الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

QCCS CB Quality and Management System Manual

[CB-4-MAN-QMSM]

Manual

Qatar Common Criteria Scheme Certification Body

28.03.2022

v2.0

Public

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Document Authorization

This page detail may intentionally be removed or hidden when publicly published or shared

DOCUMENT TITLE:	QCCS CB Quality and Management System Manual
DOCUMENT REFERENCE:	[CB-4-MAN-QMSM]
ISSUE:	v2.0
DATE:	28.03.2022

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

DISCLAIMER / LEGAL RIGHTS

National Cyber Security Agency (NCSA) has designed and created this publication, titled "QCCS CB Quality and Management System Manual" - v2.0 - Public, in order to demonstrate operations with sound quality assurance and information security management systems.

QCCS CB is responsible for the review and maintenance of this document.

Any reproduction of the present document either in part or full and irrespective of the means of reproduction; shall acknowledge QCCS CB and NCSA as the source and owner of the "QCCS CB Quality and Management System Manual".

Any reproduction concerning this document with intent of commercialization shall seek a written authorization from the QCCS CB and NCSA. QCCS CB and NCSA shall reserve the right to assess the functionality and applicability of all such reproductions developed for commercial intent.

The authorization from QCCS CB and NCSA shall not be construed as an endorsement of the developed reproduction and the developer shall in no way publicize or misinterpret this in any form of media or personal / social discussions.

LEGAL MANDATE(S)

Article 18 of the Emiri Decree no (4) for the Year 2016 setting the mandate of Ministry of Transport and Communications (was referred as "MOTC") provided that MOTC had the authority to regulate and develop the sector of Information and Communications Technology in the State of Qatar in a manner consistent with the requirements of national development goals, with the objectives to create an environment suitable for fair competition, support the development and stimulate investment in these sectors; to secure and raise efficiency of information and technological infrastructure; to implement and supervise e-government programs; and to promote community awareness of the importance of ICT to improve individual's life and community and build knowledge-based society and digital economy.

Based on Cabinet decision (26) for the year 2018, the Compliance & Data Protection Department (was referred as CDP) was entrusted by the Ministry of Transport and Communications (MOTC) as the competent authority, responsible for determining, in the public interest, the technical competence and integrity of organizations such as those offering assessments, testing and compliance services and the Issuance of Certifications those seeking certificates of compliance within the State of Qatar. In 2021, the National Cyber Security Agency (NCSA) has taken over the role as the competent authority and assumed the responsibility from MOTC since.

This Manual has been prepared to take into consideration the current applicable laws of the State of Qatar. If a conflict arises between this document and the laws of Qatar, the latter shall take precedence. Any such term shall, to that extent be omitted from this Document, and the rest of the document shall stand without affecting the remaining provisions. Amendments, in that case, shall then be required to ensure compliance with the relevant applicable laws of the State of Qatar.

REFERENCES

- All references are listed in [CB-2-LST-DocRefList] Documentation Control Reference List

Table of Contents

1 Introduction

Qatar government has recognized the need for excellence in the certification services it provides through Qatar Common Criteria Scheme Certification Body within National Cyber Security Agency, Qatar.

In order to achieve high levels of quality, security and reliable management system that are required by customers of QCCS, the QCCS CB has developed this Quality and Management System Manual in order to demonstrate operations with sound quality assurance and information security management systems.

QCCS CB commitment to quality, security and compliance is made in the belief that the adopted standards and requirement is sensible, both commercially and practically, and will ensure that the organization's integrity and reputation is enhanced through its provided services.

This document defines the high-level organizational basis for the operation of the Qatar Common Criteria Scheme (QCCS) under the Certification Body (hereafter referred as 'CB'), for IT Security within the National Cyber Security Agency (hereafter referred to 'NCSA').

CB may also be referred as QCCS CB (Qatar Common Criteria Scheme Certification Body).

1.1 Purpose

The document is written with the aim to provide customers at all times with a service that in line to comply various international standards and requirements.

The referenced standards and requirements are primarily the following:

- CCRA: Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology [CCRA] – Obligatory requirement.
- ISO/IEC 17065: Conformity Assessment – Requirements for bodies certifying products, processes and services [17065] – Non-obligatory requirement but as a guidance.

Note: This CB is not accredited under ISO/IEC 17065 at the moment.

This manual defines the plans, high level procedures and standards to be implemented by the QCCS CB, to ensure the certification processes meet the respective requirements as per the references of this document.

2 Scope

The processes specified in this Quality and Management System Manual are applicable to QCCS CB operations within the NCSA facilities. The services provided by QCCS CB comprise the following:

a) Qatar Common Criteria Scheme scope of certification services are as stated in Section 4.1 of the Scheme Certification Procedure [CB-4-PCD-QCCS]. This includes:
   i. the security evaluation and certification of ICT products, systems, protection profiles;
   ii. the assurance maintenance for security certified ICT products and systems; and
   iii. site certification

To support the delivery of the above certification services, QCCS CB delivers the following additional supporting services:

a) Engagement with CCRA member countries and participation in the development and maintenance of the CCRA, ISO/IEC 15408, ISO/IEC 18045 on behalf of the Qatar Government;
b) Provision of support to third party assessors for the purpose of assessing compliance of:
   i. the Common Criteria Scheme with CCRA requirements (Voluntary periodic assessment),
   ii. accreditation of Evaluation Bodies (EBs) to against ISO/IEC 17025;
c) Provision of Training and Development for Certifiers, and interested customers;
d) Management of Scheme publications including the QCCS Certified Products Register that lists scheme certified products;
e) Recognition (licensing) and management of Evaluation Bodies (EB's); and
f) Interpretation or Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. An interpretation may be either a national or international interpretation.

QCCS certification confirms that an IT product fulfills relevant IT standards or other normative documents, security principles, laws or regulations depending on the applied scheme.

The current Quality and Management System Manual is valid for IT product certification services offered by QCCS CB. It describes the quality and management system of the QCCS CB. It is structured based on the requirements of the CCRA and ISO/IEC 17065 standard as a reference guidance.

The Quality and Management System Manual is intended

- for internal use in planning, controlling and monitoring quality assurance activities enacted by the CB
- as a description for external use proving that the CB fulfills the requirements of relevant standards

This Quality and Management System Manual is the basic work manual for all employees of the CB within QCCS operation. All detailed procedures necessary for daily operation are provided in additional referenced documents. The document list [CB-2-LST-DocRefList] contains all related documents.

The CB operates the following IT product certification scheme:

- Common Criteria Scheme Certification [CB-4-PCD-QCCS]. – Where the primary scope of this document is covering

Additionally, the CB operates the national ISMS regulations as a scheme:

- National Information Assurance (NIA) (Note: This would theoretically require compliance of the CB with ISO 17021 as this standard is for bodies, which audit and certify management systems. But (1) NIA is not an international standard, and (2) it is probably better to have some kind of internal regulation for the NIA certification body.)

Note: This NIA scheme is not covered in the scope of this document

3 Organizational Structure

The Certification Body (CB) was formed in 2015 (according to the [CB-3-LTR-CBEstablish] QCCS CB Establishment Letter) and operated under the surveillance of MOTC under the mandate from the ministry approval itself when it was known as IctQATAR. The previously known MOTC was formally identified as IctQATAR and then changed its name to MoICT. The forming of QCCS under the Certification Body was based on the approval letter of the ministry dated 22nd January 2015, Reference Letter No: MICT/CSD/CIIP/001-2015. (See [CB-3-LTR-CBEstablish]).

Ministry of Transport and Communications (MOTC) was the owner of the Qatar Common Criteria Scheme. In 2021, the National Cyber Security Agency (NCSA) has taken over the role as the competent authority and responsibility from MOTC since. The Scheme Director has authority for the strategic management and oversight of the QCCS CB.

The scheme provides a model for recognition or licensing (government and commercial) Evaluation Bodies (EBs) to conduct security evaluations of ICT products, systems and

protection profiles against internationally recognized standards; Common Criteria (ISO/IEC 15408) and Common Evaluation Methodology (ISO/IEC 18045).

The QCCS CB is organized in four functional areas:

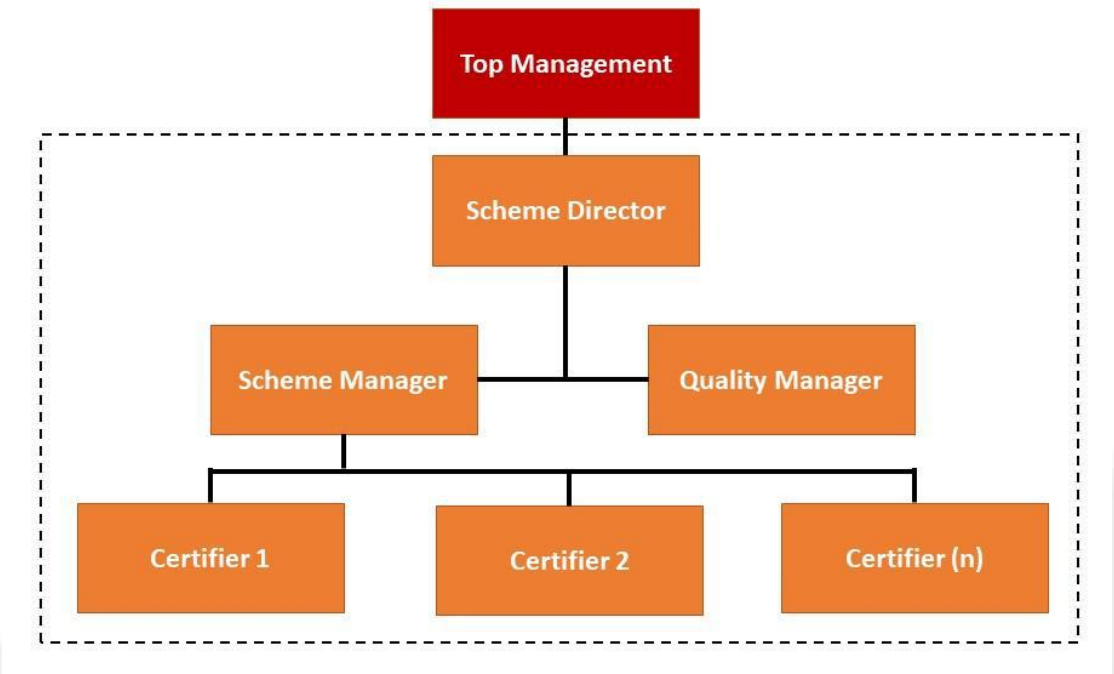
- Scheme Director, responsible for the whole operation of the CB,
- Quality Manager, responsible for quality assurance of the certification and quality management process,
- Scheme Manager, responsible for administration and human resources,
- Certifier, responsible for individual certification projects.

The above roles are detailed in Scheme Certification Procedure [CB-4-PCD-QCCS]. Jobs description for each role are defined in [CB-3-JobDesc].

In addition to these functions, the CB has a Top Management from the organization that ensures the impartiality of the CB.

QCCS CB scheme organization structure is depicted in Figure 1 below.

Figure 1 QCCS CB Scheme Organization



The organizational structure of the QCCS within the CB is described in CB organizational structure [CB-4-QCCSOrgChart]

4 Operation

The following chapters onwards describe how this manual are structured based on the clauses mentioned in ISO/IEC 17065. The chapter numbering in this Quality and Management System Manual reflects the numbering of the ISO/IEC 17065 chapters starting from chapter 4 (written as 4.4 “General requirements”) until chapter 8.8 (written as 4.8.8 “Preventive actions (Option A)”). Since chapter 1 to 3 of ISO/IEC 17065 have no relevance for this Manual, these are omitted from chapter numbering in the current document and replaced by Introduction, Scope and Organizational Structure. Chapter 7.1 until 7.11 are specified in Scheme Certification Procedure [CB-4-PCD-QCCS].

4.4 General requirements

4.4.1 Legal and contractual matters

ISO/IEC 17065 clause 4.1, CCRA Annex C C.3d, C.9b

4.4.1.1 Legal responsibility

The CB was established in ictQatar and MOTC as laid down in [CB-3-LTR-CBEstablish] approval letter of the ministry dated 22nd January 2015, Reference Letter No: MICT/CSD/CIIP/001-2015. In 2021, the National Cyber Security Agency (NCSA) has taken over the role as the competent authority and assumed responsibility from MOTC since.

4.4.1.2 Certification Agreement

The Sponsor and Evaluation Body shall work together to submit the Certification Application Form [CB-4-FRM-CertAppl] with completed documentation as mentioned in [CB-4-PCD-QCCS], section 4.2.2 Application Phase. The Certification Application Form has an additional area where Generals Terms and Conditions for certifications the sponsor (and Evaluation Body) must agree before signing, as a Certification Agreement.

Note: Sponsors should take care in ensuring that other contractual arrangements are appropriate to their needs as the CB will not involve itself in contractual dispute matters between Evaluation Body and Sponsor (or its clients).

In circumstances where the sponsor cannot resolve technical evaluation issues with an Evaluation Body, the CB may be contacted for assistance with resolving the issues. The most appropriate mechanism for this resolution is through a project progress meeting called between the stakeholders of the project.

However, any stakeholders may at any time lodge a complaint or appeal to the CB.

4.4.1.3 Use of Marks, License, and Certificates

Sponsor, Developer, Evaluation Body, or any non-CB party may not use the marks or logo (such as CCRA logo and mark, CB logo or NCSA logo) in anyway other than those described in this section unless explicitly authorized by the QCCS CB or NCSA.

The CB will relatively monitor and research the use of the marks and logo in public domain such as search engines and official marketing platforms. If it is found to be misusing either of the marks or logo, the CB will take one or more of the following actions:

a. Notify the infringing party of the issue as a warning; and/or

b. Withdraw the certificate(s) that is associated with the infringement.

c. Worst case is to take legal action

Further description such as the usage of marks and logo in marketing and notification responsibility is detailed in [CB-4-PCD-QCCS], section 4.8.1.

4.4.2 Management of Impartiality

ISO/IEC 17065 clause 4.2

The CB has defined details on the Management of Impartiality and Mechanism for safeguarding impartiality in Impartiality Management Procedure [CB-3-PCD-ImpartialMgmt].

The CB and any part of the same legal entity and entities under its organizational

control (for example; government lab under NCSA and NCSA itself) shall not:

a) be the designer, manufacturer, installer, distributer or maintainer of the certified product;

b) be the designer, implementer, operator or maintainer of the certified process;

c) be the designer, implementer, provider or maintainer of the certified service;

d) offer or provide consultancy (see 3.2) to its clients;

e) offer or provide management system consultancy or internal auditing to its clients where the certification scheme requires the evaluation of the client's management system.

Any CB personnel must declare themselves and exclude themselves from work (specified above) in which they have already been involved for at least the last two years.

4.4.3 Liability and Financing

ISO/IEC 17065 clause 4.3

The CB has adequate arrangements to cover liabilities arising from its operations and/or activities. The Certification Body has financial stability and resources required for the operation of the certification system, in the form of budgetary support from the organization it is under, and the government.

The QCCS CB also publishes its price list for certification services to recover costs for the delivery of QCCS scheme.

Note: Under certain circumstances, when the certification project involves National interests, the cost of certification service will be subsidized or waived by the respective ministry that is going to use the product.

4.4.4 Non-discriminatory conditions

ISO/IEC 17065 clause 4.4, CCRA Annex C C.1

The QCCS CB offers its services to any customer without restriction, obstruction or discrimination. All the procedures adopted by the CB are administered in a non-discriminatory manner. The Certification Body makes its services accessible to all applicants, without any undue financial or other conditions.

The CB provides unhindered access without any pre-condition to all the applicants seeking certification of their IT Product/ protection profiles, whose activities fall within its declared field of operation, without undue financial or other conditions.

The QCCS CB advertises its services in Qatar and in the international community interested in the applied schemes.

The product complexity and the certification scheme chosen are the only input figures for the calculation of effort and time required for a certification. The certification fees are not dependent on the size of the company, the number of certificates already issued for that customer or any memberships whatsoever.

The QCCS CB decides about the certification based on product requirements as specified in the respective certification scheme. The QCCS CB publishes annotations or interpretations it applies in its certification decisions in addition to the applicable certification scheme.

All product requirements, the evaluations conducted, and decisions taken by the QCCS CB refer only to the context agreed with the customer in the certification application and the corresponding scheme document.

4.4.5 Confidentiality

ISO/IEC 17065 clause 4.5, CCRA Annex C C.10

QCCS CB is required to access privileged and sensitive information in order to assess conformity to requirements for certification adequacy. As a business unit under NCSA, QCCS CB operates in accordance with the security requirements specified by the NCSA. The security requirements defined in the following sections are specific to QCCS CB and are in addition to NCSA processes. Where the requirements below differ from NCSA processes, the stronger security measure may apply.

QCCS CB shall implement security mechanisms and processes in accordance with the requirements of the scheme operated by QCCS CB, primarily CCRA requirements, guided by ISO/IEC 17065:2012, and associated corporate policies and procedures.

The Scheme Manager is responsible for the security of QCCS CB and the confidentiality of customer information.

Personnel

All QCCS CB staff involved in any certification project (certifiers) signs a Project Declaration Form [CB-3-FRM-ProjDecForm] before starting the project to ensure impartiality and confidentiality for delivering their task within the project.

Upon hired either permanently or contracted by the QCCS CB, all the staff will sign a one-time Employee Declaration Form [CB-3-FRM-EmpDeclare] to ensure impartiality and confidentiality for delivering their task within the scheme. Internal personnel within NCSA who being appointed to involved with QCCS CB day-to-day operation are also required to sign the above Employee Declaration Form.

Information

There are several types of information that QCCS CB personnel deal with. These types of information may need to be handled differently and therefore are categorized below for ease of reference in the following sections.

QCCS CB information can be broadly categorized into the following types:

a) **Management Information.** This is information that is related to the organization management processes such as personnel records, budget information and planning materials. This information is handled in accordance with organization requirements such as NCSA corporate Information Security policy (as applicable).
b) **Certification Task Information**. This is information that is specific to a certification task such as customer details, evaluation results and certification records. This information shall be handled in accordance with the requirements of this document.
c) **Reference Material**. This is publicly available information such as standards and guidance documents. This information has no specific handling requirements.

All QCCS CB information is subject to the protective marking policies of the respective law and regulations.

Access to Certification Task Information shall be restricted to personnel with a need to access the information (i.e. certifiers or any individual not assigned to a particular evaluation should not have access to that Certification Task Information).

Certification Task Information shall be handled in accordance with the Documentation and Record Control Procedure [CB-3-PCD-DocRecCtrl].

Facility

Access to QCCS CB office facility shall be restricted to authorized personnel only. The QCCS CB Scheme Manager shall have sole responsibility for approving access to QCCS CB facilities.

Visitors (all non-CB personnel) to CB facility:

a) shall be escorted at all times;
b) shall be logged into a visitor register at reception; and
c) may be issued with a tag that identifies them as a visitor.

Service or maintenance staff such as cleaners and electricians may be allowed unescorted access when all protectively marked and task-specific material has been secured. However, their purpose of activities and access to which areas shall be known.

Logical

QCCS CB shall employ logical security mechanisms to ensure the confidentiality, integrity and availability of Certification Task Information during storage, processing and transmission.

Client Information

The QCCS CB keeps confidential any information about a certification project that is marked as confidential by any party. Only information declared by the customer to be public may be treated differently.

The QCCS CB will only disclose information about a certification project to project participants to the extent that the information is required to fulfill the respective task within the project. The QCCS CB will only disclose information collected during a certification project when the customer agrees (see section 8 Certification Application Form [CB-4-FRM-CertAppl]. The QCCS CB also keeps confidential any information about the customer, even if it is received from other sources than the customer (e.g. from regulators, from complaints).

Regulations or laws may require disclosure of information collected during a certification project. In such cases, the QCCS CB will disclose the information and the customer will be informed about this fact.

Also, another body responsible for the international recognition of the QCCS CB may require disclosure of information from certification projects, e.g. CCRA recognition. In such cases, disclosing of information to these bodies requires that they sign confidentiality agreement (example; Auditor NDA) and agree explicitly to the limited disclosure.

Scheme Manager is responsible to ensure enforcement of the confidentiality requirements and to ensure the secure handling of confidential information (e.g. documents, records) is supported through the provisioning of adequate and appropriate equipment and facilities.

4.4.6 Publicly available information

ISO/IEC 17065 clause 4.6, CCRA Annex C C.11

The QCCS CB provides general information about its operation to customers and interested parties in its website. This includes but is not limited to the delivery of the following information upon request:

- Document of the official CB establishment by NCSA
- Quality and Management System Manual (this document)
- Scheme Certification Procedure (see [CB-4-PCD-QCCS])
- Certification application form (See [CB-4-FRM-CertAppl])
- List of certified products
- Fees

Only documents that are authorized and identified as public in [CB-2-LST-DocRefList] can be published. Otherwise, they remained as internal and confidential.

The certification scheme requirements are listed in the respective scheme documents (see [CB-4-PCD-QCCS]). If any party shall require more information, the QCCS CB will provide information about where to find that information and how to interpret it. The QCCS CB also publishes its price list for certification services to recover costs for the delivery of QCCS scheme.

The Certification Application Form must be signed before the certification project starts. Additional information about the scheme or requirements will be provided by the QCCS CB upon request.

The certification application shall describe the context for which the certification is valid. All product requirements, the evaluations conducted, and decisions taken by the QCCS CB will refer only to the context agreed with the customer in the certification application.

The requirements, restrictions, or limitations on the use of the CB's certification mark, logo or license are in section 4.4.1.3. Information about Termination, reduction, suspension or withdrawal of certification can be found in Scheme Certification Procedure [CB-4-PCD-QCCS].

Any stakeholders may at any time lodge a complaint or appeal to the CB following the process in this document or Scheme Certification Procedure [CB-4-PCD-QCCS].

4.5 Structural requirements

4.5.1 Organizational structure and top management

ISO/IEC 17065 clause 5.1, CCRA Annex C C.3a, C.9e

The certification activities of the QCCS CB are structured and managed to safeguard impartiality.

The QCCS CB is an independent organizational unit within NCSA. Its position within NCSA is described in NCSA Organization Chart [CB-4-NCSAOrgChart]

The QCCS CB is organized in four functional areas:

- Scheme Director, responsible for the whole operation of the CB,
- Quality Manager, responsible for quality assurance of the certification and quality management process,
- Scheme Manager responsible for administration and human resources,
- Certifier responsible for individual certification projects.

The organizational structure and detailed roles of the QCCS CB is described in

- QCCS CB Organization Chart [CB-4-QCCSOrgChart]
- QCCS CB Jobs Description [CB-3-JobDesc]

Each personnel assigned for each role was appointed officially and has signed a declaration form to ensure confidentiality, impartiality, and no conflict of interest.

The Scheme Director as part of Top Management identifies the persons or organizational units having overall authority and responsibility. These may include but are not limited to:

- development of policies relating to the operation of the certification body;
- supervision of the implementation of the policies and procedures;
- supervision of the finances of the certification body;
- development of certification activities;
- development of certification requirements;
- evaluation;
- review;
- decisions on certification;
- delegation of authority to committees or personnel, as required, to undertake defined activities on its behalf;

- contractual arrangements;
- provision of adequate resources for certification activities;
- responsiveness to complaints and appeals;
- personnel competence requirements;
- management system of the certification body.

Note: Some the above responsibility may be delegated by Scheme Director to Scheme Manager or next subordinates when necessary.

4.5.2 Mechanism for safeguarding impartiality

ISO/IEC 17065 clause 5.2

The mechanism for safeguarding impartiality is described in section 4.4.2 and 3.0 where the management of the impartiality is covered in non-discriminatory conditions and the Organizational Structure.

Further details on the Mechanism for safeguarding impartiality is defined in Impartiality Management Procedure [CB-3-PCD-ImpartialMgmt].

4.6 Resource requirements

4.6.1 Certification body personnel

ISO/IEC 17065 clause 6.1, CCRA Annex C C.4, C.9c, d

4.6.1.1 General

QCCS CB personnel shall be employed by NCSA. If any outsourcing service is involved, a proper contractual agreement taking care of confidentiality, impartiality and non-conflict of interest shall be applied.

The Scheme Manager shall ensure that current responsibilities for all scheme roles are maintained (see [CB-4-QCCSOrgChart] QCCS CB Organization Chart).

The Scheme Manager, with advice from the most senior certifier, shall ensure the competence of all personnel to deliver certification services.

QCCS CB shall employ, and/or have access to, a sufficient number of certifiers and technical experts to cover all of its activities and to handle the volume of audit work performed.

The QCCS CB management makes sure that the QCCS CB has sufficient personnel to fulfill its tasks and the certification projects. The Scheme Manager responsible for human resources takes care of the planning and supportive tasks required to supply sufficient personnel.

The QCCS CB only employs competent personnel. Each member of the QCCS CB is trained according to the Training and Competency Procedure [CB-3-PCD-Training] and other training may be added from time to time to improve knowledge and skills.

This procedure covers general aspects applicable for all members of the staff and detailed training requirements for the technical certification staff.

In order to ensure that the certifications are comparable and are conducted with competence, the technical staff is supported by scheme specific flowcharts and workflows. (See [CB-4-PCD-QCCS] Scheme Certification Procedure).

Any personnel working for the QCCS CB on the basis of a contract or permanent, shall sign a confidentiality declaration either in general form in their work contracts or as a project-based agreement. (See the Employee Declaration Form [CB-3-FRM-EmpDeclare] and Project Declaration Form [CB-3-FRM-ProjDecForm]).

Any personnel related information compiled by the QCCS CB shall be kept confidential. Generally, only the Top Management, Scheme Director and the Scheme Manager responsible for human resources are allowed to access the information. The privilege to access the information may be delegated to Quality Manager or anyone within QCCS CB by Scheme Manager if necessary.

4.6.1.2 Management of competence for personnel involved in the certification process

The Scheme Manager responsible for human resources analyses the competence requirements of the QCCS CB on a yearly basis. The analysis may cover the following aspects but not limited to:

- required competence(s) in the QCCS CB based on the roles assigned,
- number of staffs in the QCCS CB having the respective competence,
- assessment, if the number of staffs having the respective competence is sufficient,
- forecast number of staffs required in the next year,
- plan how to build up the required competences,
- identify needs for training, new hires or outsourcing contracts.

The above analysis will be done by the help of Employee Training and Competency Matrix [CB-3-LST-TrainingMatrix]

Based on the analysis, the Scheme Director takes action recommended by the Scheme Manager.

The QCCS CB maintains formal authorizations for the technical tasks it carries out during certification projects. Personnel may only carry out a particular task when it is formally authorized to do so. The QCCS CB documents the required competences for the roles in the QCCS CB.

The QCCS CB monitors the performance of its personnel on yearly basis or more if no changes.

The Scheme Manager maintains records about the personnel of the CB. For every employee, the following information may be recorded:

- name (and address if applicable);
- employer(s) and position held;
- educational qualification and professional status;
- experience and training;
- the assessment of competence;
- performance monitoring;
- authorizations held within the certification body;
- date of most recent updating of each record.

4.6.1.3 Contract with the personnel

All personnel of the QCCS CB that is involved in certification projects shall sign a project declaration form [CB-3-FRM-ProjDecForm] in which they commit themselves at least to the following:

- Comply with the rules of the QCCS CB, the confidentiality and the impartiality requirements,
- Declare any prior or present association with suppliers, designers or producers of products to the evaluation or certification they will be assigned to,
- Reveal any circumstances that may put them or the QCCS CB in an interest conflict.

Information received from employees regarding threats to their impartiality will be fed into the management processes maintaining the impartiality of the QCCS CB (see chapters 4.4.2 and 4.5.2). In the context of these processes, further action may be triggered.

4.6.1.4 Subcontracting of CB work

The QCCS CB may subcontract certification work associated with defined certification projects to competent subcontractors.

The subcontractors have to prove their competence as follows:

- Every member of the subcontractor's staff to be involved in the certification project has to fulfill the current competence requirements for the particular certification project as identified in the analysis according to chapter 4.6.1.2
- Every member of the subcontractor's staff to be involved in the certification project has to sign a declaration according to chapter 4.6.1.3.

4.6.2 Resources for evaluation

ISO/IEC 17065 clause 6.2, CCRA Annex C C.4, C.9f, h,

4.6.2.1 Internal resources

The CB itself does not carry out evaluations.

4.6.2.2 External resources (outsourcing)

The QCCS CB recognizes (also known as licensing) EBs for delegating evaluations to them.

The QCCS CB makes sure that only EBs passing the recognition procedure (also known as licensing) of the respective certification scheme will be recognized and can provide evaluation services in agreement with the QCCS CB.

(See Evaluation Body Recognition Procedure [CB-4-PCD-EBRecog])

The recognition procedures for the certification schemes make sure that the EBs fulfill

- the requirements of international standards including ISO/IEC 17025
- any technical, organizational and personnel requirements required by the particular certification scheme,
- the confidentiality and impartiality requirements of the CB,
- the security requirements for EBs (see Evaluation Body Recognition Procedure section 4.0 [CB-4-PCD-EBRecog]).

The QCCS CB does not recognize non-independent EBs (e.g. manufacturer labs) for evaluations. If evaluation activities shall be performed by a non-independent entity, e.g. a manufacturer lab, the responsible EB needs the explicit permission of the QCCS CB. In such cases, the recognized EB has to provide a justification (e.g. lack of lab capacity, EB has special equipment, etc.) and must completely control the activity to make sure that the requirements of the QCCS CB and the certification scheme are fulfilled.

Upon recognizing an EB, the QCCS CB enters a contractual relationship with the EB to make sure that the QCCS CB has sufficient control over the evaluation process. This may be achieved by having a specific term duration of agreement between the QCCS CB and the Evaluation Body Evaluation Body Recognition Agreement [CB-2-AGR-EBRecog]. During the term of agreement is valid, the EB has responsibility to deliver the evaluation service when assigned to a specific project or client, otherwise the project will not commence.

The QCCS CB maintains a list of the recognized EBs, see QCCS CB Master Register [CB-2-LST-CBMaster].

The QCCS CB may accept certification applications, if the customer has contracted a recognized EB in the process of recognition. It is advisable that the customer only contacts the EB for technical assistance or on their own separate arrangements. However, the QCCS CB has definitive rights to assign which EB will evaluate the product in the end.

If the QCCS CB subcontracts any certification or evaluation related tasks, e.g. to a recognized EB, this is only done on the basis of a contract agreement.

When the QCCS CB becomes aware, that a recognized EB does not fulfill the contract or other requirements from the certification scheme, the Certifier and the Scheme Director assess the result of the deviation, decide on corrective action and on information of the customer.

Note: The CB will not involve itself in contractual dispute matters between Evaluation Body and Sponsor (or its clients) or whatsoever arrangement unknown to CB. For example; the EB outsourced the evaluation to other EB without notifying the CB.

4.7 Process requirements

The certification body operates the following certification schemes:

- Common Criteria Certification [CB-4-PCD-QCCS] – operated by this QCCS CB
- National Information Assurance Scheme (Note: Not covered in this Quality Management System Manual)

The following process are structured based on ISO/IEC 17065 which are covered in the scheme certification procedure document (see [CB-4-PCD-QCCS]). The chapters refer to the subchapters of ISO/IEC 17065. The chapters aims to cover requirement of CCRA, not ISO/IEC 17065 accreditation. **Note: This CB is not accredited under ISO/IEC 17065 at the moment.**

7.1 General

7.2 Application

7.3 Application review

7.4 Evaluation

7.5 Review

7.6 Certification decision

7.7 Certification documentation

7.8 Directory of certified products

7.9 Surveillance

7.10 Changes affecting certification

7.11 Termination, reduction, suspension or withdrawal of certification

Note: In order for the chapter numbering to reflect the clause numbering in ISO/IEC 17065 the following chapters 4.7.1 to 4.7.11 were omitted in this document (yet they are covered in Scheme Certification Procedure). Find them in [CB-4-PCD-QCCS].

4.7.12 Records

See chapter 4.8.4 Control of documents (Option A)

4.7.13 Complaints and appeals

ISO/IEC 17065 clause 7.13, CCRA Annex C C.9i, C.12

Any employee of the QCCS CB may receive complaints or appeals about his work or the work from the sponsor or any other stakeholder of the CB (including clients which are non-CB). Complaints or appeals need to be communicated to the CB in writing, either as a paper letter, a fax or as an email.

The employee receiving a complaint or appeal sends the message to the above channels and they are usually attended by the Quality Manager and Scheme Manager will be in loop. The Quality Manager takes care for the orderly treatment of the complaint or appeal. The complaint or appeal will be entered into an issue list, see QCCS CB Issue list [CB-3-LST-IssueList]

The Quality Manager confirms to the complainant in writing (preferably in electronic form such as email) that the QCCS CB has received the complaint or appeal. The complainant should receive the confirmation within two working days after the complaint or appeal was received by the QCCS CB.

The Quality Manager sends the complaint or appeal to the Scheme Director. The Scheme Director coordinates the treatment of the complaint or appeal:

- When the complaint or appeal addresses a certification project, the Scheme Director may consult the responsible Certifier or another employee who is familiar with the project in question. (see section 4.10 in Scheme Certification Procedure [CB-4-PCD-QCCS])

- When the complaint or appeal addresses general quality or procedural issues, the Scheme Director may consult the Quality Manager.
- When impartiality or confidentiality issues are addressed, the Scheme Director consults the Top Management.

The Scheme Director decides about how the QCCS CB deals with the complaint or appeal:

- When the complaint or appeal is due to a different understanding of matters between QCCS CB, EB or sponsor, the Scheme Director invites the parties to discuss the issue before starting further action.
- When the complaint or appeal is rooted in a failure of the QCCS CB, the Scheme Director may decide on corrective action to immediately solve the complaint or appeal, and/or on preventive action to prevent it from recurring.
- When the complaint or appeal is rooted in a failure of the EB, the Scheme Director may decide to instruct the EBs to change their procedures to solve the complaint or appeal and/or prevent it from recurring.

The Scheme Director decides whether or not the QCCS CB shall send a formal answer to the complainant about the treatment of the complaint. When the complainant filed an appeal, he will always receive a formal answer from the CB about how his appeal was or will be solved.

During the processing, the Quality Manager documents discussions and decisions about of the complaint or appeal. In particular, corrective or preventive action may be triggered to solve the complaint or appeal. For details on corrective or preventive action, see chapter 4.8.7 and 4.8.8 in this document.

The Certifier or any other employee involved in a particular project may not be consulted when he or she delivered consulting services to the stakeholder filing the complaint or appeal during the last two years. Instead, another employee having the technical competence to discuss and decide about a complaint or appeal shall take place. In the case where the Quality Manager is the person who are being complained, the complaint shall be attended by the Scheme Manager. The Scheme Director may delegate the coordination of complaint and appeal process to Scheme Manager or any other authorized impartial person if necessary.

4.8 Management system requirements

4.8.1 Options

ISO/IEC 17065 clause 8.1

The CB maintains a management system according to option A of ISO/IEC 17065 clause 8.1.2

4.8.2 General management system documentation (Option A)

ISO/IEC 17065 clause 8.2, CCRA Annex C C.9a

The current Quality and Management System Manual is the management system documentation for the fulfillment based on ISO/IEC 17065 clause 4 (general requirements), 5 (structural requirements), 6 (resource requirements) and 8 (management system requirements).

The certification scheme includes the management system documentation of ISO/IEC 17065 clause 7 (process requirements).

The aforementioned documents reference all documentation required to cover ISO/IEC 17065.

The Top Management describes the QCCS CB's commitment to fulfillment of the Quality Management System (this document) and the certification scheme in the certification policy statement. (See Quality and Management System Policy [CB-2-POL-QMSP].)

The Quality Manager is responsible and has the authority to report to the Top Management and the Scheme Director about the performance of the management system and any need for improvement. This assessment is done at least on a yearly basis in internal audits.

Based on the information from the performance assessment, the Top Management and the Scheme Director decide about changes to the management system. The Scheme Director initiates the changes to the management system and monitor their implementation.

The Quality Management System Manual (this document) and the Scheme Certification Procedure (see [CB-4-PCD-QCCS]) are available to all staff of the CB in electronic form.

4.8.3 Control of documents (Option A)

ISO/IEC 17065 clause 8.3, CCRA Annex C C.5

The Scheme Manager assisted by Quality Manager, responsible for document service maintains the list of all documents required to fulfill this Quality Management System Manual (see [CB-2-LST-DocRefList]). All documents in this list are covered by document control. Quality Manager serves as the document controller that maintain quality documents register that records the current revision status of each quality related document.

Prior to use, all controlled documents have to be approved by the Scheme Director. Controlled documents are Policies, Manuals, Procedures and Guidelines.

Documents generated as live document from the approved templates does not require any approvals, however they may be recorded and tracked (see [CB-2-LST-DocRefTrack] Document Tracking).

Approvals may only be given after the document in question was reviewed by the manager (Quality and Scheme Manager) and any problems or errors found in the document were

corrected. Reviews may have to check documents for legibility, correctness, completeness, topicality, compliance with standards and correct identification.

All controlled documents carry a version number and the approval date. Changes to a controlled document version over the previous version have to be recorded in the document or otherwise made available.

The document with the latest approval date is the valid version for use in QCCS CB work. All other versions may only be used when a reasonable justification is given (e.g. use of an older version is required by the certification scheme).

External documents can also be kept under document control for use in the QCCS CB. Such documents have to be identified and recorded as coming from an external source (e.g. from the maintainer of a particular certification scheme).

All controlled documents are usually stored within the premises of the QCCS CB, which may include secured cloud storage used by the department. All employees of the QCCS CB must have at least read access to the documents that are relevant to their assigned tasks. The Scheme Director, Certifiers and the Scheme Manager involved in document control must have writing access in order to fulfill their tasks.

Security provisions for the QCCS CBs are generally following the NCSA Policy. The Security Guidelines [CB-3-GUI-SecGuide] and Security Architecture [CB-3-GUI-SecArc] are covering physical and logical security for the QCCS CB.

The documentation structure and management are described in more detail in

- Documentation and Record Control Procedure [CB-3-PCD-DocRecCtrl]

Certification schemes may use a different structure for their procedural documents. The details are described in the respective scheme operation documents.

4.8.4 Control of records (Option A)

ISO/IEC 17065 clause 8.4, CCRA Annex C C.6

Electronic documents are stored on the server of the QCCS CB, which will be both in local and secured cloud storage used by the department. Only QCCS CB personnel involved in the respective certification project has access to the records.

The QCCS CB may produce or receive paper records. Paper records may be scanned to image files. The files are kept and controlled in the same way as original electronic documents. The paper records can be either destroyed once scanned or be kept securely in individual project files in printed form. Records are protected from unauthorized access by applying an access control system to set appropriate access rights for the respective documents. Physical records shall be physically secured.

Confidentiality requirements for the records are covered in the declaration forms signed by the personnel as a part of its work contract.

If the QCCS CB is communicating with sensitive electronic information such as critical customer data that requires secrecy, the CB personnel shall encrypt its communication (by encrypting the email or the file itself).

The standard retention time for all records is five (5) years. Retention times may be differently specified for management system records, certification scheme records or individual certification projects. During the retention time, records can be retrieved from the internal document management by the authorized QCCS CB staff. In most cases, digital records more than 5 years may be kept in archived for future reference or in case there will be a need for re-evaluation of product. Where required by contractual or legal obligation, this will override the default retention time.

The Scheme Manager responsible for document service keeps a list of the retention times. They may randomly check on a yearly basis if the retention time for records is over. After this time, the records are either listed for destruction or stored in a long-term archive.

- When the Scheme Director approves for destruction, the Scheme Manager destroys the records. However, the Scheme Manager may retain a minimal data set so that the QCCS CB retains the information that a particular project or activity existed.
- When records get stored in a long-term archive, the Scheme Manager moves the data to the QCCS CB archive and takes care that no more changes can be made to it.

There are two kinds of records pertaining to the fulfillment of this International Standard:

- Records required to maintain the management system
- Records required by the certification scheme in use

The record structure, storage location and identification are described in more detail in [CB-3-PCD-DocRecCtrl] Documentation and Record Control Procedure and [CB-2-LST-DocRefList] Documentation Control Reference List.

Request for access to non-public documents such as Internal, Confidential and Restricted levels shall be made in writing and require NCSA Top Management approvals.

ISO/IEC 17065 clause 7.12 Records

Records required by the certification scheme in use, the structure and identification of these records are described in more detail in the respective certification scheme. These may include but are not limited to:

- Proposals, orders, order confirmations, invoices
- Project plans
- Electronic mails and scanned paper-based communication
- Sponsor documents

- Scanned paper documents
- Result documents (e.g. evaluation reports, reports review protocols, certification decision protocols, certificates and certificate drafts)

All documents pertaining to an individual certification project carry the certification ID according to the certification scheme document. Every individual certification project is stored under its unique certification ID.

4.8.5 Management review (Option A)

ISO/IEC 17065 clause 8.5, CCRA Annex C C.13

4.8.5.1 General

The QCCS CB reviews its management system at least on a yearly basis according to the Management Review procedure described in [CB-3-PCD-MgmtReview] to ensure its continuing suitability, adequacy and effectiveness.

4.8.6 Internal audits (Option A)

ISO/IEC 17065 clause 8.6

The QCCS CB conducts internal audits to verify that the management system is effectively implemented and maintained.

The audits are planned by the Quality Manager according to the Internal Audit Procedure [CB-3-PCD-IntAudit]

The Quality Manager plans audit so that every aspect of the management system will be audited at least once a year. However, based on the stability or effectiveness of particular aspects of the management system, audits may be held more or less often. The audit planning as well as reasons for changing the frequency of audits for particular aspects of the management system is documented.

The Quality Manager functions as the auditor for most aspects of the management system. The Scheme Manager audits the Quality Manager's work. However, any staff of the QCCS CB having the appropriate training can conduct internal audits provided that they do not audit their own work. The Quality Manager may also appoint or hire external auditor (or any auditor from other functional units within NCSA that not involved with QCCS CB operation). This may also include personnel from Internal Audit Department, if needed.

When the audit is completed, the auditor documents its results. The personnel responsible for the management system or the certification scheme will be informed about the result. They will take action to make sure that deviations are dealt with in a timely and appropriate way and that all opportunities for improvement are identified.

4.8.7 Corrective actions (Option A)

ISO/IEC 17065 clause 8.7

Nonconformities may arise from management reviews, internal audits, customer complaints or other sources. Based on an analysis of the nonconformity, corrective actions can be determined. Corrective actions are documented and tracked for timely implementation.

The Quality Manager and the Scheme Manager are responsible for analyzing nonconformities and stating corrective actions. The staff of the QCCS CB implements corrective actions. Afterwards, the Quality Manager and the Scheme Manager may assess the effectiveness of corrective actions in correcting the nonconformity.

Corrective actions shall be taken in accordance with the Corrective and Preventive Action Procedure [CB-3-PCD-CorPrevAct].

4.8.8 Preventive actions (Option A)

ISO/IEC 17065 clause 8.8

The QCCS CB manages preventive actions in the same way as corrective actions, see chapter 4.8.7. Preventive action shall be handled in accordance with the Corrective and Preventive Action Procedure [CB-3-PCD-CorPrevAct].

5 Terms and Definitions

5.1 Terms

The current document mainly uses terms as defined in ISO/IEC 17065 and the CCRA

5.2 Abbreviations

QCCS Qatar Common Criteria Scheme

CC Common Criteria

CB Certification body

EB Evaluation Body

AB Accreditation Body

QM Quality Manager

CCRA Common Criteria Recognition Arrangement

MOTC Ministry of Transport and Communications

NCSA National Cyber Security Agency

6 History

Version	Date	Comments	Author
0.4	2015-10-02	First Draft	TÜViT
0.8	2019-10-15	Update	TÜViT
0.9	2019-10-20	Update	TÜViT
0.91	2019/10/28	Name reference changes	MOTC
0.92	2020/03/24	Updated review	MOTC
0.93	08/05/20	Comments /review	CB/MOTC
1.0	2020/08/27	Final – update new template	MOTC

Version	Date	Comments	Author
2.0	2022/03/28	Major update: -changed logo, removed qcert logo, changed organization details	NCSA

End of Document