is constituted by Processes and, Activities, Handbooks and Service Provisions.

360 The following parts of the from *FMV VHL* are used as reference in the Quality Management System:

361 Procedures for project management:

- Planera och genomföra projekt

362 Procedures for competence development:

- Genomföra kompetensförsörjning

363 Procedures for individual career development discussion:

- Medarbetarsamtal

364 Procedures for recruitment:

- Genomföra rekrytering

365 Procedures for staffing:

- Bemanning

366 Procedures for handling subcontractors:

- Upphandling

367 Procedures for procurement of consultants:

- Köpa uppdragskonsult eller bemanna med inhyrd personal

368 The Quality Management System at FMV is written in Swedish.