الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

QCCS CB Evaluation Body Recognition Procedure

[CB-4-PCD-EBRecog]

Procedure

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 Evaluation Body Recognition Procedure
DOCUMENT REFERENCE:	CB-4-PCD-EBRecog
ISSUE:	v2.0
DATE:	28.03.2022

DISCLAIMER / LEGAL RIGHTS

National Cyber Security Agency (NCSA) has designed and created this publication, titled "QCCS CB Evaluation Body Recognition Procedure" - v2.0 - Public, to define the steps of recognition for both Internal and External IT Security Evaluation Laboratory.

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 Evaluation Body Recognition Procedure".

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 Procedure 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 8
2 Scope 8
3 Recognition of evaluation bodies (EBs) 8
3.1 Preface 8
3.2 Precondition 9
3.3 Recognition process 10
3.3.1 Preparation phase 10
3.3.2 Assessment phase 12
3.3.3 Recognition phase 14
3.4 Scheme Meetings 16
3.5 Cooperation of CB and EB 16
4 Security Requirements 16
4.1 Goals 16
4.2 Asset Classification and Scope Requirements 17
4.3 Security Measures and Controls 17
4.3.1 Physical Facility Requirements 18
4.3.2 Personnel Requirements 19
5 Management Requirements 19
5.1 Contract Agreement with QCCS CB 19
5.2 Fees 19
5.3 EB Obligation 19
6 Terms and Abbreviations 20
6.1 Terms 20
6.2 Abbreviations 20
7 History 20

1 Introduction

This Evaluation Body Recognition Procedure defines the steps for recognition for both Internal and External IT Security Evaluation Laboratory, (hereafter referred to “Evaluation Body” or “**EB**”) under Qatar Common Criteria Scheme (hereafter referred to “**QCCS**”) for the Certification Body (CB) in National Cyber Security Agency (NCSA). This recognition enables the EB to perform the Common Criteria (CC) evaluations under QCCS.

2 Scope

This document is mandatory for all EBs that shall be recognized by the QCCS CB of NCSA. Furthermore, it shall be applied if the QCCS CB or EB sub-contract tasks to external evaluation body (hereafter also referred to “**EEB**”) that include the appropriate handling of confidential data regarding an evaluation or certification activity. Other subcontracted tasks shall not be affected, e.g. consulting support that is not directly related to actual evaluation or certification projects.

3 Recognition of evaluation bodies (EBs)

3.1 Preface

The Qatar Common Criteria Scheme (QCCS) is responsible for Qatar National Certification Body for IT security. In this function, the QCCS CB certifies IT products according to their IT security when positively evaluated by a recognized EB or EEB according to one of the evaluation schemes the CB supports. Such scheme is Common Criteria Certification Scheme based on international standards ISO/IEC 15408 and recognized as a scheme under a Certification Body by Common Criteria Recognition Arrangement.

When a product manufacturer seeks certification for his product, they can consult the website of the QCCS CB for any recognized EBs. They may then make contract with any of the recognized EBs to perform the evaluation and to contact the QCCS CB for supervision of the evaluation process.

EBs conducting IT security evaluations need a formal recognition before they can submit their evaluations to the QCCS CB for certification. The recognition is granted as the result of a recognition process described in this document. In the course of the recognition process, the evaluation body has to fulfill a number of requirements listed in the current document.

Any potentially to be recognized EB or EEB that has been accredited under ISO/IEC 17025 and been recognized by other scheme under CCRA, will most probably be easily accepted, however all the processes required by QCCS is only to verify if they really have it.

Note: All activities within this recognition process, the QCCS CB will record this information in EB Recognition Checklist [CB-3-LST-EBRecog].

*Note: The items numbered as **Req.x.x** will be the guidance for auditor auditing requirements. They will be available in this document.*

3.2 Precondition

An EB that seeks to be recognized by the QCCS under the CB shall fulfill all following requirements:

1. **Req.1.1** The EB shall be an **accredited testing laboratory according to latest ISO/IEC 17025** with the scope of ICT product and security evaluation and testing. The accreditation scope shall match the tasks that are required for the intended certification scheme (Common Criteria, ISO/IEC 15408); and
2. **Req.1.2** The EB shall be **licensed or accredited CC laboratory** by one of the National CB of CCRA authorizing members, an accreditation licensing certificate shall be provided; (National Lab of QCCS, namely National Technology Vetting Lab (NTVL) is exempted from this requirement **Req.1.2**)
3. **Req.1.3** The documented information of the EB has professional experience with **at least five (5) CC evaluation projects** (statement of the projects, project scope and work carried out); (National Lab of QCCS, NTVL is exempted from this requirement **Req.1.3**)

The EB with the following experiences, qualification or accreditation (according to the latest requirements), will be given priority to consideration (not mandatory but recommended):

1. Successful projects in Protection Profile (PP) develop, evaluation and certification in emerging technology, i.e. automotive, IoT…etc.
2. Information Security Management Systems (ISO/IEC 27001) Certification;
3. National Voluntary Laboratory Accreditation Program (NVLAP) accredited FIPS-140-2 Cryptographic Module Testing Laboratory (CMT);
4. Successful project in National CC scheme and evaluation facilities establishment, capacity building and awarded the CCRA recognized as a certificate consuming member and certificate authorizing member.

3.3 Recognition process

3.3.1 Preparation phase

The lab which has the intention to become recognized EB within Qatar Common Criteria Scheme shall contact the QCCS CB to arrange for application. The QCCS CB offers a preparation meeting to interested EBs to introduce the QCCS and the EB recognition process. In the meeting, the parties may discuss the setup of the (planned) EB, organizational, personnel and technical issues.

The EB shall meet the precondition (section 3.2) above before providing any of the following documents.

The EB seeking for recognition shall provide the following documents:

1. **Req.2.1** Documentation of a quality management system of the EB according to the latest ISO/IEC 17025, includes but not limited to
   a. The latest ISO/IEC 17025 accreditation certificate with the competence scope;
   b. Description of the EB, impartiality and confidentiality;
   c. Description of EB structure, personnel with competence;
   d. Records of latest internal audits (such as latest date conducted and how many findings. Details of internal audit is not required);
   e. Records of latest management reviews (such as latest date conducted. Details of management reviews is not required);

   Note: The scope of quality management system shall cover the location of IT security evaluation work of the EB. The document describing how the EB fulfils the ISO/IEC 17025 has to list the measures the EB took to fulfil the aspects of the standard. The document has to provide detailed references into the quality management system manual.

2. **Req.2.2** Documentation of an information security management system to demonstrate the EB fulfill the requirement according to Security Requirements (see section 4.0 of this document)
   Note: The document describing how the EB fulfils Security Requirements (at section 4.0 of this document) has to list the measures the EB took to fulfil the aspects. The document also has to provide detailed references into the relevant information security management system manual.

3. **Req.2.3** The EB shall nominate have at least two evaluators who have relevant professional background in IT security evaluation.
Note: The professional background mentioned can be fulfilled by either through formal education/ exam taken or IT security experience. Skills or knowledge listed in professional profiles or Curriculum Vitae (CV's) have to be proven with certificates,

diplomas or other official documents. Alternatively, skills or knowledge mentioned in the CVs may be checked by the auditors during the assessment phase.

After receiving the full document set from the EB, the QCCS CB conducts an initial assessment of the documentation provided by the EB:

- The CB checks the company status for potential threats to impartiality
  - By checking the impartiality statement in fulfilling the ISO/IEC 17025 requirement
- The CB checks the management system documentations for comprehensiveness and plausibility.
- Special attention will be given to the qualifications of the evaluators listed by the EB. Evaluators shall have the following skills and knowledge:
  - Professional knowledge of ICT and ICT security
  - Common Criteria (CC) evaluation training
  - Working experience in CC evaluations

In case of nonconformities with the requirements, the EB will receive notice from the QCCS CB and is allowed to perform the corrective actions. (e.g. take appropriate measures, change an internal procedure, provide an updated document) before the recognition procedure continues.

When the EB – after the corrective actions – finally fails the initial appraisal, the QCCS CB will terminate the recognition process and reject the application.

When the EB passes the initial appraisal, the QCCS CB decides about the audit team to conduct the **on-site** assessments. The QCCS CB may contract external auditors to conduct audits.

Note: In case of unexpected circumstances where travelling is not possible, remote audit can be done at early stage and approved with condition, and then continued when travelling is allowed again. (this includes Assessment Phase and Recognition Phase as well)

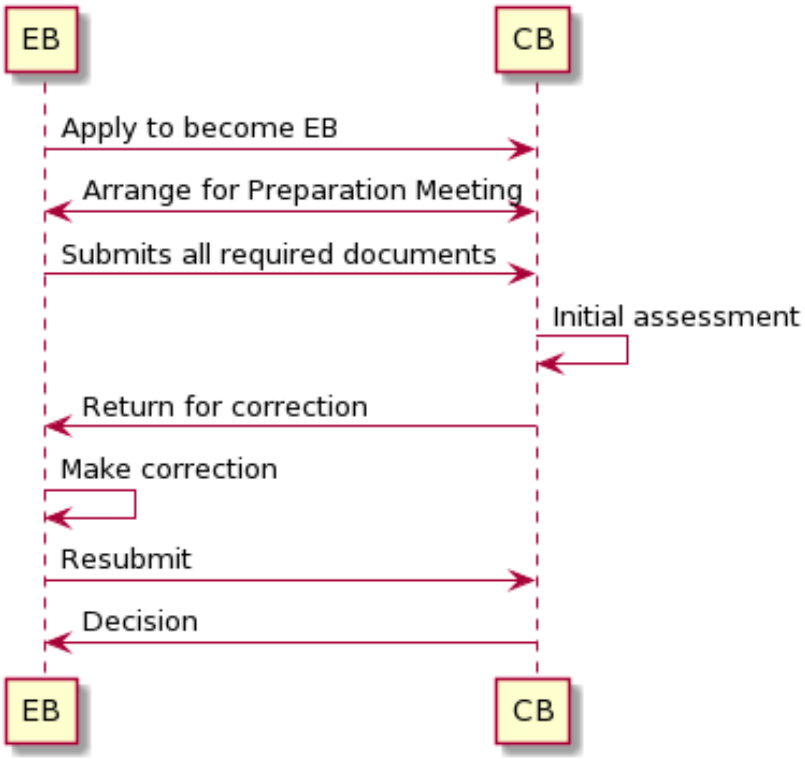

Figure 1: Preparation Phase

3.3.2 Assessment phase

In the assessment phase, the QCCS CB conducts an **on-site** assessment in order to ensure the EB has sufficient provisions and know-how to become recognized by the QCCS CB. Off-site assessment is not acceptable because full observation of the premise environment must be done.

Note (Important): In case of travel ban is imposed where on-site audit is not possible, other methods of verification can be done such as **remote audit** through online interviews, presentations, review of verified evidence such as pictures, plans, videos and other verified documentations.

On-site assessment is meant to confirm the requirement to the Security Requirement (see section 4.0 of this document).

The following assessments have to be passed:

- Quality management system according to ISO/IEC 17025

- Information security managements system according to Security Requirements (see section 4.0 of this document)
- Provisions made by the EB to fulfil the Scheme Certification Procedure [CB-4-PCD-QCCS]

The auditors set up an audit plan for the upcoming audit procedure. The audit plan contains place, dates and scope of the planned audits as well as the names of the planned auditors.

The EB may refuse a certain auditor because of impartiality reasons (e.g. the auditor is a competitor of the EB, the auditor used to work for the EB or a customer of the EB, etc.). When this is the case, the EB has to state the reason in writing to the QCCS CB. The QCCS CB may suggest a different auditor to overcome the problem.

The EB has to make sure that the relevant employees, technical installations or other evidence are available during the audit. Therefore, the auditors send the audit plan to the EB timely before the audit. Audits are usually scheduled for two working days to cover all subjects in the relevant standards.

Audits are conducted at the premises of the EB. During the audits, the auditors may

- inspect evaluation project records,
- inspect technical installations (e.g. test equipment, IT security provisions),
- interview evaluators and employees,
- conduct sample evaluations, or
- collect other evidence

to settle that the EB is working according to the relevant standards, that the personal has sufficient expertise and that all required measures are in place.

After the audit, the auditors give a short summary of the inspections done and the results achieved. When deviations from the standards were found, these will be discussed with the EB. Also, corrective or preventive measures will be agreed between the auditors and the EB.

The auditors provide an audit report as result of their work. The report will cover the inspections and the findings of the audit as well as any corrective or preventive measures agreed. The report may include a recognition recommendation from the QCCS CB. However, the assessment of the recognition does not end yet.

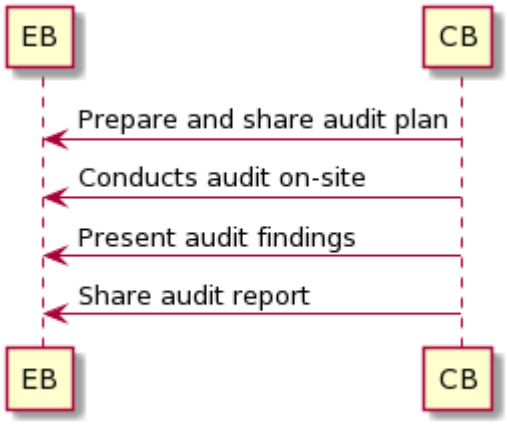

Figure 2: Assessment Phase

3.3.3 Recognition phase

Based on the audit report and corrective action (as appropriate), the QCCS CB decides about the recognition of the EB.

When the QCCS CB decides positively about the recognition, the EB receives a recognition letter with the decision and a recognition agreement for signature (QCCS CB will use EB Recognition Agreement [CB-2-AGR-EBRecog]). Each EB will be assigned with a unique EB Identifier number for example 'L01' for the first recognized EB and 'L02' for the next and onwards.

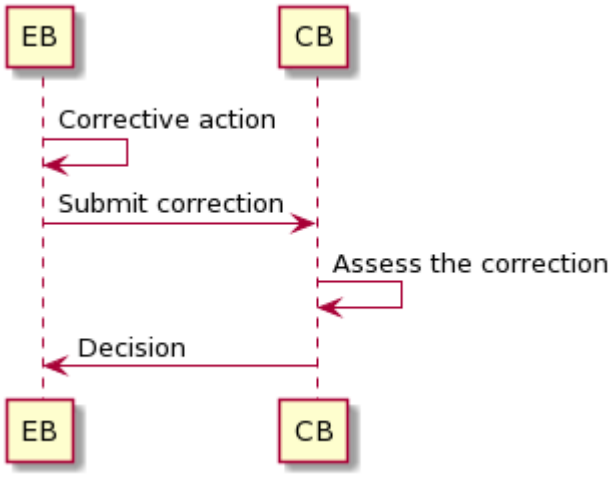

Figure 3: Recognition Phase

The QCCS CB may impose additional requirements on a recognized EB. When this is the case, the EB has the right to comment on the requirements and to decide how to implement these. In case the EB is not able to implement the requirements, the EB may refuse the recognition by the QCCS CB.

When the QCCS CB decides negatively about the recognition of an EB, it has to explain to the EB in writing why the recognition process failed. The EB has the right to comment on the reasons for the decision or to implement additional measures to fix the problem that led to the negative recognition decision.

A recognition is valid for **three (3) years** after the date of the recognition decision. During this period, the QCCS CB oversees the EB's activity from its participation in individual evaluation projects as described in Scheme Certification Procedure [CB-4-PCD-QCCS]. The EB personnel and EB information will be recorded in the QCCS CB Master Register [CB-2-LST-CBMaster].

Note: To assist the QCCS CB in monitoring the EB personnel competency and training, the QCCS CB may use *internal* Training and Competency Procedure [CB-3-PCD-Training] as well as QCCS CB Master Register [CB-2-LST-CBMaster].

When incidents cast doubt about the quality of evaluations conducted by the EB, the QCCS CB may

- invite the EB for consultations with the QCCS CB,
- require organizational or technical provisions or additional training of the EB staff to overcome quality problems,
- schedule additional audits according to the procedure described in chapter 3.3.3
- revoke or limit the recognition,

When the recognition validity period is over, the EB has the responsibility to apply for a renewal of the recognition. In order to receive the renewal of the recognition without interruption, the EB should apply for the renewal **six (6) months** before the recognition expired. Failure to renew within six (6) months before period and the validity expired, the QCCS CB will assume the EB is not interested to continue being recognized and shall be removed from the EB list. The EB has to apply again after the expiry period is over.

Based on the positive results of the EB witnessed by the QCCS CB during the validity period of the recognition, the CB may grant the renewal without or few further assessments. When the EB did not perform any evaluations for the QCCS CB during the validity period, the EB has to undergo a re-assessment of its ability as described in chapter 3.3.1 and 3.3.2 upon renewing its recognition.

3.4 Scheme Meetings

The QCCS CB periodically invites EBs to scheme meetings of the recognized EBs. The meetings cover the following subjects:

- Scheme requirements and interpretations update;
- Communication of changes to the scheme;
- Discussion of quality issues in current evaluations;
- Information exchange about attack and analysis methods

Every recognized EB has to send at least one nominated evaluator to participate in the meetings.

3.5 Cooperation of CB and EB

In order to ensure standardization of information exchange process between QCCS CB and EB, a defined method of communication, management and security process shall be agreed between them.

4 Security Requirements

4.1 Goals

Each EB that performs IT security evaluations in the scope of a certification scheme managed by the QCCS CB must protect confidential information. This is derived from confidentiality requirements from different sources, e.g. ISO/IEC 17025 or Common Criteria Recognition Arrangement (CCRA) requirement, which have to be fulfilled by EBs and CBs, respectively.

Conformance to the latest requirements of ISO/IEC 17025 and ISO/IEC 27001 or accredited by this standard is most preferred where it has already demonstrated the fulfilment of international standard security requirement. Adopting any other standards or security management system may be accepted provided they have proven sound implementation.

*Note: All items marked as **Req.x.x** below will be the guidance for auditor auditing requirements. They will be reviewed both during application review and assessment phase.*

4.2 Asset Classification and Scope Requirements

Req.3.1 The EB shall describe how it protects the confidentiality of its assets.

The EB may take the following information security objectives and controls from ISO/IEC 27001 or, adopting any other standards or security management system, and Annex A of CCRA requirements into consideration:

- Asset management

The asset classification and the organizational scope shall cover the primary data that must be protected from disclosure. This includes all confidential customer data that is suitable to enable attacks on the provided Target of Evaluation (hereafter referred to "**TOE**"), e.g. confidential source code, design information and specific security related site information.

Secondary data regarding the access control may be covered by the operational controls but are not part of the mandatory classification stipulated by this document.

4.3 Security Measures and Controls

Req.3.2 The EB shall describe how it implements Security Measures and Controls.

The EB may take the information security objectives and controls from ISO/IEC 27001 or, adopting any other standards or security management system, and Annex A of CCRA requirements into consideration, as appropriate.

The EB may also consider the controls of Qatar's National Information Assurance Policy (hereafter referred to "**NIA**") in their information security management systems (hereafter referred to "**ISMS**"). The EB shall ensure sufficient NIA compliance to an extent that ensures that the preconditions described above are covered. Due to this, the EB is not required to establish controls that do not cover this focus. A wider ISMS (ISO/IEC 27001) scope may be necessary to fulfil other standards, but they are not part of the mandatory scope required by this document.

During an audit, the EB shall be able to provide reasoning, why and how the different controls have been applied and why others have been omitted.

4.3.1 Physical Facility Requirements

Req.3.2.1 The physical facility requirement compliance will be verified during the recognition and assessment process by the QCCS CB as below:

4.3.1.1 Location and Space

Req.3.2.1.1 The EB shall describe the location and space of the EB.

The EB may take the physical and environmental security objectives and controls from ISO/IEC 27001 or, adopting any other standards or security management system, and Annex A of CCRA requirements into consideration.

The EB shall have a permanent physical facility address where it can be contacted (by a telephone number or other video and/or audio conference software), and sufficient equipment space available for the technical evaluation to be performed. An oversight of a testing on-site must provide an area for the CB staff to perform the audit of the technical evaluation by the EB.

4.3.1.2 IT Infrastructure

Req.3.2.1.2 The EB shall describe its IT Infrastructure. The EB may take the following information security objectives and controls from ISO/IEC 27001 or, adopting any other standards or security management system, andAnnex A of CCRA requirements into consideration:

- Access control;
- Cryptographic;
- Operations security;
- Communications security;
- System acquisition, development and maintenance;
- Supplier relationship;
- Information security incident management;
- Information security aspects of business continuity management;
- Compliance;

The EB shall be able to provide a sufficient ICT infrastructure to support:

- word processing, for the production of reports in Microsoft Word;
- generation of documents in PDF format (if required);
- secure e-mail communication with the CB;
- internet access; and
- specialized tools as may be required for CC evaluation work.

4.3.2 Personnel Requirements

Req.3.3.2 The EB shall describe its personnel requirements.

The EB may take the following information security objectives and controls from ISO/IEC 27001 or, adopting any other standards or security management system, and Annex A of CCRA requirements into consideration:

- Human resource security

The Company shall maintain sufficient staff members: at least one of the staff's members shall meet the eligibility requirements for designation as a Lead Evaluator and have performed the role of CC evaluator, and another one as normal evaluator

5 Management Requirements

5.1 Contract Agreement with QCCS CB

In the end, each facility must sign and adhere to the contract agreement (as stated in EB Recognition Agreement [CB-2-AGR-EBRecog]) when the EB is formally ready to be recognized as the licensed EB in the QCCS CB. Only after this formal agreement been made, then the license certificate of recognition can be awarded to the EB.

5.2 Fees

In the case where a licensed fee and renewal fee is imposed, this fee will be informed in prior either publicly through QCCS CB website page or in the contract agreement itself.

5.3 EB Obligation

During the validity of the license, the recognized EB is responsible to provide its services to the sponsor (of product) who they have been assigned to by the QCCS CB. However, the recognized EB may voluntarily choose to refuse the assignment and provide valid reasons.

With this responsibility in place, in any project contract agreement between the QCCS CB and the sponsor (where the EB is assigned to), the EB shall provide its details of service such as work breakdown detail, timelines, and details of cost if applicable. This EB service details will be attached with the contract agreement.

6 Terms and Abbreviations

6.1 Terms

The current procedure uses terms as defined in ISO/IEC 17065 and CC.

6.2 Abbreviations

CB	Certification body
CC	Common Criteria for Information Technology Security Evaluation (http://www.commoncriteriaportal.org)
EB	Evaluation body
Annex A	Annex A at Arrangement of the Recognition of Common Criteria Certificate in the Field of IT Security
ISMS	Information Security Management System
NIA	National Information Assurance Policy

7 History

Version	Date	Comments	Author
0.1	2015/10/25	First Draft	TÜViT
0.2	2019/10/20	2nd Draft	TÜViT
0.3	2019/10/29	Name and reference changes	MoTC
0.4	2019/11/26	3rd amendment	MoTC
0.5	2020/03/24	Updated review	MoTC
0.6	5/8/20	Comments/review	CB/MOTC
1.0	2020/08/27	Final – update new document template	MoTC
1.1	2020/10/07	Minor amendment	MoTC
2.0	2022/03/28	Major changes: -changed logo, remove qcert logo	NCSA

Version	Date	Comments	Author
		- changed organization name	

End of Document