Harmonized and Unified Cybersecurity Certification System

A Guidance of Part 3 of OIC-CERT 5G Security Framework

Version 1.0

OICCERT-5-GUI-01-HUCSS-V1

Date: 30 October 2023

Disclaimer

It is recognized and accepted by all audiences, especially by each of the practitioners under the Harmonized and Unified Cybersecurity Certification System (HUCCS), that this document does not create any substantive or procedural rights, liabilities, or obligations for them.

This document has no binding effect in national or international law, and all practitioners under the HUCCS will not attempt to enforce this document in any domestic or international court or tribunal. If to implement this document or others partially or totally under the HUCCS would cause a practitioner to act in a manner inconsistent with applicable national and international laws or regulations, the practitioner should comply with applicable national and international laws or regulations.

In addition, this document makes no representation, warranty or undertaking with respect to and does not accept any responsibility for the accuracy or completeness or timeliness of the information contained in this document. In the event of any inconsistency between the actual implementation and this document, the actual implementation shall prevail.

TABLE OF CONTENT

Glossary

TERM OR CONCEPT	ABBREVIATION	DEFINITION
Harmonized and Unified Cybersecurity Certification System	HUCCS	A mechanism for the purpose of cross-recognizing of different cybersecurity certifications against the same standards. It is developed to guide OIC-CERT member states to plan, implement, improve, and continuously optimize cybersecurity certifications in a harmonized and unified manner, so that individually certified objectives in terms of cybersecurity by one country can be accepted by others in equivalent.
Practitioners	-	Entities involved in the establishment and operation of HUCCS.
OIC-CERT Member States	-	The member states of Organization of The Islamic Cooperation – Computer Emergency Response Teams.
HUCCS Member States	-	OIC-CERT member states which sign the HUCCS agreement and become member states of the HUCCS.
Conformity Assessment Body	CAB	A body is responsible for managing the overall establishment, implementation, and maintenance of HUCCS, forming by the OIC-CERT 5G Working Group. It contains two separate groups: CAB Executive and CAB Working Group.
CAB Executive	-	The top-level management group of HUCCS, which is responsible for decision-making in significant matters such as approving and releasing HUCCS policies and operation specifications.
CAB Working Group	CAB WG	The implementation group of CAB, and is responsible for general operations of establishment, implementation, and maintenance of the HUCCS such as, drafting policies and operation specifications, reviewing, and evaluating CB and EB's qualification, reviewing the compliance of certificate, and filing for record.
Certification Body	CB	Authorized third-party assessment entities that are responsible for operating certification schemes and overseeing issuance of certificates.
Evaluation Body	EB	Authorized third-party evaluation entities that perform one or more certification activities: audit, test, sampling, and associated with subsequent evaluating activities.
Applicant	-	Normally refers to providers, operators, or vendors that provide, operate, or supply the ICT applications, or equipment.

TERM OR CONCEPT	ABBREVIATION	DEFINITION
		Applicant could voluntarily apply for the cybersecurity certifications under the HUCCS.
Certificate	-	The official proof issued by CB to demonstrate the assurance level of applicants under selected cybersecurity standards.
Certification Activity	-	Certification activity refers to that activities taken by CB to assess the compliance with the mandatory requirements of cybersecurity standards for products and services or applicants to be certified.
Documentary System	-	Series of documents that are developed, managed, and improved in the operation of the HUCCS including HUCCS Policies, Operation Specifications and Certificate Basis and Records.
Cybersecurity Standards	-	Technical specifications, rules, or guidelines that can be commonly used for certification activities in the field of cybersecurity. Selected cybersecurity standards are cybersecurity standards selected and approved by CAB Executive, which are used for certificating in the HUCCS. Cybersecurity here refers to the confidentiality, integrity and availability of network and data, including but not limited to 5G security, data security, cloud security, etc.
Accredited CB and EB List	-	A list of CB and EB that have qualifications, necessary expertise, experiences in certification activities and are accredited by CAB Executive. Before examined and authorized by CAB Executive, such list collected and formed by CAB WG prior will be treated as CB and EB Candidate List.
Conformity level	-	The highest level of certification activities that CB and EB have the capability to perform.
RACI Matrix	-	A commonly used matrix for clarifying which individual or group is responsible for the successful completion of an activity, and the role that each will play. The matrix contains four roles: Responsible, Accountable, Consulted, and Informed and the definitions of each role list as follows: **Responsible (R):** Roles responsible for the implementation of the mandate. **Accountable (A):** Role with full responsibility for each activity. **Consulted (C):** Personnel with the information or capabilities needed to complete the activity.

TERM OR CONCEPT	ABBREVIATION	DEFINITION
		Informed (I): The one who should be notified of the result in a timely manner, but it is not necessary to consult for advice.

1 Introduction

Harmonized and Unified Cybersecurity Certification System (HUCCS) aims at an assurance mechanism that could help a one-region certified security assurance to be also accepted in different OIC-CERT member states. It can increase the efficiency of deploying common cybersecurity certifications in OIC-CERT member states. As a result, HUCCS can help to improve the overall level of cybersecurity for the OIC-CERT member states.

This document as a guidance defines the construction of the HUCCS precisely. By introducing the composition of the HUCCS, this document would further explain how different practitioners collaborate along with what kinds of descriptions. At the same time, this document proposes actions and approaches to maintain the HUCCS effectively in the long term. It also provides suggested guidelines for OIC-CERT member states to implement the process of certification and cross-recognition.

1.1 Objectives

The primary objectives of this document are to:

a. Set up HUCCS based on Part 3 of the OIC-CERT 5G security framework.

b. Direct OIC-CERT member states to design, execute, improve, and continuously optimize cybersecurity certifications in a harmonized way, so that the individually certified result by one OIC-CERT member state could be cross-recognized by others.

1.2 Scope

The scope of this document is to provide a detailed introduction and description of how to establish, implement and maintain HUCCS for OIC-CERT member states, which are the main service recipients of HUCCS and may voluntarily decide to join the HUCCS agreement.

Note: The establishment and election of specific practitioners are not involved in this document.

1.3 Outline

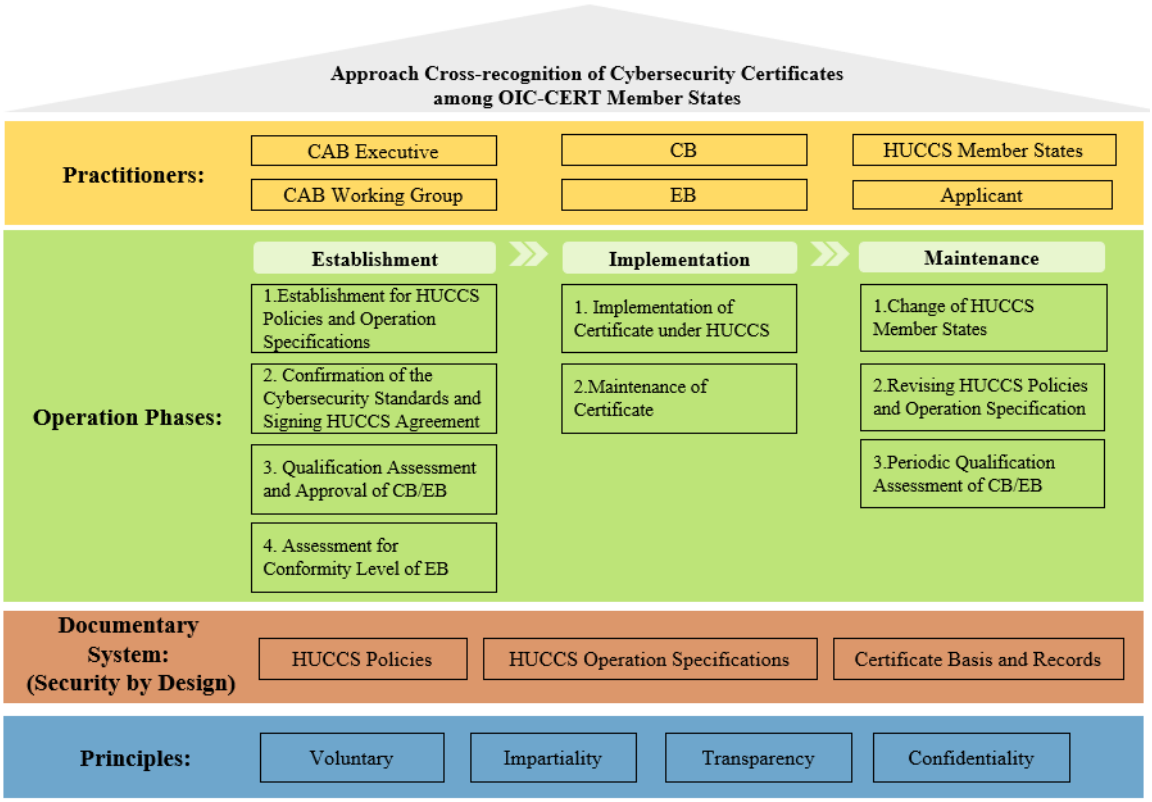
In this document, chapter 2 mainly introduces the architecture of the HUCCS, including the practitioners and their responsibilities, principles, and the documentary system of HUCCS to be followed. After that, chapter 3,4 and 5 present the main processes and actions of establishing, implementing, and maintaining the HUCCS, respectively.

2 HUCCS Overview

This chapter lays the foundation for the overall operation of the HUCCS by describing the basic principles, roles, responsibilities, operation phases, and the documentary system required or to be generated.

2.1 HUCCS Architecture

An architecture shown below is to clarify what the HUCCS contains. The objective of HUCCS is to approach cross-recognition of cybersecurity certificates among OIC-CERT member states. To achieve this objective, four basic principles and a documentary system are defined. And the operation of the HUCCS, divides into establishment, implementation, and maintenance, while different roles are responsible for their corresponding works. The principles, roles and documentary system are described thoroughly in this chapter.



Specifically, the establishment of HUCCS is illustrated in Chapter 3, which is to build up a basic operational system for cross-recognition. This phase includes establishing the HUCCS documentary system, selecting the cybersecurity standards for cross-recognition, signing the HUCCS agreement by OIC-CERT member states, and selecting CB and EB with professional qualifications to implement the certification activities.

The implementation of HUCCS states in chapter 4 is to promote HUCCS by conducting individual certification activities in the member states who joined the HUCCS (HUCCS member states). The specific processes of certification activities and maintenance of certificates are introduced.

Once the HUCCS is established, all roles in the HUCCS should continuously maintain the HUCCS to ensure its validity and applicability among HUCCS member states. Therefore, three common scenarios and

corresponding processes are provided in Chapter 5 to guide the roles to maintain the HUCCS, including change of HUCCS member states, revising HUCCS policies and operation specifications, and assessing qualifications of CB and EB periodically.

2.2 Principles

Voluntary

Voluntary means that each OIC-CERT member state voluntarily participates in the HUCCS or terminates its membership, which is subject to the consideration of national circumstances and demands for certification of the member states. The HUCCS does not create any substantive or procedural rights, liabilities, or obligations for OIC-CERT member states that are not signatories to HUCCS agreements.

Impartiality

Impartiality means non-discrimination and the exclusion of conflicts of interest. For instance, during the establishment of HUCCS, there should be no discrimination against partial member states due to economic, geographic, or religious factors. On the other hand, unless there is a lawful provision, there should not be any reason to impede or prevent eligible applicants from applying for or obtaining a certificate. CAB WG should review independence and conflicts of interest in the organizational structure of accredits CB and EB candidates and submit to CAB Executive for final accreditation. Furthermore, the accredited CB and EB should not have any conflict of interest with applicants or any other third parties involved in certification activities, which should also exclude any adverse influence on the certification activities and provide confidence in the reliability of certificates.

Transparency

Transparency means that practitioners should ensure transparency in specific operation of HUCCS and certification activities. For example, documents such as the Accredited CB and EB List should be accessible for public. Before the certification activities, applicants should be fully informed of not only relevant rights and obligations but also information on complaints and appeals procedures in a timely manner.

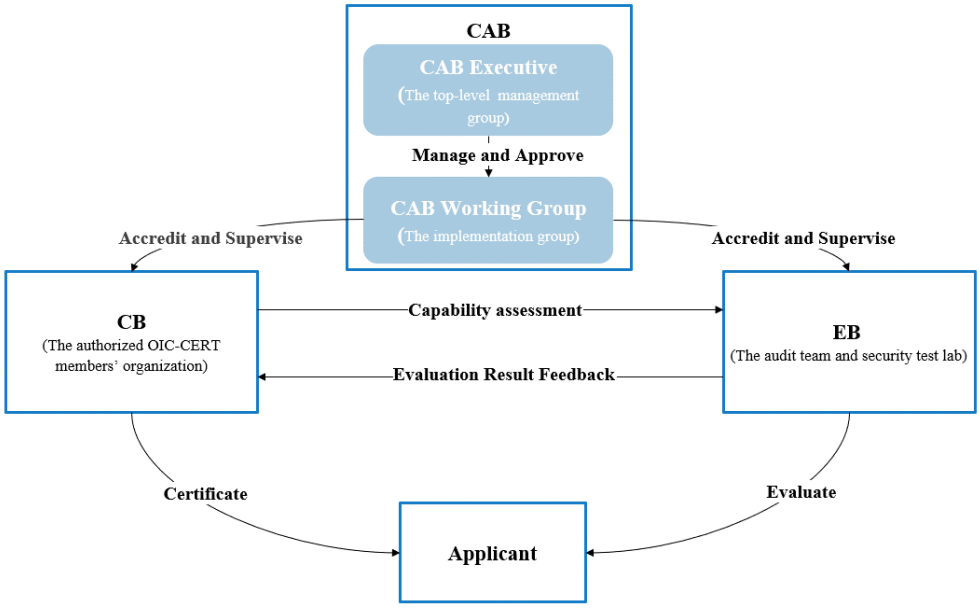
Confidentiality

Confidentiality means that practitioners and their personnel have the responsibility to maintain the confidentiality of confidential information obtained from applicants during certification activities under local regulation or any provision of national law, except for legal requirements. Confidential information generally includes personal information, commercially confidential information, trade secrets of the applicant, and other information claimed to use for the certification only. In practice, it is essential to reach non-disclosure agreements between applicants and relevant practitioners to certainly confirm the scope of confidential information.

2.3 Responsibilities of Practitioners

2.3.1 Relationships among Practitioners

To achieve proper operation of the HUCCS, practitioners work in the manner shown below.



2.3.2 CAB Executive

The CAB Executive is responsible to:

a) Review, approve and release the HUCCS policies and operation specifications and their revision.

b) Approve selected cybersecurity standards for certification activities.

c) Approve the changes of the HUCCS membership.

d) Review, approve and release the Accredited CB and EB List with the conformity level of CB.

e) Decide on matters that may have significant impacts on the HUCCS.

2.3.3 CAB Working Group (CAB WG)

The CAB WG is responsible to:

a) Record all documents (such as records of certificates granted), opinions, feedbacks, or other files in writing.

b) Collect demands, advice, and feedbacks from other practitioners.

c) Draft and revise work proposals, HUCCS policies, operation specifications, qualification assessment plans and other rules to support the HUCCS in future.

d) Correct before release of HUCCS polices and operation specifications.

e) Collect and analyze alternative cybersecurity standards for certifications.

f) Convene the HUCCS regular meetings and inform the relevant parties to participate.

g) Review and evaluate qualifications of CB and EB, including the conformity level of CB.

h) Supervise the certification process and evaluate the performance of CB and EB.

i) Continuously assess and analyze the effectiveness and availability of the HUCCS for optimization.

2.3.4 Certification Body (CB)

CB is responsible to:

a) Apply and maintain their own qualification and conformity level.

b) Evaluate conformity levels of accredited EB.

c) Assess evaluation processes, audit and evaluation reports of EB, and issue certificates to applicants.

d) Inform applicants of annual evaluation within the validity period of certificates.

e) Terminate the certificate of an applicant after its validity duration or failed on annual evaluation.

f) Report to CAB WG about the work summary and feedbacks during operation

In addition to above responsibilities, CB should develop information security, anti-corruption, and anti-bribery policies to fulfill the principles of confidentiality and transparency.

2.3.5 Evaluation Body (EB)

EB is responsible to:

a) Apply and maintain their own qualification and conformity level.

b) Accept certification applications, generate evaluation plans, and perform audits, technical tests, annual evaluation, and associate with subsequent evaluating activities.

c) Review and confirm rectifications and risk mitigation plans of all nonconformity issues found during the evaluation.

d) Produce the audit and evaluation reports.

e) Report to CAB WG on the work summary and feedbacks during operation.

f) Implement the annual evaluation of the applicant informed by CB.

Besides above responsibilities above, EB should develop information security, anti-corruption, and anti-bribery policies to fulfill the principles of confidentiality and transparency.

2.3.6 Applicant

Applicant is responsible to:

a) Submit certification applications to accredited EB.

b) Provide clear and accurate information and evidence required for the certification activities and cooperate with EB or CB in the certification process.

c) Rectify all non-conformities or implement risk mitigation plans.

d) Appoint annual evaluation with EB.

e) Sign the relevant commitments and ensure that there is no illegal behavior in certification activities.

2.4 Documentary System

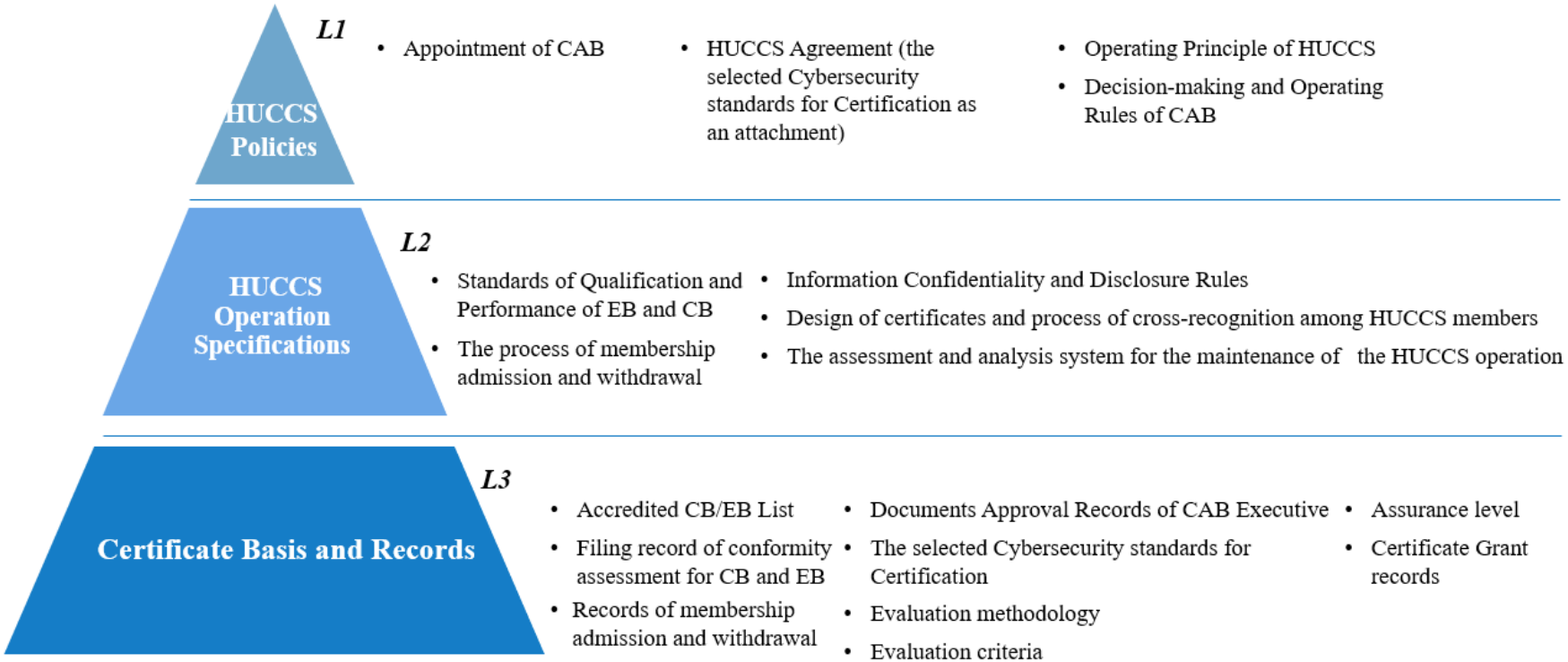
To ensure the operation of the HUCCS, it is necessary to establish a fundamental documentary system to stipulate the principles, the roles and responsibilities and operational rules etc.

The documentary system is divided into three levels, including the HUCCS policies, the HUCCS operation specifications, and certificate basis and records.

- Level 1: The HUCCS policies are the top-level documents that serve as a foundation for all practitioners in terms of decision-making, commitment and the overall direction and objective of the HUCCS.
- Level 2: The HUCCS operation specifications provide specific requirements and operation rules for all practitioners to implement specific activities under the HUCCS.
- Level 3: The certificate basis and records include referenced documents as well as working documents created during the operation of HUCCS for recording purposes.

  During the operation of HUCCS, a variety of working documents in Level 3 are generated including records, forms, and draft versions such as First Draft of Work Proposal, Meeting Minutes, Accreditation Letter, and Security and Technical Evaluation Report. A critical part of Certificate Basis and records are listed in following image and section 2.4.3 as a sample, while all types Certificate Basis and records are in Appendix II and all details of them are described in RACI tables of Chapters 3 to 5.

The specific levels and classification with examples are as follows：



* The documents' name shown here is for reference only. The actual name of documents created during the writing process maybe change.

2.4.1 Level 1 – HUCCS Policies

The HUCCS policies contain documents as follow:

Name	Drafter	Approver	Users	Main Content
Appointment of CAB	CAB WG	CAB Executive	• CAB Executive • CAB WG • OIC-CERT member states • CB • EB	Rules of appointing members of the CAB Executive and CAB WG and attached with the letter of appointment.
The HUCCS agreement	CAB WG	CAB Executive	• OIC-CERT member states	The agreement signing by the OIC-CERT member states serves as their endorsement of the HUCCS. The Cybersecurity standards selected and approved by the CAB Executive for certification should be included in the agreement as an attachment.
Operating principle of the HUCCS	CAB WG	CAB Executive	• CAB Executive • CAB WG	The basic principle for the HUCCS operation including voluntary, impartiality, transparency, confidentiality.
The Decision-making and operating rules of CAB	CAB WG	CAB Executive	• CAB Executive • CAB WG	Rules for CAB Executive to make decisions, including voting rules, voting procedure, and essential decision documents, etc., and for CAB WG to clarify processes and methods of carrying out its work, such as the contact channel, the way of holding meetings, the drafting process, the approval process, etc.

2.4.2 Level 2 – HUCCS Operation Specifications

The HUCCS operation specifications contain documents as follow:

Name	Drafter	Approver	Users	Scope of Content
Standards of qualification and performance of CB and EB	CAB WG	CAB Executive	• CAB Executive • CAB WG	Standards for CAB Executive and WG to assess the compliance of qualification and performance of CB and EB.
The assessment and analysis specifications for the	CAB WG	CAB Executive	• CAB Executive • CAB WG	Specifications for optimizing the HUCCS by getting feedbacks from relevant parties, assessing and analyzing the operation situation.

Name	Drafter	Approver	Users	Scope of Content
maintenance of the HUCCS operation				
The process of the HUCCS membership admission and withdrawal	CAB WG	CAB Executive	• CAB Executive • CAB WG • OIC-CERT member states • HUCCS member states	The process and guidelines for the admission, withdrawal, and removal (if applicable) of the HUCCS member states.
Confidentiality and disclosure rules	CAB WG	CAB Executive	• CAB Executive • CAB WG • HUCCS member states • CB • EB	The rules for confidentiality and disclosure issues regulate duties and responsibilities of different roles for confidential information protection. The rights of reasonable disclosure and the define of confidential level for each document should be included as well.
Design of certificates and process of cross-recognition among the HUCCS member states	CAB WG	CAB Executive	• HUCCS member states • CB • EB	The form and content of the certificate are defined to support the CB in issuing a compliant and formal certificate. The process that how the certificate is cross-recognized among HUCCS member states.

2.4.3 Level 3 – Certificate Basis and Records

The examples of certificate basis and records are as follows:

Name	Drafter	Approver	Users	Scope of Content
Accredited CB and EB List	CAB WG	CAB Executive	• CB • EB • Applicants	List of accredited CB and EB that have met qualifications, the necessary expertise and experience in relevant certification activities.
Filing record of conformity assessment for CB and EB	CAB WG	CAB Executive	• CB • EB • Applicants	This document is used to record the highest conformity level of accredited CB and EB that they can certify or evaluate, and to support the recognition of certificates in the HUCCS.
Records of membership admission and withdrawal	CAB WG	CAB Executive	• HUCCS member states	The record of admission, withdrawal, and removal (if applicable) of the HUCCS member states.

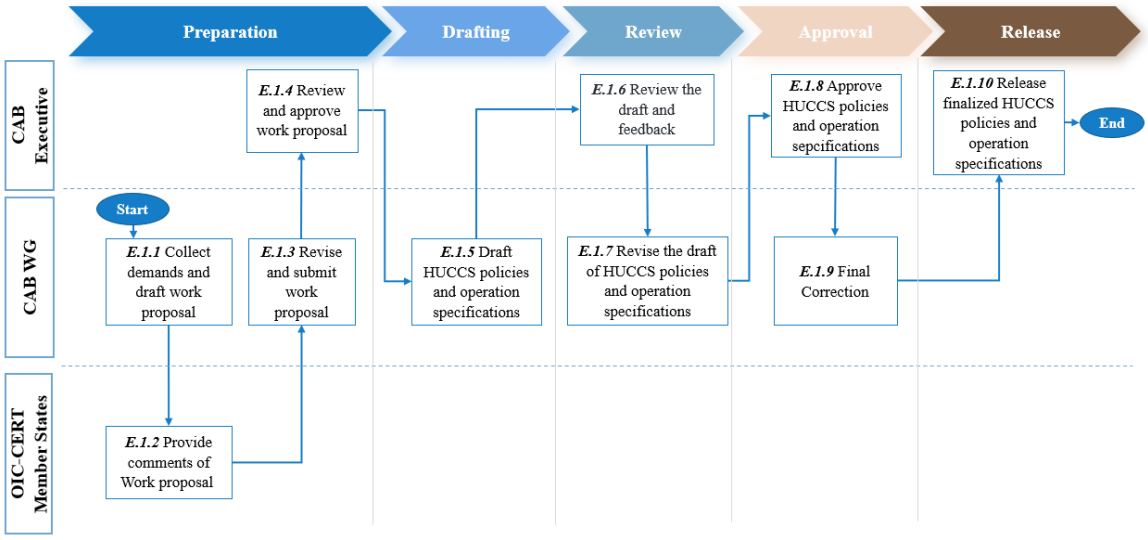
Name	Drafter	Approver	Users	Scope of Content
Documents approval records of CAB Executive	CAB WG	CAB Executive	• CAB Executive	The record for documents that CAB Executive has approved.
The selected cybersecurity standards for certification	N/A[1]	CAB Executive	• CB • EB	The content of selected cybersecurity standards, used by CB and EB in certification activities, includes the security requirement, the auditing target, and other supporting materials. The selected cybersecurity standards are also the basis for the development of the evaluation methodology, evaluation criteria, and assurance level.
Evaluation criteria	N/A	CAB Executive	• CB • EB	Evaluation criteria are designed as grading rules for CB and EB to evaluate and measure the conformity of the applicant or its evaluated product or service with the selected cybersecurity standards.
Evaluation methodology	N/A	CAB Executive	• CB • EB	Evaluation methodology describes the evaluation methods and processes performed by CB and EB in certification activities, documentary management of related information, and testing requirements for applicants.
Assurance levels	N/A	CAB Executive	• CB • EB	Assurance levels are assigned based on different results of compliance with cybersecurity standards and cross-recognition levels among the HUCCS member states.
Certificate grant records	CB	CAB WG	• CAB WG • CB • EB	A record of certificates issued by CB to applicants.

[1] The selected cybersecurity standards for certification, Evaluation criteria, Evaluation methodology and Assurance levels are only selected but not drafted by the practitioners of the HUCCS. These documents are drafted by the original authors.

3 Establishment of the HUCCS

The establishment of HUCCS is introduced in this chapter in four scenarios. Each scenario has a corresponding flowchart and each step in the flowchart is described in detail in the form of R.A.C.I matrix table.

3.1 Establishment for HUCCS Policies and Operation Specifications



3.1.1 Preparation

E.1.1 Collect demands and draft work proposal			
Input List		-	
RACI	**R**	CAB WG	
	A	-	
	C	OIC-CERT member states	
	I	CAB Executive	
Actions		1. The CAB WG should collect certification demands from the OIC-CERT member states.	
		2. The CAB WG should draft work proposal based on demands collected.	
		3.The CAB WG should send drafted work proposal to the OIC-CERT member states for comments.	
Output List		**Entity**	**Output**
		OIC-CERT member states	Feedback of Certification Demands
		CAB WG	First Draft of Work Proposal

Output Description	**First Draft of Work Proposal** Work Proposal should contain following contents: a) Necessity and feasibility of developing HUCCS policies and operation specifications. b) Main components of each HUCCS policy and operation specification, which include description of the role collaboration, coverage, and the value to OIC-CERT member states. c) Person in charge of this work. d) Budget. e) Work plan, which includes due date for key milestones in the work.

E.1.2 Provide comments of work proposal			
Input List		First Draft of Work Proposal	
RACI	**R**	OIC-CERT member states	
	A	OIC-CERT member states	
	C	-	
	I	CAB WG	
Actions		1. OIC-CERT member states should review the first draft of work proposal.	
		2. OIC-CERT member states should provide comments to CAB WG.	
Output List		**Entity**	**Output**
		OIC-CERT member states	Comments on Work Proposal
Output Description		**Comments on Work Proposal** There should be channels for OIC-CERT member states to provide comments, such websites, email etc. Comments should contain specific comments, and the form of the comments should be provided in writing with a clear record of who made them. The CAB WG should collect all the comments and form a record.	

E.1.3 Revise and submit work proposal			
Input List		Comments on Work Proposal	
RACI	**R**	CAB WG	
	A	CAB WG	
	C	OIC-CERT member states	
	I	CAB Executive	
Actions		1. The CAB WG should revise work proposal based on the comments from OIC-CERT member states.	
		2. The CAB WG should record all the revisions and correlate them with the comments from OIC-CERT member states.	
		3. The CAB WG should communicate and agree on the modification notes with the OIC-CERT member who submitted the comments.	
		4. The CAB WG submit work proposal and convene a meeting with the CAB Executive.	
Output List		**Entity**	**Output**
		CAB WG	Response to Comments and Revised Records

	CAB WG	Final Draft of Work Proposal
Output Description	**Final Draft of Work Proposal** Final Draft of Work Proposal should be revised based on comments from OIC-CERT member states, all the revisions should be recorded: a) Necessity and feasibility of developing HUCCS policies and operation specifications. b) Main components of each HUCCS policy and operation specification, which include description of the role collaboration, coverage, and the value to OIC-CERT member states. c) Person in charge of this work. d) Budget. e) Work plan which includes due date for key milestones in the work.	

E.1.4 Review and approve work proposal			
Input List		Final Draft of Work Proposal	
RACI	**R**	CAB Executive	
	A	CAB Executive	
	C	-	
	I	CAB WG, OIC-CERT member states	
Actions		1. The CAB Executive should review the work proposal submitted by the CAB WG.	
		2. The CAB Executive should evaluate and vote on the work proposal to decide whether to pass it or not.	
		3. The CAB Executive should record and inform the CAB WG of the result of voting and opinions.	
Output List		**Entity**	**Output**
		CAB Executive	Meeting Minutes and Opinions
Output Description		**Meeting Minute and Opinions** Meeting time, location, participants, vote results, opinions from different parties, and conclusion of the evaluation should be recorded during the meeting. The minutes should be sent to participants in writing after the meeting. The CAB Executive should evaluate work proposal prior to the formal vote and present their conclusions at the meeting. The result should be voted by the CAB Executive at the meeting, with general rule of OIC-CERT on how to record votes. The followings should be considered when evaluating the work proposal: a) Expected impacts and benefits of HUCCS. b) If there is any conflict with provisions and laws of OIC-CERT member states. c) Comparison and analysis with other similar international mechanism or certification. d) If budget and plan are set up appropriately. There should exist two results: approval or disapproval of the work proposal. If disapproval, and the CAB Executive should provide specific reasons.	

3.1.2 Drafting

<table>
<tr><th colspan="4">E.1.5 Draft HUCCS policies and operation specifications</th></tr>
<tr><td colspan="2">Input List</td><td colspan="2">Approved Work Proposal</td></tr>
<tr><td rowspan="4">RACI</td><td>R</td><td colspan="2">CAB WG</td></tr>
<tr><td>A</td><td colspan="2">CAB WG</td></tr>
<tr><td>C</td><td colspan="2">-</td></tr>
<tr><td>I</td><td colspan="2">CAB Executive</td></tr>
<tr><td colspan="2" rowspan="4">Actions</td><td colspan="2">1. The CAB WG should draft HUCCS policies and operation specifications based on the principles and purpose of the work proposal as well as the comments from the OIC-CERT member states.</td></tr>
<tr><td colspan="2">2. The CAB WG should conduct regular meetings internally to discuss and clarify current progress, content and methodology of the draft and report to the CAB Executive.</td></tr>
<tr><td colspan="2">3. The CAB WG should record all drafting processes and form an explanation of compilation.</td></tr>
<tr><td colspan="2">4. CAB WG should submit the first draft of policies and operation specifications to the CAB Executive.</td></tr>
<tr><td colspan="2" rowspan="5">Output List</td><td>Entity</td><td>Output</td></tr>
<tr><td>CAB WG</td><td>Explanation of Compilation</td></tr>
<tr><td>CAB WG</td><td>Meeting Minutes</td></tr>
<tr><td>CAB WG</td><td>First Draft of HUCCS Policies</td></tr>
<tr><td>CAB WG</td><td>First Draft of HUCCS Operation Specifications</td></tr>
<tr><td colspan="2">Output Description</td><td colspan="2">Explanation of Compilation
It is recommended that the following contents be included:
a) A brief description of the work, which includes the source of the tasks, background information on the work, and the drafting process.
b) Principles of drafting work, main content, and its reference when revising the HUCCS policies and operation specifications, which should include a comparison of content before and after the revision.
c) Results, process, and evidence of dealing with disagreements.
d) Explanations related to copyrights and patents.
e) Advice for the transition period and implementation dates.

Meeting Minutes
Record of an internal regular meeting of the CAB WG.

First Draft of HUCCS policies
These policies should include the following documents:
a) Appointment of CAB.
b) HUCCS Agreement (the selected Cybersecurity standards for Certification as an attachment involved in the agreement).
c) Operating Principle of HUCCS.
d) CAB Constitution - the Decision-making and Operating Rules of CAB.</td></tr>
</table>

	First Draft of HUCCS Operation Specifications These specifications should include the following documents: a) Standards of Qualification and Personnel Professional Identification of EB and CB. b) Supervisory mechanism for the continuing operation of the HUCCS. c) The process of membership admission and withdrawal. d) Information Confidentiality and Disclosure Rules. e) Design of certificates and process of cross-recognition among HUCCS member states.

3.1.3 Review

E.1.6 Review the draft and feedback			
Input List		First Draft of HUCCS Policies	
		First Draft of HUCCS Operation Specifications	
RACI	**R**	CAB Executive	
	A	CAB Executive	
	C	-	
	I	CAB WG	
Actions		1. The CAB Executive should conduct first-draft review meetings.	
		2. The CAB Executive should review the rationality, applicability and normative of HUCCS policies and operation specifications.	
		3. The CAB Executive should record the review meeting and form feedbacks in writing, then send feedbacks to the CAB WG.	
Output List		**Entity**	**Output**
		CAB Executive	Meeting Minutes and Feedbacks
Output Description		**Meeting Minutes and Feedbacks** The CAB Executive should review the contents of HUCCS policies and operation specifications at the review meeting. Meeting minutes should be clear and confirmed by all the participants. Feedbacks generated by the CAB Executive during the meeting should be recorded and forwarded to the CAB WG.	

E.1.7 Revise the draft of HUCCS policies and operation specifications		
Input List		Meeting Minutes and Feedbacks
RACI	**R**	CAB WG
	A	CAB WG
	C	CAB Executive
	I	-
Actions		1. The CAB WG should revise the HUCCS policies and operation specifications based on the feedbacks from the CAB Executive.
		2. The CAB WG should communicate with the CAB Executive about the purpose and modality of the amendment.
		3. The CAB WG should submit the revised version of HUCCS policies and operation specifications.

Output List	**Entity**	**Output**
	CAB WG	Revised HUCCS Policies
	CAB WG	Revised HUCCS Operation Specifications
	CAB WG	Submitted Explanation of Compilation
Output Description	**Revised HUCCS Policies** These policies should be modified by the CAB WG based on feedbacks from the CAB Executive. **Revised HUCCS Operation Specifications** These specifications should be modified by the CAB WG based on feedbacks from the CAB Executive.	

3.1.4 Approval

E.1.8 Approve HUCCS policies and operation specifications		
Input List		Revised HUCCS Policies
		Revised HUCCS Operation Specifications
RACI	**R**	CAB Executive
	A	CAB Executive
	C	-
	I	CAB WG
Actions		1. The CAB Executive should review the HUCCS Policies, HUCCS Operation Specifications, and Explanation of Compilation submitted by the CAB WG.
		2. The CAB Executive should vote on revised HUCCS policies and operation specifications, and the results should be tallied by the CAB Executive member states at the meeting.
		3. The CAB Executive should record the review meeting and form approval conclusion in writing, then inform the CAB WG.
Output List	**Entity**	**Output**
	CAB Executive	Meeting Minutes
Output Description	**Meeting Minutes** Meeting time, location, participants, vote results, opinions from different parties, and the conclusion of the evaluation should be recorded during the meeting. The minutes should be sent to participants in writing after the meeting. The CAB Executive should evaluate the work proposal prior to the formal vote and present their conclusions at the meeting. The result should be voted on by the CAB Executive at the meeting, with the general rule of OIC-CERT on how to record votes.	

E.1.9 Final Correction		
Input List		HUCCS Policies
		HUCCS Operation Specifications
RACI	**R**	CAB WG
	A	CAB Executive

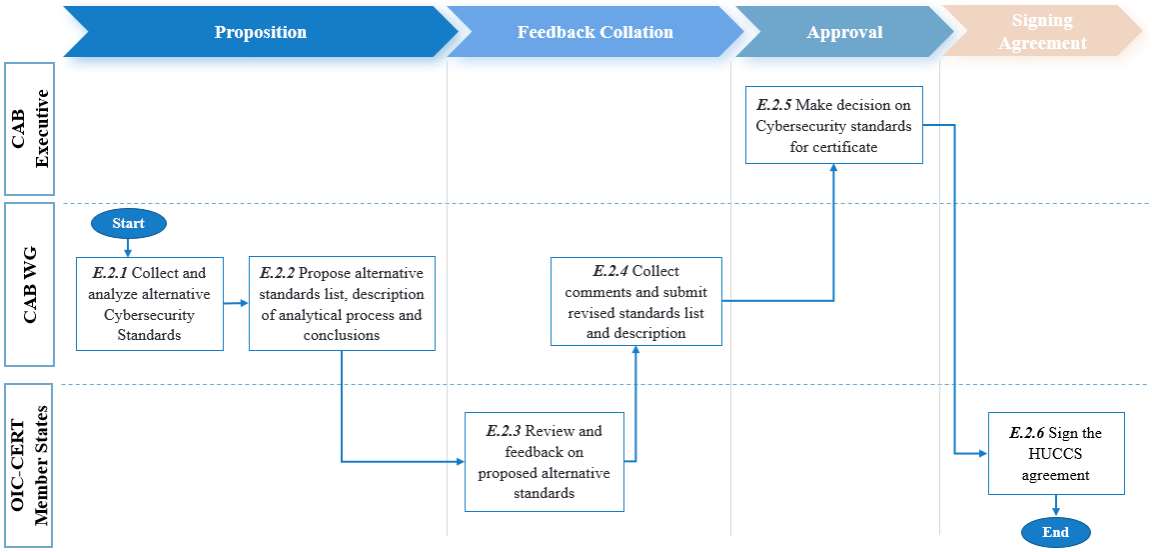
	C	-
	I	-
Actions		1. After the CAB Executive approve the final draft of HUCCS policies and operation specifications, the CAB WG should finally check the contents to ensure there are no textual or formatting errors.
		2. After finalizing the HUCCS policies and operation specifications, CAB WG should submit them to the CAB Executive and serve as a record.
Output List		**Entity** / **Output**
		CAB WG / Finalized HUCCS Policies
		CAB WG / Finalized HUCCS Operation Specifications
		CAB WG / Filing Record
Output Description		**Finalized HUCCS Polices & Operation Specifications** The CAB WG finalized the typo and format. If a typo exists, the CAB WG should correct and record it to ensure corrections can be tracked. **Filing Record** The CAB Executive keeps HUCCS policies and operation specifications on records for future reference.

3.1.5 Release

E.1.10 Release finalized HUCCS policy and operation specifications		
Input List		Finalized HUCCS Policies
		Finalized HUCCS Operation Specifications
RACI	**R**	CAB Executive
	A	CAB Executive
	C	-
	I	OIC-CERT member states
Actions		1. The CAB Executive should publish an announcement within the organization to state the release of HUCCS policies and operation specifications, as well as their main contents and objectives. In the meantime, provide channels for the OIC-CERT member states to access for details.
Output List		**Entity** / **Output**
		CAB Executive / HUCCS Policies Final Version for Release
		CAB Executive / HUCCS Operation Specifications Final Version for Release
Output Description		**HUCCS Policies & Operation Specifications Final Version for Release** HUCCS policies and operation specifications should be shared within the organization, and the target audience should be considered. Sharing channels include official websites, internal repositories, emails, etc. The OIC-CERT member states should be encouraged to understand the context and purpose of its release and to increase their interest in it.

3.2 Confirmation of the Cybersecurity Standards and Signing HUCCS Agreement

The following flowchart shows the process of confirming cybersecurity standards and signing the HUCCS agreement. This process can be implemented in parallel with ***E.1.5*** after the Work Proposal in ***E.1.4*** has been approved. It is important to note that the selected cybersecurity standards should be supplemented on the HUCCS agreement released in ***E.1.10***.



3.2.1 Proposition

E.2.1 Collect and analyze alternative Cybersecurity Standards			
Input List		-	
RACI	**R**	CAB WG	
	A	CAB WG	
	C	OIC-CERT member states	
	I	-	
Actions		1.The CAB WG should collect and form a list of cybersecurity-related standards in the industry.	
		2. The CAB WG should hold discussions with HUCCS member states on the standards on the list to initially identify the scope of the standards being analyzed.	
		3. The CAB WG should analyze the compatibility with the demands of the OIC-CERT member states and the scientific and acceptance by industries of the standards in the list.	
Output List		**Entity**	**Output**
		CAB WG	List of Alternative Cybersecurity Standards
Output Description		**List of Alternative Cybersecurity Standards** The list should include the following information: name, object, region covered, publisher of the standards, version, association, and explanatory document.	

E.2.2 Propose alternative standards list, description of analytical process and conclusions			
Input List		List of Alternative Cybersecurity Standards	
RACI	**R**	CAB WG	
	A	CAB WG	
	C	-	
	I	-	
Actions		1. The CAB WG should develop a proposal for recommended cybersecurity standards based on the analysis process, approach, and suggestions.	
		2. The CAB WG should send the drafted proposal to OIC-CERT member states for review and feedback.	
Output List		**Entity**	**Output**
		CAB WG	Drafted Proposal of Recommended Cybersecurity Standards
Output Description		**Drafted Proposal of Recommended Cybersecurity Standards** The proposal is used to describe the standards recommended to be introduced and the analytical process, the main contents include: a) Purpose. b) Analysis method. c) The scope of selected standards and considerations. d) Introduction of standards. e) Analysis of advantages and disadvantages of standards (scientific, timeliness, recognition, scope of application, etc.). f) Compatibility between standards and demands. g) Suggested standards.	

3.2.2 Feedback Collation

E.2.3 Review and feedback on drafted proposal			
Input List		Drafted Proposal of Recommended Cybersecurity Standards	
RACI	**R**	OIC-CERT member states	
	A	OIC-CERT member states	
	C	-	
	I	CAB WG	
Actions		1. The OIC-CERT member states should review the proposal and provide specific feedback.	
		2. The OIC-CERT member states should submit their feedbacks in writing to the CAB WG.	
Output List		**Entity**	**Output**
		OIC-CERT member states	Feedback Comments
Output Description		**Feedback Comments** Written comments with specific opinions and clear record of the author are required. The CAB WG ought to compile every comment and create a record.	

E.2.4 Collect comments and submit revised standards list and description			
Input List		Feedback Comments	
RACI	**R**	CAB WG	
	A	CAB WG	
	C	OIC-CERT member states	
	I	-	
Actions		1. The CAB WG should revise the proposal based on the comments from the OIC-CERT member states.	
		2. The CAB WG should record all the revisions and correlate them with the comments from the OIC-CERT member states.	
		3. The CAB WG should communicate and agree on the modification notes with the OIC-CERT member states that submitted the comments.	
		4. The CAB WG submit a finalized proposal and convenes a meeting with the CAB Executive.	
Output List		**Entity**	**Output**
		CAB WG	Response to Comments and Revised Records
		CAB WG	Finalized Proposal of Recommended Cybersecurity Standards
Output Description		**Response to Comments and Revised Records** All comments should be recorded and responded to by the CAB WG. The type of response may include a description of the modifications to the content, an explanation and description of the original proposal, or an explanation of the non-adoption of the comment. **Finalized Proposal of Recommended Cybersecurity Standards** Updates based on the drafted version should be consistent with revised records.	

3.2.3 Approval

E.2.5 Make decision on Cybersecurity standards for certificate			
Input List		Finalized Proposal of Recommended Cybersecurity Standards	
RACI	**R**	CAB Executive	
	A	CAB Executive	
	C	-	
	I	CAB WG, OIC-CERT member states	
Actions		1. The CAB Executive should review the proposal submitted by the CAB WG.	
		2. The CAB Executive should evaluate and vote on the proposal to decide on selected cybersecurity standards.	
		3. The CAB Executive should record and inform the CAB WG and OIC-CERT member states of the result of voting and opinions.	
Output List		**Entity**	**Output**
		CAB Executive	Meeting Minutes and Opinions

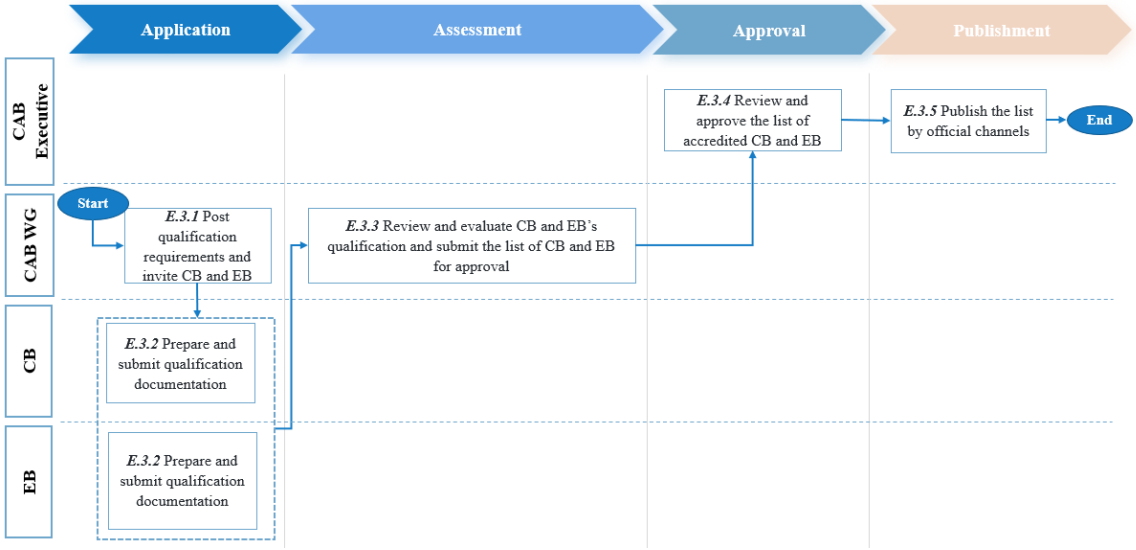
Output Description	**Meeting Minutes and Opinions** Meeting's time, locations, participants, voting results, opinions from various parties, and conclusion should all be recorded. The minutes should be sent to participants in writing after the meeting. The selected cybersecurity standards, along with any further details like assessment process, assurance, etc., the decision's justifications, and the standards' current version, should be included in the meeting's conclusions.

3.2.4 Signing Agreement

E.2.6 Sign the HUCCS agreement			
Input List		Meeting Minutes and Opinions	
RACI	**R**	OIC-CERT member states	
	A	CAB Executive	
	C	-	
	I	CAB WG	
Actions		1. The CAB WG should include the approved standards in the HUCCS agreement for signing.	
		2. The CAB WG should distribute the HUCCS agreement to OIC-CERT member states;	
		3. OIC-CERT member states are expected to provide feedback on whether to sign up for participation within a specified period.	
		4. The CAB WG should collect feedbacks, communicate the results to the CAB Executive and form a released version of the HUCCS agreement.	
Output List		**Entity**	**Output**
		OIC-CERT member states	Signed Feedback
		CAB WG	Released Version of the HUCCS Agreement
Output Description		**Signed Feedback** If a member agrees to sign the agreement, a representative must be designed to provide the CAB WG with written feedback within a predetermined time limit. **Released Version of the HUCCS Agreement** This document should include the list of OIC-CERT member states that have decided to sign the agreement. In addition, the document structure should be checked again to ensure that it complies with the OIC-CERT's document format requirements. Depending on how the document will be used, non-editable and editable versions of the document should be created for release and filing. There should be at least the file name, version number, release date, and copyright information.	

3.3 Qualification Assessment and Approval of CB and EB

The following flowchart shows the processes for electing accredited CB and EB. In this scenario, CAB Executive publishes the list of accredited EB and CB; in the meanwhile, the conformity level of CB are defined. The details of the assessment are expanded in the following R.A.C.I matrix tables.



3.3.1 Application

E.3.1 Post qualification requirements and invite CB and EB		
Input List		Standards of Qualification and Performance of CB and EB
RACI	**R**	CAB WG
	A	CAB Executive
	C	HUCCS member states
	I	CB and EB Candidates
Actions		1. The CAB WG posts requirements for CB and EB based on the cybersecurity standards.
		2. The CAB WG should convene to recommend CB and EB to HUCCS member states.
		3. The CAB should open enrollment channels to CB and EB in HUCCS member states.
Output List	**Entity**	**Output**
	CAB WG	Recruitment Announcement
Output Description	**Recruitment Announcement** The following requirements of CB and EB should be included in this announcement, but not exclusively: a) Certificates under cybersecurity standards. b) Business license. c) Business scope. d) Evaluation equipment. e) Experience with certificates, auditing, and technical testing. f) Other requirements based on cybersecurity standards.	

	For CB, there is an additional requirement: g) Assurance level that CB can certificate and proof documents.

E.3.2 Prepare and submit qualification documentations			
Input List		Recruitment Announcements	
RACI	**R**	CB and EB Candidates	
	A	-	
	C	CAB WG	
	I	CAB WG	
Actions		1. CB and EB should evaluate internally whether they meet the requirements based on the announcement and determine the scope and assurance level of the application.	
		2. The CAB WG should provide consulting channels for CB and EB to consult on the questions corresponding to qualifications.	
		3. CB and EB should prepare documents that demonstrate their qualifications.	
		4. CB and EB should submit their qualification documentation to the CAB WG.	
Output List		**Entity**	**Output**
		CB	Qualification Documentations
		EB	Qualification Documentations
Output Description		**Qualification Documentations** All requirements indicated in E.3.1 should be satisfied, and qualification paperwork should be submitted in accordance with the guidelines outlined in recruitment announcements. The document's content must be accurate and thorough.	

3.3.2 Assessment

E.3.3 Review and evaluate CB and EB's qualification and submit the list of CB and EB for approval			
Input List		Qualification Documentations	
RACI	**R**	CAB WG	
	A	CAB Executive	
	C	-	
	I	CB and EB Candidates	
Actions		1. The CAB WG should review the qualification documents and check for completeness.	
		2. The CAB WG should verify the accuracy of the documentation submitted by the CB and EB through interviews, visits, inspections etc., and identify whether the documentation can fulfill the requirements.	
		3. The CAB WG should form a list of CB and EB who meet requirements and submit it to the CAB Executive for approval.	
Output List		**Entity**	**Output**
		CAB WG	CB and EB Candidate List

Output Description	**CB and EB Candidate List** CB and EB on this list are preliminary until they have been examined and authorized by the CAB Executive. The qualifications of management, technical professionals, understanding of cybersecurity, compliance with laws, capability of CB and EB, number of professional staff, and equipment that can support certifying or evaluating are just a few of the factors considered during reviews and evaluations.

3.3.3 Approval

E.3.4 Review and approve the list of accredited CB and EB			
Input List		CB and EB Candidate List	
RACI	**R**	CAB Executive	
	A	CAB Executive	
	C	-	
	I	CAB WG, HUCCS Member states, CB, and EB Candidates	
Actions		1. The CAB Executive should review the list of CB and EB, including qualifications and compliance with the CAB WG's selection of CB and EB.	
		2. The CAB Executive should approve the list of CB and EB.	
		3. The CAB WG should issue accreditation letters to CB and EB on the list.	
Output List		**Entity**	**Output**
		CAB Executive	Accredited CB and EB List
		CAB WG	Accreditation Letter
Output Description		**Accredited CB and EB List** CB and EB on the list are officially approved by the CAB Executive and will receive accreditation letters from the CAB WG. **Accreditation Letter** This letter should list the parties that are accrediting and accredited, the scope of the assessment or certification that is accredited, the duration of the evaluation, etc. The letter of accreditation for CB should also include the highest assurance level for the CB certificate.	

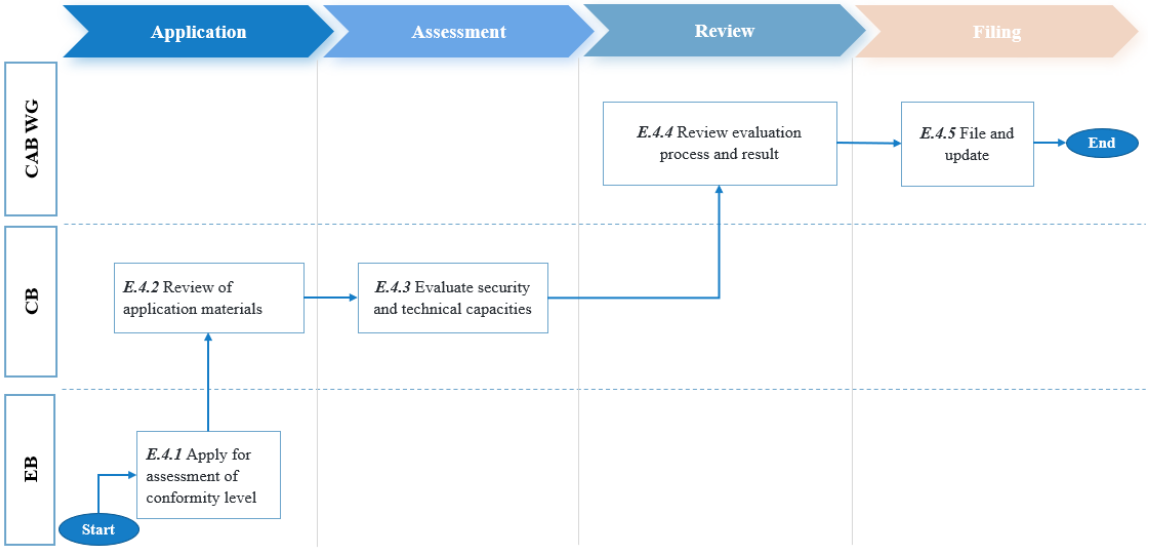
3.3.4 Publishment

E.3.5 Publish the list by official channels			
Input List		Accredited CB and EB List	
RACI	**R**	CAB Executive	
	A	CAB Executive	
	C	-	
	I	HUCCS member states, Applicant, CB, and EB Candidates	
Actions		1. The CAB Executive releases the list via official channels, such as their website or email.	
Output List		**Entity**	**Output**
		CAB Executive	Released Accredited CB and EB List

Output Description	**Released Accredited CB and EB List** The released version should be published through official channels accessible to HUCCS member states or applicants so that it is easy to locate the available CB or EB. Released versions only include accredited CB and EB and the conformity level of CB. The conformity level of EB will continuously update after passing the CB evaluation.

3.4 Assessment for Conformity Level of EB

The following flowchart shows the processes by which CB assesses conformity level of EB. The information on the Accredited CB and EB List is updated as the EB conformity levels are finalized. The details of the assessment are expanded in the following R.A.C.I matrix tables.



3.4.1 Application

E.4.1 Apply for assessment of conformity level			
Input List		Standards of Qualification and Performance of CB and EB	
RACI	**R**	Accredited EB	
	A	Accredited EB	
	C	-	
	I	Accredited CB	
Actions		1. The accredited EB should self-assess the conformity level based on the documentation and prepare materials according to the qualification requirements corresponding to the applied level.	
		2. The accredited EB should submit the corresponding materials to the accredited CB according to the application requirements.	
Output List		**Entity**	**Output**
		EB	Application Materials

Output Description	**Application Materials** These materials include, but not be limited to the following: a) Certificates under cybersecurity standards. b) Personnel qualifications. c) Equipment qualifications. d) Past projects on security tests.

E.4.2 Review of application materials			
Input List		Application Materials	
RACI	**R**	Accredited CB	
	A	Accredited CB	
	C	-	
	I	Accredited EB	
Actions		1. CB should review the completeness of the application materials submitted by EB.	
		2. CB should formulate a security and technical evaluation plan.	
Output List		**Entity**	**Output**
		CB	Security and Technical Evaluation Plan
Output Description		**Security and Technical Evaluation Plan** This plan should contain the basic information for the security and technical evaluation, such as purpose, subject, and scope. The specific implementation plan should also be clear. The overall evaluation plan should include organizational and staffing arrangements, time schedules, etc., the specific implementation plan should include arrangements for the investigation aspects of the security and technical evaluation.	

3.4.2 Assessment

E.4.3 Evaluate security and technical capacities			
Input List		Security and Technical Evaluation Plan	
RACI	**R**	Accredited CB	
	A	Accredited CB	
	C	-	
	I	Accredited EB	
Actions		1. The CB should confirm the accuracy of the application information through interviews, walk-throughs, technical tests, inspections, etc., to identify the highest conformity level that can be granted.	
		2. The CB should determine the highest assurance level that EB can carry out based on the evidence.	
		3. The CB should issue a security and technical evaluation report.	
Output List		**Entity**	**Output**

	CB	Security and Technical Evaluation Records
	CB	Security and Technical Evaluation Report
Output Description	**Security and Technical Evaluation Records** These records can be evidence of evaluation results, which should include all matters evaluated during the process. **Security and Technical Evaluation Report** The following information should be included in this report, but not exclusively: a) Evaluating CB. b) Evaluation Process. c) Conclusion of the conformity level of EB. d) Scope of security and technical testing of EB.	

3.4.3 Review

E.4.4 Review evaluation process and result			
Input List		Security and Technical Evaluation Report	
RACI	**R**	CAB WG	
	A	CAB WG	
	C	-	
	I	Accredited CB	
Actions		1.The CAB WG should review the evaluation report submitted by CB to check the compliance of the evaluation process and result.	
Output List		**Entity**	**Output**
		CAB WG	Review Result
Output Description		**Review Result** This result should be a clear conclusion about whether the evaluation report is accepted and whether the evaluation process meets reasonable and lawful requirements.	

3.4.4 Filing

E.4.5 File and update		
Input List		Security and Technical Evaluation Report
		Accredited CB and EB List
RACI	**R**	CAB WG
	A	CAB WG
	C	-
	I	CB, EB, OIC-CERT member states, Applicant
Actions		1. The CAB WG should record and archive the reviewed evaluation reports and conclusions.
		2. The CAB WG should update the list of CB and EB by adding the conformity level of EB.

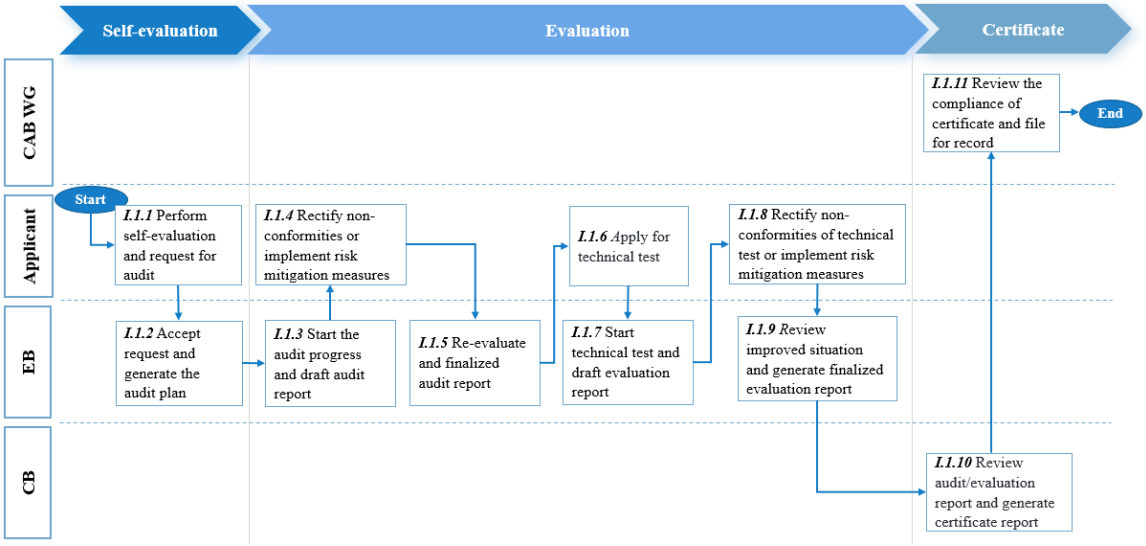
Output List	Entity	Output
	CAB WG	Newly Accredited CB and EB List
Output Description	**Newly Accredited CB and EB List** After determining the conformity level of EB, the CAB WG should update this new information to the EB List.	

4 Implementation of the HUCCS

The implementation of HUCCS introduces in this chapter under two scenarios. Each scenario has a corresponding flowchart and each step in the flowchart is described in detail in the form of R.A.C.I matrix table.

4.1 Implementation of Certificate under HUCCS

The following flowchart shows the processes for implementing certificates under HUCCS. Certification is conducted under elected cybersecurity standards in the phase of establishment.



4.1.1 Self-evaluation

I.1.1 Perform self-evaluation and request for audit		
Input List		-
RACI	**R**	Applicant
	A	Applicant
	C	-
	I	EB
Actions		1. The applicant should perform self-evaluation based on the certificates they want to apply. Self-evaluating should base on the security requirements of cybersecurity standards.
		2.The applicant should sign the conformance claims to prove that development and lifecycle of assessed product/service conform to the requirements of cybersecurity standards.

	3. The applicant should submit the self-evaluation reports and conformance claims to EB for requesting audit.	
Output List	**Entity**	**Output**
	Applicant	Self-evaluation Report
	Applicant	Conformance Claim
Output Description	**Self-evaluation Report** This report should record the process of self-evaluation performed by the applicant; it should include but not be limited to: a) Evaluated product/service. b) Assurance level. c) Compliance with the development and lifecycle of the evaluated product/service. d) Other requirements under the certification of cybersecurity standards. **Conformance Claim** This claim should prove that the development and lifecycle of the evaluated product/service conform to the security requirements defined in the cybersecurity standard.	

I.1.2 Accept request and generate the audit plan			
Input List		Self-evaluation Report	
		Conformance Claim	
RACI	**R**	EB	
	A	EB	
	C	-	
	I	Applicant	
Actions		1. The EB should accept audit request if applicant provide complete application materials and can prove applied assurance level is consistent to applicant's self-evaluation.	
		2. The EB audit team should review the self-evaluation report and conformance claims submitted by applicant.	
		3. The EB audit team should generate the audit plan based on the communication with applicant.	
Output List		**Entity**	**Output**
		EB	Audit Plan
Output Description		**Audit Plan** The following information should be included in this plan, but not exclusively: a) Basis of audit. b) Audit object. c) Audit period. d) Audit scope. e) Audit principle. f) Audit date. g) Audit type. h) Audit methodologies. i) Personnel arrangement. j) Related internal documents of applicant.	

4.1.2 Evaluation

<table>
<tr><th colspan="4">I.1.3 Start the audit progress and draft audit report</th></tr>
<tr><td colspan="2">Input List</td><td colspan="2">Audit Plan</td></tr>
<tr><td rowspan="4">RACI</td><td>R</td><td colspan="2">EB</td></tr>
<tr><td>A</td><td colspan="2">CB</td></tr>
<tr><td>C</td><td colspan="2">-</td></tr>
<tr><td>I</td><td colspan="2">Applicant</td></tr>
<tr><td colspan="2" rowspan="6">Actions</td><td colspan="2">1. The EB audit team should conduct an on-site assessment in accordance with the implementation plan and send the Documents Required List to the applicant prior to the on-site visit.</td></tr>
<tr><td colspan="2">2. The applicant should prepare development lifecycle supporting materials of audited product/service based on the Documents Required List.</td></tr>
<tr><td colspan="2">3. The applicant should prepare the workspace, supporting staff and other support required for the assessment;</td></tr>
<tr><td colspan="2">4. The EB audit team generate the audit report based on the evidence collected during the audit process and sends it to CB for review.</td></tr>
<tr><td colspan="2">5. The CB should review the audit report. If there is any doubt or uncertainty, CB should communicate and reach consensus with EB.</td></tr>
<tr><td colspan="2">6. EB audit team should revise the audit report and send it to CB and applicant, then communicate the nonconformity issues with Applicant.</td></tr>
<tr><td colspan="2" rowspan="4">Output List</td><td>Entity</td><td>Output</td></tr>
<tr><td>EB</td><td>Documents Required List</td></tr>
<tr><td>EB</td><td>Draft Audit Report</td></tr>
<tr><td>EB</td><td>List of Nonconformity Issues</td></tr>
<tr><td colspan="2">Output Description</td><td colspan="2">Documents Required List
The EB should prepare a DRL in advance based on the evaluation criteria and the subject to be audited, which will be given to the applicant to prepare for the audit to enhance efficiency. The DRL is not unchanged. As the audit proceeds, it may be necessary to supplement or adjust the relevant information to be obtained to achieve the audit objectives.

Draft Audit Report
The audit report should provide a complete, accurate, concise, and clearly documented record of the audit and include the following elements:
a) Basis of audit.
b) Audit objectives.
c) Audit scope.
d) Audit client (Applicant).
e) Audit entity (EB) and team members.
f) Audit time and location.
g) Evaluation Criteria.
h) Audit findings and related evidence.
i) Conclusions.
j) Statement of the degree of compliance with the audit guidelines.
k) Discrepancies between the audit team and the auditee.

List of Nonconformity Issues
Upon completion of the audit, a list of all non-conformities is required to be issued for the applicant to rectify or supplement mitigation measures.</td></tr>
</table>

I.1.4 Rectify non-conformities or implement risk mitigation measures			
Input List		Audit Report	
		List of Nonconformity Issues	
RACI	**R**	Applicant	
	A	Applicant	
	C	EB	
	I	-	
Actions		1. The applicant should implement internal measures to rectify nonconformity issues based on the audit report and list of nonconformity issues.	
		2. The applicant should implement risk mitigation measures if nonconformity issues cannot be avoided completely. These risk mitigation measures should be able to reduce the frequency of losses or the magnitude of the impact of a risk.	
		3. The applicant should record these rectification and risk mitigation measures as evidence.	
Output List		**Entity**	**Output**
		Applicant	Rectification Records
Output Description		**Rectification Records** These records should include but not be limited to the following: a) Rectification or risk mitigation measures of each non-conformity matter. b) Rectification processes. c) Rectification results.	

I.1.5 Re-evaluate and finalized audit report			
Input List		Rectification Records	
RACI	**R**	EB	
	A	CB	
	C	-	
	I	CB, Applicant	
Actions		1. The EB audit team should evaluate the rectification records and ensure all nonconformities have been cleared.	
		2. The EB audit team should finalize the audit report based on the rectification results and submit it to CB for reviewing.	
		3. The applicant should sign compliance declaration to clarify that all requirements are satisfied.	
Output List		**Entity**	**Output**
		EB	Audit Report
		Applicant	Compliance Declaration

Output Description	**Audit Report** The audit report should complement rectification measures and results should correspond to each nonconformity issue. **Compliance Declaration** This declaration should indicate that the development and lifecycle of the evaluated product/service are compliant with cybersecurity standards and allow the applicant to apply for technical tests. In addition, the audit process should be included in the compliance declaration.

I.1.6 Apply for technical test			
Input List		Audit Report	
		Compliance Declaration	
RACI	**R**	Applicant	
	A	EB	
	C	-	
	I	EB	
Actions		1. The applicant should apply for technical tests and submit an audit report and compliance declaration to the EB security test lab.	
Output List		**Entity**	**Output**
			N/A
Output Description		**N/A**	

I.1.7 Start technical test and draft evaluation report		
Input List		Audit Report
		Selected Cybersecurity Standards for Certification
		Compliance Declaration
RACI	**R**	EB
	A	CB
	C	-
	I	Applicant
Actions		1. The EB audit team should provide the audit report to EB security test lab to support the compliance declaration given by the applicant at I.1.1.
		2. The EB security test lab should evaluate the audited processes base on the security requirements and evaluate the security of the product.
		3. The EB security test should generate an evaluation report to reflect how much the applicant has complied with the equipment security and equipment development and lifecycle process requirements, and the security level of the product and then submit it to CB for review.
		4. The CB should review the audit report. If there is any doubt or uncertainty, CB should communicate and reach consensus with EB.
		5. The EB security test lab should communicate the nonconformity issues with the applicant.

Output List	**Entity**	**Output**
	EB	Draft Evaluation Report
	EB	List of Nonconformity Issues
Output Description	**Draft Evaluation Report** The evaluation report should contain at least the following: a) Testing provider and information. b) Test objective. c) Test object. d) Testing methods (different methods that may be adopted depending on the products and standards, such as code auditing, vulnerability scanning, penetration testing, etc.). e) Testing process. f) Testing tools and versions. g) Test findings and evidence. h) Conclusion. **List of Nonconformity Issues** Upon completion of the technical evaluation, a list of all non-conformities is required to be issued for the applicant to rectify or supplement mitigation measures.	

I.1.8 Rectify non-conformities of technical test or implement risk mitigation measures			
Input List		Evaluation Report	
		List of Nonconformity Issues	
RACI	**R**	Applicant	
	A	Applicant	
	C	EB	
	I	EB	
Actions		1. The applicant should implement internal measures to rectify nonconformity issues based on the evaluation report and list of nonconformity issues.	
		2. The applicant should implement risk mitigation measures if nonconformity issues cannot be avoided completely. These risk mitigation measures should be able to reduce the frequency of losses or the magnitude of the impact of a risk.	
		3. The applicant should record these rectification and risk mitigation measures as evidence.	
Output List		**Entity**	**Output**
		Applicant	Rectification Records
Output Description		**Rectification Records** The following information should be included in these records, but not exclusively: a) Rectification or risk mitigation measures of each non-conformity matter. b) Rectification processes. c) Rectification results.	

I.1.9 Review improved situation and generate finalized evaluation report			
Input List		Rectification Records	
RACI	**R**	EB	
	A	EB	
	C	-	
	I	Applicant	
Actions		1. The EB security test lab should evaluate the rectification records and ensure all security requirements are satisfied.	
		2. The EB security test lab should finalize the evaluation report to clarify the rectification results.	
		3. The EB security test lab should submit the finalized evaluation report to CB.	
Output List		**Entity**	**Output**
		EB	Evaluation Report
Output Description		**Evaluation Report** The finalized evaluation report should complement rectification measures and results should correspond to each nonconformity issue.	

4.1.3 Certificate

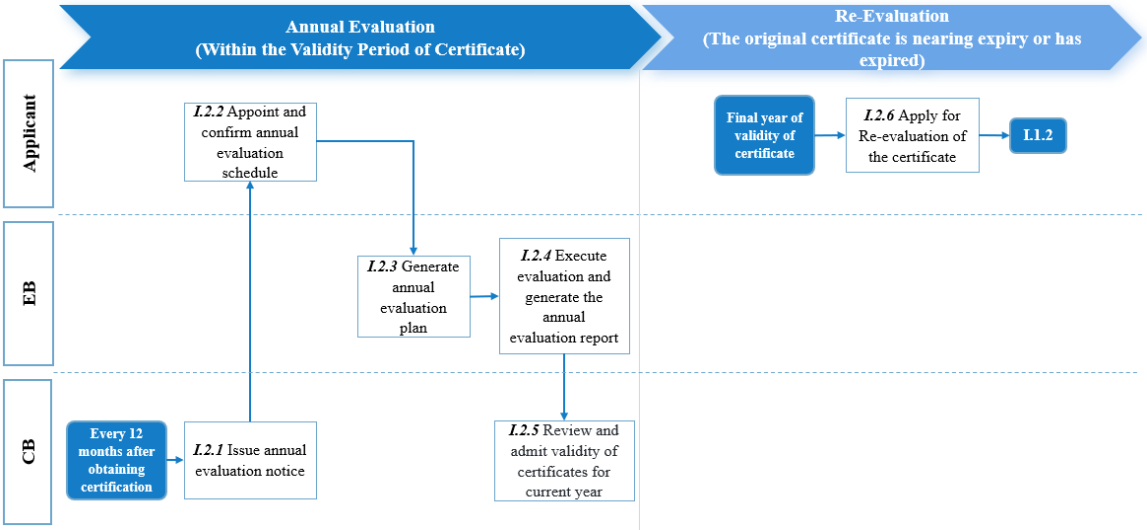
I.1.10 Review audit/evaluation report and generate certificate report			
Input List		Audit Report	
		Evaluation Report	
RACI	**R**	CB	
	A	CB	
	C	EB	
	I	Applicant	
Actions		1. The CB should review the audit report and evaluation report generated by EB, the review should include but not be limited to: satisfied security requirements, rectification results, compliance with evaluation, etc.	
		2. The CB should generate a certificate report if all requirements for evaluated product/service are satisfied.	
		3. The CB should inform the applicant of the certification result.	
Output List		**Entity**	**Output**
		CB	Certificate
Output Description		**Certificate** The following information should be included in the certificate, but not exclusively: a) Basic information of the applicant. b) Evaluated product/service. c) Certification results. d) Security level of the product/service. e) Validity period. f) Annual evaluation date.	

I.1.11 Review the compliance of certificate and file for record			
Input List		Certificate	
RACI	**R**	CB	
	A	CAB WG	
	C	-	
	I	CAB WG	
Actions		1. The CAB WG should review the compliance of certification process. If there is any doubt or uncertainty, the CAB WG should communicate and reach consensus with CB.	
		2. The CB should file this certificate with the CAB WG for its future tracking.	
Output List		**Entity**	**Output**
		CAB WG	Filing Record
Output Description		**Filing Record** This record should be the evidence for the CAB WG's future tracking. The following information should be included in this record, but not exclusively: a) Filing time. b) Basic information about CB and EB (name of bodies, conformity level, etc.). c) Basic information about the applicant (name of organization, product/service, etc.).	

4.2 Maintenance of Certificate

The following flowchart shows the processes for maintaining certificate which are divided into two scenarios:

- Within the validity period of certificate: annual evaluation is required to determine whether the applicant still meets the security requirements of the certificates. If the annual review fails, the validity of the certificate may be terminated by CB.
- The original certificate is nearing expiry or has expired: in the last year of the validity period of certificates, the applicant should apply for re-evaluation and re-open the certification process.



4.2.1 Annual Evaluation (With the Validity Period of Certificate)

I.2.1 Issue annual evaluation notice		
Input List		Certificate Report
RACI	**R**	CB
	A	CB
	C	-
	I	Applicant
Actions		1. The CB should maintain the validity period of issued certificate reports and specify their annual evaluation schedule.
		2. The CB should issue an annual assessment notice to the applicant about every 12 months after issuing the certificate report as long as within the validity period of the certificates report.
Output List	**Entity**	**Output**
	CB	Annual Evaluation Notice
Output Description		**Annual Evaluation Notice** The notice should include the recipient, the certificates and the scope of the annual evaluation, and specify the latest time to carry out the annual evaluation.

I.2.2 Appoint and confirm annual evaluation schedule		
Input List		Annual Evaluation Notice
RACI	**R**	Applicant
	A	Applicant
	C	EB
	I	CB
Actions		1. Upon receipt of the notice, the Applicant should contact the EB that issued the audit report and assessment report within the specified time;
		2. The Applicant should communicate with the EB on when the annual evaluation will be conducted.

Output List	Entity	Output
	Applicant	Return Receipt
Output Description	**Return Receipt** The receipt as the response to annual evaluation notice should clarify the attitude of the applicant: whether applicant agrees or disagrees the annual evaluation or wants to change applications.	

I.2.3 Generate annual evaluation plan			
Input List		-	
RACI	**R**	EB	
	A	EB	
	C	-	
	I	Applicant	
Actions		1. The EB should develop an evaluation plan based on a negotiated start time, evaluation scope, and evaluation objectives, and reach a consensus with the Applicant.	
Output List		**Entity**	**Output**
		EB	Annual Evaluation Plan
Output Description		**Annual Evaluation Plans** The structure of the annual evaluation plan should be the same as the plan for the first certification, differing only in the scope of the evaluation and the subject matter (narrowed or consistent). The annual evaluation plan should be included as follows: a) Evaluation object. b) Evaluation period. c) Evaluation scope. d) Evaluation principle. e) Evaluation date. f) Evaluation type. g) Evaluation methodologies. h) Personnel arrangement. i) Related internal documents of the applicant.	

I.2.4 Execute evaluation and generate the annual evaluation report		
Input List		Annual Evaluation Plan
RACI	**R**	EB
	A	EB
	C	-
	I	Applicant
Actions		1. The EB should conduct an on-site assessment in accordance with the annual evaluation plan and send the Documents Required List to the applicant prior to the on-site visit.
		2. The Applicant should prepare development lifecycle supporting materials for the audited product/service based on the Documents Required List.
		3. The EB should generate the annual evaluation report based on the evidence.

	4. The EB should communicate the nonconformity issues with the applicant if there is any.	
Output List	**Entity**	**Output**
	EB	Annual Evaluation Report
Output Description	**Annual Evaluation Reports** The content of the annual evaluation report should be based on its specific evaluation scope, which can be referred to the description of the audit report in ***I.1.3*** or the evaluation report in ***I.1.7***.	

I.2.5 Review and admit validity of certificates for current year			
Input List		Annual Evaluation Report	
RACI	**R**	CB	
	A	CB	
	C	EB	
	I	Applicant	
Actions		1.The CB should review the annual evaluation report. If there is any doubt or uncertainty, the CB should communicate and reach consensus with the EB.	
		2. The CB should decide and inform public of the validity of certificates for the current year.	
Output List		**Entity**	**Output**
		CB	Notification of Annual Evaluation Conclusion
Output Description		**Notification of Annual Evaluation Conclusion** The notification should indicate the results of the annual evaluation and the continued validity of the certificate.	

4.2.2 Re-Evaluation (The original certificate is nearing expiry or has expired)

I.2.6 Apply for Re-evaluation of the certificate			
Input List		Audit Reports	
		Evaluation Reports	
RACI	**R**	Applicant	
	A	Applicant	
	C	-	
	I	EB	
Actions		1.The Applicant should sign the conformance claims to prove that the development and lifecycle of the re-assessed product/service conform to the requirements of cybersecurity standards.	
		2.The Applicant should submit the re-certification application, conformance claims, former audit, and evaluation reports to the EB for re-evaluation.	
Output List		**Entity**	**Output**
		Applicant	Re-certification Application
		Applicant	Conformance Claim

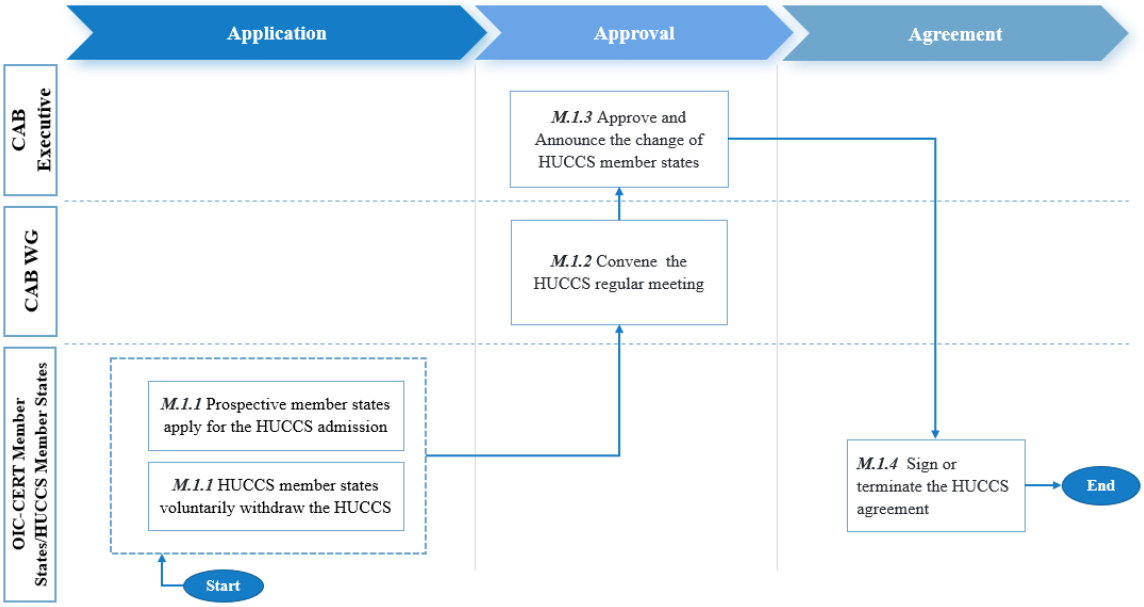
Output Description	**Re-certification Application** The materials needed for the initial certification should at least be provided in the re-certification application, together with all audit and evaluations reports from the initial certification's validity period. **Conformance Claim** This claim should prove that the development and lifecycle of the evaluated product/service conform to the security requirements defined in the cybersecurity standard.

5 Maintenance of the HUCCS

The maintenance of HUCCS is introduced in this chapter in three scenarios. Each scenario has a corresponding flowchart and each step in the flowchart is described in detail in the form of R.A.C.I matrix table.

5.1 Change of HUCCS Member states

The following flowchart shows the processes for changing of HUCCS member states. There are approvals and announcements for admission and withdrawal of HUCCS member states in the HUCCS regular meeting. The details of the process are expanded in the following R.A.C.I matrix tables.



5.1.1 Application

M.1.1 Prospective member states apply for the HUCCS admission			
Input List		The Process of Membership Admission and Withdrawal	
RACI	**R**	OIC-CERT member states	
	A	OIC-CERT member states	
	C	-	
	I	CAB WG	
Actions		1. According to the process of membership admission and withdrawal, OIC-CERT member states that volunteer to join the HUCCS should complete an application for admission and submit it to the CAB WG.	
Output List		**Entity**	**Outputs**
		OIC-CERT member states	Application for HUCCS Admission

Output Description	**Application for HUCCS Admission** a) The application should contain the following contents: An application for HUCCS admission, including the name of the member state, the application date, contact department or representative personnel, etc. b) A commitment to voluntarily recognize and promote the HUCCS, comply with the HUCCS policies and operation specifications, and introduce and recommend domestically the selected cybersecurity standard, evaluation methodology evaluation criteria, and assurance level. c) A commitment to voluntarily sign the HUCCS Agreement and Information Confidentiality and Disclosure Rules.

M.1.1 HUCCS member states voluntarily withdraw from HUCCS			
Input List		The Process of Membership Admission and Withdrawal	
RACI	**R**	HUCCS member states	
	A	HUCCS member states	
	C	-	
	I	CAB WG	
Actions		1. According to the process of membership admission and withdrawal, HUCCS member states could complete an application to withdraw and submit it to the CAB WG.	
Output List		**Entity**	**Outputs**
		HUCCS member states	Application for the HUCCS Withdrawal
Output Description		**Application for the HUCCS Withdrawal** a) The application should contain the following contents: An application for the HUCCS voluntary withdrawal, including the name of the member state, the application date, contact department or representative personnel, etc. b) A commitment to voluntarily terminate the HUCCS agreement and agree to accept the consequences of termination. c) A commitment to continue confidentiality obligations under the signed Information Confidentiality and Disclosure Rules.	

5.1.2 Approval

M.1.2 Convene HUCCS regular meeting	
Input List	The Process of Membership Admission and Withdrawal
RACI **R**	CAB WG
A	CAB WG
C	-
I	OIC-CERT member states, HUCCS member states, CAB Executive
Actions	1.The CAB WG should submit the collected application for the change of HUCCS member states to the CAB Executive.
	2. The CAB WG should convene HUCCS regular meeting and inform the CAB Executive, prospective member states or the HUCCS member states to participate in the meeting.
	3. The CAB WG should record the topics for discussion and conclusions in the meeting minutes.

Output List	Entity	Outputs
	CAB WG	Meeting Minutes
Output Description	**Meeting Minutes** Each participant must sign the meeting minutes, which must be sent to each participant after the meeting, to document the process of membership admission and withdrawal. The minutes must also include the meeting time, location, participants, opinions of the parties, and statement of the conclusions.	

M.1.3 Approve and announce the change of HUCCS member states			
Input List		The Process of Membership Admission and Withdrawal	
RACI	**R**	CAB Executive, CAB WG	
	A	CAB Executive	
	C	-	
	I	HUCCS member states, OIC-CERT member states	
Actions		1. If the application is complete and not procedurally flawed, the CAB Executive should issue approvals of the changes for the HUCCS member states.	
		2. The CAB WG should update and release the revised HUCCS agreement on behalf of the CAB Executive and send it to OIC-CERT member states.	
Output List		**Entity**	**Outputs**
		CAB Executive	Approval for the Change of the HUCCS member states
		CAB WG	Revised HUCCS Agreement
Output Description		**Approval for the Change of HUCCS Member States** The CAB Executive should give written approval for the change of the HUCCS member states and release the written approval through official channels.	

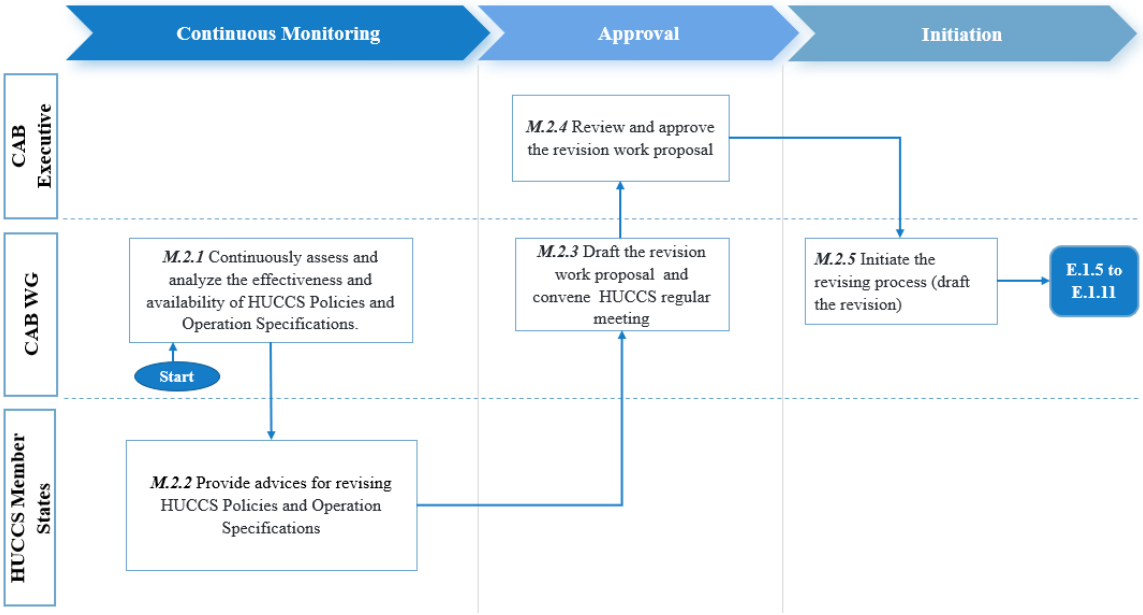
5.1.3 Agreement

M.1.4 Sign or terminate the HUCCS agreement			
Input List		Revised HUCCS Agreement	
RACI	**R**	OIC-CERT member states, HUCCS member states	
	A	CAB WG	
	C	-	
	I	CAB Executive	
Actions for Signing		1. OIC-CERT member states should review the revised HUCCS agreement.	
		2. OIC-CERT member states should submit a written statement by the designated representative that the member state has formally acceded to HUCCS.	
Actions for Termination		1. HUCCS member states should submit a written statement by the designated representative that the member state will continue to comply with the commitments made on the application form in ***M.1.1*** after withdrawal.	
Output List		**Entity**	**Outputs**

	OIC-CERT member states	Statement of Admission
	HUCCS member states	Statement of Withdraw
	CAB WG	Records of membership admission and withdrawal
Output Description	**Statement of Admission/Withdraw** The statement is issued by the OIC-CERT member state or HUCCS member states to demonstrate that they confirm their willingness to accede or withdraw and their commitment to obey the rules applicable to them under the HUCCS. **Records of Membership Admission and Withdrawal** According to the signing and termination of the HUCCS agreement, CAB WG should file records of membership admission and withdrawal.	

5.2 Revising HUCCS Policies and Operation Specifications

The following flowchart shows the processes for revising HUCCS policies and operation specifications. The details of the process are expanded in the following R.A.C.I matrix tables.



5.2.1 Continuous Monitoring

M.2.1 Continuously assess and analyze the effectiveness and availability of HUCCS Policies and Operation Specifications		
Input List		The Assessment and Analysis Specifications for Maintenance of the HUCCS
RACI	**R**	CAB WG
	A	CAB WG
	C	CAB Executive, CB, EB, HUCCS member states
	I	-

Actions	1. Based on the Assessment and Analysis Specifications for Maintenance of the HUCCS, CAB WG should continuously monitor the operation of the HUCCS by reviewing filings on record and collecting feedback from CAB Executive, CB, EB, and HUCCS member states.	
	2. CAB WG is recommended to generate the annual assessment report for HUCCS operation, which summarizes the HUCCS performance and points out the essential optimization for effective HUCCS Policies and Operation Specifications.	
Output List	**Entity**	**Outputs**
	CAB WG	Annual Assessment Report for HUCCS Operation
Output Description	**Annual Assessment Report for HUCCS Operation** The CAB WG should evaluate annual work including the performance of HUCCS and continuously collect feedback from HUCCS member states, CB, and EB and produce an annual report that should focus on the risks and issues of HUCCS and assess the effectiveness and applicability of the HUCCS Policies and Operation Specifications.	

M.2.2 Provide advice for revising HUCCS Policies and Operation Specifications		
Input List		-
RACI	**R**	HUCCS member states
	A	CAB WG
	C	-
	I	-
Actions		1. HUCCS member states should provide written advice for revising HUCCS Policies and Operation Specifications
Output List	**Entity**	**Outputs**
	HUCCS member states	Written Advice
Output Description	**Written Advice** Written Advice should be a clear opinion and provide adequate support for the opinion. It may include: a) Involved Document. b) Involved Article. c) Revising advice. d) Reason or justification for revising.	

5.2.2 Approval

M.2.3 Draft the revision work proposal and convene HUCCS regular meeting		
Input List		Written Advice
RACI	**R**	CAB WG
	A	CAB WG
	C	HUCCS member states
	I	-

Actions	1.The CAB WG should generate the revision work proposal for HUCCS polices and operation specifications according to collected advice.	
	2. The CAB WG should discuss with the HUCCS member states whether the advice is accepted, whether it has been reacted to the proposal, the way of revising, and eventually reach a consensus.	
Output List	**Entity**	**Output**
	CAB WG	The Revision Work Proposal
Output Description	**The Revision Work Proposal** The revision work proposal is recommended to take account of HUCCS annual reports and advice from HUCCS member states. The revision work proposal shall contain the following contents: a) The list of HUCCS policies and operation specifications to continue to be valid, to be abolished, or to be revised. b) The background, necessity, and objective of revising. c) Main components to be revised. d) Person in charge of this work. e) Budget. f) Work plan. g) Reference.	

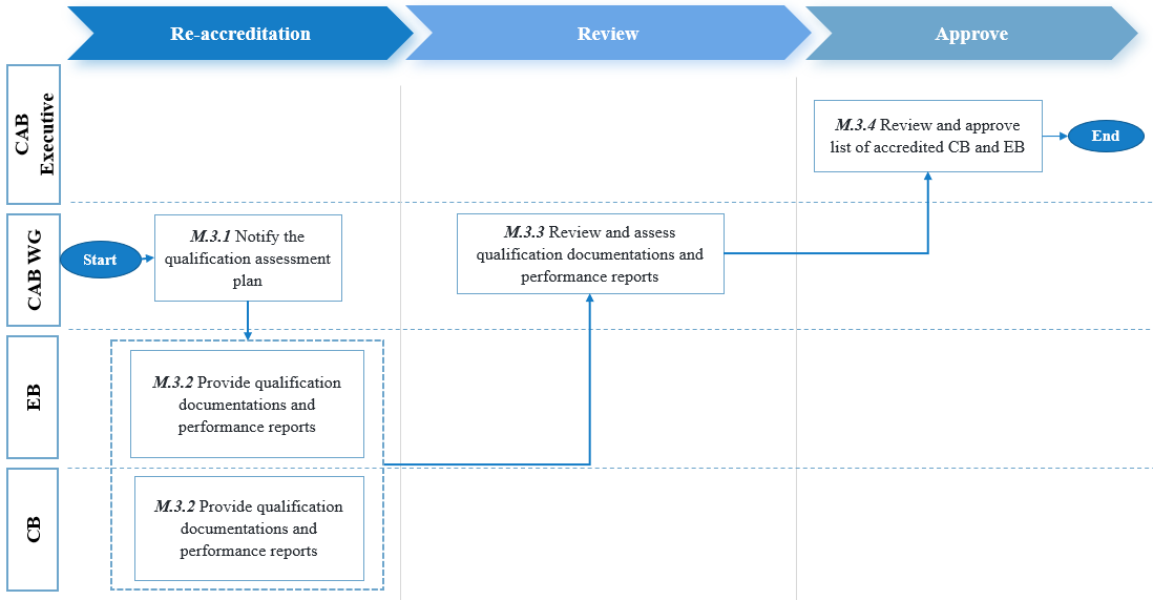
M.2.4 Review and approve the revision work proposal			
Input List		The Revision Work Proposal	
RACI	**R**	CAB Executive	
	A	CAB Executive	
	C	-	
	I	-	
Actions		1. The CAB Executive should review the Revision Work Proposal submitted by CAB WG.	
		2. The CAB Executive should evaluate and vote on the Revision Work Proposal to decide whether to pass it or not.	
		3. The CAB Executive should record and inform the CAB WG of the result of voting and opinions.	
Output List		**Entity**	**Output**
		CAB Executive	Approval of the Revision Work Proposal
Output Description		**Approval of the Revision Work Proposal** The CAB Executive should assess, vote, and conduct their conclusions for the Revision Work Proposal at the HUCCS regular meeting. There are two types of conclusions: approval and disapproval. In the case of disapproval, it is required to provide specific stated reasons. Before making the decision, CAB Executive is suggested to assess the applicability of the HUCCS polices and operation specifications in the HUCCS annual report, the necessity and impact of revising, and the consistency of the revised items and directions with the overall objective.	

5.2.3 Initiation

M.2.5 Initiate the revising process (draft the revision)			
Input List		Approval of the Revising Work Proposal	
RACI	**R**	CAB WG	
	A	CAB WG	
	C	-	
	I	-	
Actions		1. CAB WG should initiate the revising process according to E.1.5 to E.1.11.	
Output List		**Entity**	**Outputs**
		-	N/A
Output Description		**N/A**	

5.3 Periodic Qualification Assessment of CB and EB

The following flowchart shows the process of periodic qualification assessment for CB and EB. The details of the process are expanded in the following R.A.C.I matrix tables.



5.3.1 Re-accreditation

M.3.1 Notify the qualification assessment plan		
Input List		Standards of Qualification and Performance of CB and EB
		Released Accredited CB and EB List
RACI	**R**	CAB WG
	A	CAB WG
	C	-
	I	CB, EB

Actions	1. CAB WG should maintain a qualification assessment plan for accredited CB and EB on an annual basis.	
	2. CAB WG should inform the qualification assessment plan to accredited CB and EB and the qualification documentation should be prepared.	
Output List	**Entity**	**Output**
	CAB WG	Qualification Assessment Plan
	CAB WG	Notice on Annual Qualification Assessment
Output Description	**Qualification Assessment plan** The drafting of the plan should be based on the requirements in Standards of Qualification and Performance of CB and EB, and should include the assessment target, process, plan, and scopes. The plan should update annually to meet current management objectives and requirements for CB and EB. **Notice on Annual Qualification Assessment** The notification should contain the recipient, the proposed assessment timing, and the supporting materials to be prepared.	

M.3.2 Provide qualification documentations and performance reports		
Input List		Notice on Annual Qualification Assessment
RACI	**R**	CB and EB
	A	CB and EB
	C	CAB WG
	I	-
Actions	1. CB and EB should evaluate internally whether they meet the requirements of maintaining on assurance level.	
	2. CB and EB should review achievements of the certification or auditing efforts over the past year and write a performance report.	
	3. CB and EB should prepare documents that demonstrate their qualifications.	
	4. CB and EB should submit their qualification documentation to CAB WG.	
Output List	**Entity**	**Output**
	CB	Qualification Documentations
	CB	Performance Reports
	EB	Qualification Documentations
	EB	Performance Reports
Output Description	**Qualification Documentations** Qualification documentations should satisfy all requirements listed in M.3.1 and be prepared according to the requirements specified in notice on annual qualification assessment. The content of the document must be accurate and comprehensive. **Performance Reports** The performance report should include the number, type, and pass rate of certifications or audits conducted in the past year, as well as other performance assessment matters defined in Standards of Qualification and Performance of CB and EB.	

5.3.2 Review

M.3.3 Review and assess qualification documentations and performance reports			
Input List		Qualification Documentations	
RACI	**R**	CAB WG	
	A	CAB WG	
	C	-	
	I	CB and EB	
Actions		1. CAB WG should review the Qualification Documentations and check for completeness.	
		2. CAB WG should verify the accuracy of Qualification Documentations submitted by the CB and EB through interviews, visits, inspections etc., and identify whether the documentations can fulfill the requirements.	
		3. CAB WG should review the submitted performance reports to assess whether CB or EB can continue to support certification or auditing.	
		4. CAB WG should renew a list of CB and EB that continue to be accredited in the next year for CAB Executive to review.	
Output List		**Entity**	**Output**
		CAB WG	Accredited CB and EB List Draft
Output Description		**Accredited CB and EB List Draft** The considerations and content of this list should be consistent with the CB and EB List in ***E.3.3***.	

5.3.3 Approve

M.3.4 Review and approve the List of accredited CB and EB			
Input List		Accredited CB and EB List Draft	
RACI	**R**	CAB Executive	
	A	CAB Executive	
	C	CAB WG	
	I	CB and EB	
Actions		1. CAB Executive should review and approve the Accredited CB and EB List Draft, including qualifications, past performance, and compliance with the CAB WG assessment of CB and EB.	
		2. CAB WG should re-issue accreditation letters to CB and EB on the list.	
Output List		**Entity**	**Output**
		CAB Executive	Official Accredited CB and EB List
		CAB WG	Accreditation Letter

Output Description	**Official Accredited CB and EB List** The considerations and content of this list should be consistent with List of CB and EBs in ***E.3.4***. **Accreditation Letter** The considerations and content of this letter should be consistent with the Accreditation Letter in ***E.3.4***.

Appendix I

Appendix I is a summarized table of documents produced by the different roles in different actions.

Role	Phase	Action No.	Output
CAB Executive	Establishment Part 1	E.1.4	Meeting Minutes and Opinions
		E.1.6	Meeting Minutes and Opinions
		E.1.8	Meeting Minutes
		E1.10	HUCCS Policies Final Version for Release
			Operation Specifications Final Version for Release
	Establishment Part 2	E.2.5	Meeting Minutes and Opinions
	Establishment Part 3	E.3.4	Accredited CB and EB List
		E.3.5	Released Accredited CB and EB List
	Maintenance Part 1	M.1.3	Approval for the change of HUCCS member states
	Maintenance Part 2	M.2.4	Approval of the Revision Work Proposal
	Maintenance Part 3	M.3.4	Official Accredited CB and EB List

Role	Phase	Action No.	Output
CAB WG	Establishment Part 1	E.1.1	First Draft of Work Proposal
		E.1.3	Response to Comments and Revised Records
			Final Draft of Work Proposal
		E.1.5	Explanation of Compilation
			Meeting Minutes
			HUCCS Policies
			HUCCS Operation Specifications

Role	Phase	Action No.	Output
		E.1.7	Revised HUCCS Policies
			Revised HUCCS Operation Specifications
			Submitted Explanation of Compilation
		E1.9	Finalized HUCCS Policies
			Finalized HUCCS Operation Specifications
			Filing Record
	Establishment Part 2	E.2.1	List of Alternative Cybersecurity Standards
		E.2.2	Drafted Proposal of Recommended Cybersecurity Standards
		E.2.4	Response to Comments and Revised Records
			Finalized Proposal of Recommended Cybersecurity Standards
		E.2.6	Released Version of the HUCCS Agreement
	Establishment Part 3	E.3.1	Recruitment Announcement
		E.3.3	CB and EB Candidate List
		E.3.4	Accreditation Letter
	Establishment Part 4	E.4.4	Review Result
		E.4.5	Newly Accredited CB and EB List
	Implementation Part 1	I.1.11	Filing Record
	Maintenance Part 1	M.1.2	Meeting Minutes
		M.1.3	Revised HUCCS Agreement
		M.1.4	Records of Membership Admission and Withdrawal
		M.2.1	Annual Assessment Report for HUCCS Operation

Role	Phase	Action No.	Output
	Maintenance Part 2	M.2.3	The Revision Work Proposal
	Maintenance Part 3	M.3.1	Qualification Assessment Plan
			Notice on Annual Qualification Assessment
		M.3.3	Accredited CB and EB List Draft
		M.3.4	Accreditation Letter

Role	Phase	Action No.	Output
OIC-CERT member states	Establishment Part 1	E.1.1	Feedback of Certification Demands
		E.1.2	Comments on Work Proposal
	Establishment Part 1	E.2.3	Feedback Comments
		E.2.6	Signed Feedback
	Maintenance Part 1	M.1.1	Application for HUCCS Admission
		M.1.4	Statement of Admission

Role	Phase	Action No.	Output
HUCCS member states	Maintenance Part 1	M.1.1	Application for the HUCCS Withdrawal
		M.1.4	Statement of Withdraw
	Maintenance Part 2	M.2.2	Written Advice

Role	Phase	Action No.	Output
CB	Establishment Part 1	E.3.2	Qualification Documentations
		E.4.2	Security and Technical Evaluation Plan

Role	Phase	Action No.	Output
	Establishment Part 4	E.4.3	Security and Technical Evaluation Records
			Security and Technical Evaluation Report
	Implementation Part 1	I.1.10	Certificate Report
	Implementation Part 2	I.2.1	Annual Evaluation Notice
		I.2.5	Notification of Annual Evaluation Conclusion
	Maintenance Part 3	M.3.2	Qualification Documentations
			Performance Reports

Role	Phase	Action No.	Output
EB	Establishment Part 3	E.3.2	Qualification Documentations
	Establishment Part 4	E.4.1	Application Materials
	Implementation Part 1	I.1.2	Audit Plan
		I.1.3	Documents Required List
			Draft Audit Report
			List of Nonconformity Issues
		I.1.5	Audit Report
		I.1.7	Draft Evaluation Report
			List of Nonconformity Issues
		I.1.9	Evaluation Report
	Implementation Part 2	I.2.3	Annual Evaluation Plan
		I.2.4	Annual Evaluation Report
		M.3.2	Qualification Documentations

Role	Phase	Action No.	Output
	Maintenance Part 3		Performance Reports

Role	Phase	Action No.	Output
Applicant	Implementation Part 1	I.1.1	Self-evaluation Report
			Conformance Claim
		I.1.4	Rectification Records
		I.1.5	Compliance Declaration
		I.1.8	Rectification Records
	Implementation Part 2	I.2.6	Re-certification Application
			Conformance Claim

Appendix II

Appendix II lists all documents under the level 3 of the documentary system.

Level 3	Output
Certificate basis and records	Meeting Minutes and Opinions
	Accredited CB and EB List
	Released Accredited CB and EB List
	Approval for the change of HUCCS member states
	Approval of the Revision Work Proposal
	Official Accredited CB and EB List
	First Draft of Work Proposal
	Response to Comments and Revised Records
	Final Draft of Work Proposal
	Explanation of Compilation
	Submitted Explanation of Compilation
	List of Alternative Cybersecurity Standards
	Drafted Proposal of Recommended Cybersecurity Standards
	Finalized Proposal of Recommended Cybersecurity Standards
	Released Version of the HUCCS Agreement
	Recruitment Announcement
	CB and EB Candidate List
	Accreditation Letter
	Review Result
	Newly Accredited CB and EB List
	Filing Record
	Revised HUCCS Agreement
	Records of Membership Admission and Withdrawal
	Annual Assessment Report for HUCCS Operation
	The Revision Work Proposal

	Qualification Assessment Plan
	Notice on Annual Qualification Assessment
	Accredited CB and EB List Draft
	Feedback of Certification Demands
	Comments on Work Proposal
	Feedback Comments
	Signed Feedback
	Application for HUCCS Admission
	Statement of Admission
	Application for the HUCCS Withdrawal
	Statement of Withdraw
	Written Advice
	Security and Technical Evaluation Plan
	Security and Technical Evaluation Records
	Security and Technical Evaluation Report
	Certificate Report
	Annual Evaluation Notice
	Notification of Annual Evaluation Conclusion
	Application Materials
	Audit Plan
	Documents Required List
	Draft Audit Report
	List of Nonconformity Issues
	Audit Report
	Draft Evaluation Report
	Evaluation Report
	Annual Evaluation Plan
	Annual Evaluation Report
	Qualification Documentations

	Performance Reports
	Self-evaluation Report
	Rectification Records
	Compliance Declaration
	Re-certification Application
	Conformance Claim