NCIIPC – QCI Initiative

CONFORMITY ASSESSMENT FRAMEWORK FOR CYBER SECURITY OF CRITICAL SECTOR ENTITIES (CAF_CS_CSE)

Issue No. 1 | Feb 2024

Accreditation Scheme for IT and ICS Cyber Security Consultancy Organisations (COs)

DISCLAIMER

This Scheme is in line with the globally accepted industry/ official best practices wherein due attribution has been given to the owner for their respective content/ transcript/ excerpts/ reproduction over which no ownership is claimed by QCI as mandated by the terms of usage so declared by the said owner.

QCI merely insists for mandatory compliance of additional guidelines/standards so as to be eligible for QCI approval. The Conformity Assessment Bodies, Consultancy Organisations, Training Bodies, Critical Sector Entities and other users shall ensure that they possess a rightful copy of the applicable standard(s) and ensure that no infringement of copyright or commercial loss occurs to the originators/owners of referred standards.

All rights and credit go directly to their rightful owners. No copyright infringement intended.

PREFACE

Cyberspace has become a game-changer in the digital age and has impacted every facet of human life. There are severe threats that may cause systemic harm to entities and organisations in 'critical sectors' of the nation, further impacting national security, economy, public health and safety.

There is a need to strengthen the cyber security aspects of Critical Sector Entities (CSEs) to prevent the impact due to exploitation of any vulnerabilities and build cyber resilience in their delivery of critical functions of the nation like power generation, transmission & distribution, banking, financial services and insurance, telecommunication, government services under Digital India mission, transportation, health, and strategic capabilities.

CSEs need to protect their Critical Information Infrastructure (CII) comprising of various computer systems, networks, applications and data, the incapacitation or destruction of which shall have a debilitating impact on national security, economy, public health or safety.

National Critical Information Infrastructure Protection Centre (NCIIPC), a unit of the National Technical Research Organisation (NTRO), is a government organisation created under Section 70A of the Information Technology Act, 2000 (amended 2008), through gazette notification dated 16 Jan 2014. NCIIPC has been designated as the national nodal agency for the protection of CII.

The **Quality Council of India (QCI)** has developed a **Conformity Assessment Framework (CAF) for the Cyber Security of Critical Sector Entities**, with NCIIPC as the Scheme Owner (SO) and QCI as the National Accreditation Body & Scheme Manager to manage the scheme on behalf of NCIIPC. The CAF for the cybersecurity of CSEs comprises of the following Schemes:

- Certification Scheme for Cyber Security Management System (CSMS)
- Inspection Scheme for Information Technology and Industrial Control Systems (IT/ICS)
- Personnel Certification Scheme for Cyber Security Professionals
- Accreditation Scheme for IT/ICS Consultancy Organisations (COs)
- Accreditation Scheme for IT/ICS Training Bodies (TBs)

QCI has developed the CAF through multi-stakeholder consultation that has considered the national legal and regulatory mandates to create a robust, cyber security ecosystem at the national level. The CAF has been designed in a manner by which CSEs can adequately address the three pillars i.e. processes, people, and technology within their organisations.

This Scheme document details the requirements for accreditation of IT and ICS Cyber Security Consultancy Organisations herein after referred to as COs.

ACKNOWLEDGEMENT

Quality Council of India (QCI) would like to thank NCIIPC for entrusting us with the responsibility of creating a conformity assessment framework to secure the cyber security ecosystem across the critical sector entities in India.

We extend our sincere thanks to Shri Navin Kumar Singh, DG, NCIIPC, for entrusting us with the opportunity to collaborate on fortifying the cybersecurity ecosystem. We would also express our gratitude to Shri Lokesh Garg (DDG), NCIIPC and Col. K. Pradeep Bhat (Retd.) (Consultant), NCIIPC for their contribution to the finalisation of the documents. Special mention is due to Gp. Capt. (Dr.) R. K. Singh, (Director), NCIIPC for his apt steering of the project by building consensus among various stakeholders.

We express our gratitude to our Chairman, Shri Jaxay Shah for his constant encouragement and support. We extend our sincere thanks to our Secretary General, Shri Rajesh Maheshwari, for entrusting us with the project and for his continuous guidance during the course of the project.

We register our appreciation to the Chair(s) of the Steering Committee, Technical Committee and Certification Committee for granting approvals on the technical and conformity assessmentdocuments which have been instrumental in shaping the structure of the Scheme. We would like to acknowledge with much appreciation the technical inputs of Shri U. K. Nandwani, former DG, STQC, and Shri Manoj Belgaonkar, industry expert.

The efforts of Shri Shivesh Sharma, Accreditation Officer at PADD, in terms of his dedication, commitment and hard work is duly recognised. The document was made possible through the efforts of the team comprising of Ms. Arushi Lohani and Ms. Vaishaly Jain for their editorial inputs.

Dr. Manish Pande
Director and Head
PADD, QCI

Contributors

1. Steering Committee

S.No.	Name	Organisation
Chair		
1	Dr. Gulshan Rai	Former National Cyber Security Coordinator
Members		
2	Sh. Hemant Jain	Central Electricity Authority
3	Sh. Navin Kumar Singh	National Critical Information Infrastructure Protection Centre
4	Sh. Sridhar Vembu	National Security Advisory Board
5	Mr. G. Narendra Nath	National Security Council Secretariat

2. Technical Committee

S.No.	Name	Organisation
Chair		
1	Sh. M.A.K.P. Singh	Central Electricity Authority
Members		
2	Sh. A. K. Patel	NTPC Limited
3	Sh. A. R. Vinukumar	Centre for Development of Advanced Computing
4	Sh. Ajay Bagati	Bharat Heavy Electricals Ltd.
5	Maj. Gen. Amarjit Singh (Retd.)	Persistent System Ltd.
6	Sh. Anand Shankar	Power Grid Corporation of India
7	Sh. Anand Deep Gupta	National Accreditation Board for Certification Bodies
8	Sh. Ashutosh Bahuguna	Indian Computer Emergency Response Team
9	Prof. Faruk Kazi	Veermata Jijabai Technological Institute
10	Sh. Praveen Kumar Goyal	Noida Power Company Limited
11	Sh. Ranvijay Bihari	National Accreditation Board for Education and Training
12	Ms. Reena Garg	Bureau of Indian Standards
13	Prof. Sandeep Shukla	IIT-Kanpur
14	Ms. Seema Mittal	National Critical Information Infrastructure Protection Centre
15	Sh. Shaleen Khetarpaul	BSES Rajdhani Ltd.
16	Sh. Sivakumar V	Central Power Research Institute
17	Sh. Sushil Kumar Nehra	Ministry of Electronics and Information Technology
18	Sh. Vasant Prabhu/ Sh. Aamir Hussain	Tata Power – DDL
19	Sh. Vinayak Godse	Data Security Council of India

3. Certification Committee

S No.	Name	Organisation
Chair		
1	Dr. N. Rajesh Pillai	Defence Research and Development Organisation
Members		
2	Sh. Ajay Bagati	Bharat Heavy Electricals Ltd.
3	Sh. Anand Deep Gupta	National Accreditation Board for Certification Bodies
4	Mr. Atul Gupta	Standardisation Testing and Quality Certification
5	Sh. A. K. Patel	NTPC Limited
6	Col. Debashish Bose	National Security Council Secretariat
7	Sh. Harry Dhaul	Independent Power Producers Association of India
8	Dr. Manju Mam	National Power Training Institute
9	Sh. Manoj Belgaonkar	SIEMENS Limited.
10	Sh. Ranvijay Bihari	National Accreditation Board for Education and Training
11	Sh. Reji Pillai	India Smart Grid Forum
12	Sh. Samir Matondkar	Larsen & Toubro Limited
13	Sh. Sandeep Puri	NHPC Limited.
14	Ms. Seema Shukla	TIC Council
15	Sh. Sundeep Kumar	Bureau of Indian Standards

SECTION 1

INTRODUCTION

1. Background

1.1. Critical Sector Entities (CSEs) require IT/ICS Cyber Security Consultancy Organisations (COs) with varied competencies to assess an organization's computer systems, network, and software for vulnerabilities and to design and implement the best security solutions as per the needs of organization. Also, COs are required to provide their assistance and support during the 'preparatory phase' of various certification processes.

1.2. 'Consultancy' is the act of providing technical expertise, by an individual or an organisation deemed competent in delivering services as per the defined scope in exchange for a fee. The nature of such expertise may be technical, thematical, procedural or managerial.

1.3. There is an emergent need to put in place a system of oversight and due diligence so that only bonafide and competent COs are engaging with the clients, ensuring quality with compliance. This is proposed to be achieved by well-defining the compliance requirements of COs in order to grant them accreditation.

1.4. Through this initiative, it shall help build capacities and strengthen the CSEs through the engagement process of accredited COs, having undergone proper assessment of their competence(ies). CSEs can engage with COs either through contractual agreements for full assignments or by deploying a team of professionals to provide on-site support to clients throughout the identified process lifecycle.

1.5. The designed accreditation Scheme involved establishment of the scope of the COs, identification of the accreditation criteria, and determining the evaluation methods of the COs both in terms of Quality Management Systems/Managed Consultancy Services and the capability of employed human resources.

1.6. This document introduces a framework that assists CSEs in establishing a cyber-resilient system while maintaining acceptable system performance, cost and reliability.

2. Objective

2.1 The objective of this document is to inform about the requirements for accreditation of COs.

2.2 To institute a uniform process while providing consultancy through a structured process across sectors that will ensure that the CSEs are protected.

2.3 To provide working frameworks to the COs for systemizing their workflows by defining tenets of consultancy, especially in reference to the application of cybersecurity in different domains as per the requisitions made by the CSEs.

2.4 To ensure the compatibility and interoperability of the Scheme with regards to the other pre-existing schemes of the same framework (e.g., PrCB, TB, CSMS, etc.)

3. Scope

The scope of this document covers various procedures and processes required to operate the Scheme such as governance, accreditation criteria, accreditation process, rules for use of Scheme Mark.

4. Structure of the document

The Scheme is divided into five sections:

Section 1: Introduction
Section 2: Governing Structure
Section 3: Accreditation Criteria
Section 4: Accreditation Process
Section 5: Rules for use of Scheme Mark

5. Glossary

The definitions in this document are for reference purposes and are to be read in line with the definitions notified in IS/ISO/IEC/IEC 27000 and IEC 62443, its family of standards. In case of any differences in terminology the definitions in the IT Act 2000 [As Amended by Information Technology (Amendment) Act 2008] shall prevail.

5.1 **Accreditation** - Third-party attestation related to a conformity assessment body conveying formal demonstration of its competence to carry out specific conformity assessment tasks.

5.2 **Accreditation Body** - Authoritative body that performs accreditation. The authority of an accreditation body can be derived from government, public authorities, contracts, market acceptance or Scheme owners.

5.3 **Applicant for Personnel Certification** - Person who has submitted an application to be admitted into the certification process.

5.4 **Approval** - Permission for a product or process to be marketed or used for stated purposes or under stated conditions. Approval can be based on fulfilment of specified requirements or completion of specified procedures.

5.5 **Asset** - Anything that has value to an individual, an organisation or a government.

5.6 **Asset Owner** - Individual or company responsible for one or more assets.

5.7 **Assessment** - Process that evaluates a person's fulfilment of the requirements of the Certification Scheme

5.8 **Attest** - The process that confirms the conformance of the entity and individual certified, inspected, accredited or approved.

5.9 **Attestation** - Issue of a statement, based on a decision following review, that fulfilment of specified requirements has been demonstrated. The resulting statement, referred to in this Standard as a “statement of conformity”, conveys the assurance that the specified requirements have been fulfilled. Such an assurance does not, of itself, afford contractual or other legal guarantees. First-party and third-party attestation activities are distinguished by the terms. For second-party attestation, no special term is available.

5.10 **Candidate for Personnel Certification** - Applicant who has fulfilled specified prerequisites and has been admitted to the certification process.

5.11 **Certificate** - Document issued by a certification body under the provisions of this Standard, indicating that the named person has fulfilled the certification requirements.

5.12 **Certification** - Third-party attestation related to products, processes, systems or persons. Certification of a management system is sometimes also called registration. Certification is applicable to all objects of conformity assessment except for conformity assessment bodies themselves, to which accreditation is applicable.

5.13 **Certification Requirements** - Set of specified requirements, including requirements of the Scheme to be fulfilled in order to establish or maintain certification.

5.14 **Certification Scheme** - Competence and other requirements related to specificoccupational or skilled categories of persons.

5.15 **Certified person** – A person who holds a certificate.

5.16 **Competence** - Ability to apply knowledge and skills to achieve intended results.

5.17 **Complaint** - Expression of dissatisfaction, other than appeal, by any person or organisation to a conformity assessment body or accreditation body, relating to the activities of that body,

where a response is expected.

5.18 **Conformity Assessment** - Demonstration that specified requirements are fulfilled. Conformity assessment includes activities defined elsewhere in this document, such as but not limited to testing, inspection, validation, verification, certification, accreditation.

5.19 **Conformity Assessment Body** - Body that performs conformity assessment activities, excluding accreditation.

5.20 **Conformity Assessment Framework** - Structure of processes and specifications, related to conformity assessment system, designed to support the accomplishment of a specific task. There are various conformity assessment schemes that can be used to determine whether specified requirements are fulfilled, they include but are not limited to inspection, evaluation, audit of management system etc. In a framework, these conformity assessmentschemes / system share common vocabulary, principles and family of standards which ensure interoperability of various schemes.

5.21 **Conformity Assessment System** - Set of rules and procedures for the management of similar or related conformity assessment schemes. A conformity assessment system can be operated at an international, regional, national, sub-national, or industry sector level.

5.22 **Conformity Assessment Scheme** - Set of rules and procedures that describes the objects of conformity assessment identifies the specified requirements and provides themethodology for performing conformity assessment. A scheme can be managed within a conformity assessment system. A scheme can be operated at an international, regional, national, sub-national, or industry sector level. A scheme can cover all or part of the conformity assessment functions.

5.23 **Critical** - An important device, computer system, process, and alike elements, if compromised by an incident, could have high financial, health, safety or environment impact an organisation (or entity).

5.24 **Critical Information Infrastructure (CII)** - It means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.

5.25 **Critical Sector Entity (CSE)** - The critical sector entities are utilities having assets, systems, and networks, whether physical or virtual, that are considered so vital that their incapacitation or destruction would have a debilitating impact on national security, economy, public health or public safety, or any combination.

5.26 **Cyber Crisis Management Plan** - Outlines a framework for dealing with cyber related incidents for a coordinated, multi-disciplinary and broad-based approach for rapid identification, information exchange, swift response and remedial actions to mitigate and recover from malicious cyber related incidents impacting critical processes.

5.27 **Cyber Security Management System (CSMS)** - System designed by an organisation to maintain the cyber security of the entire organisation's assets to an established level of confidentiality, integrity and availability, whether they are on the business side or the technology side of the organisation (or entity).

5.28 **Cyber Security** - Safeguarding people, society, organisations and nations from cyber risks. The objective of adequate cybersecurity is to maintain an acceptable level of stability, continuity and safety of organisations operating in cyberspace. While it is not possible to always achieve these objectives, cybersecurity aims to reduce cyber risks to a tolerable level.

5.29 Areas of concern for cybersecurity include:

5.29.1 Stability and continuity of society, organisations and nations.

5.29.2 Property (including information) of people and organisations; and

5.29.3 Human lives and health.

5.30 **Cyber Security Professional:** An individual who has been certified for the domains as specified in the Scheme.

5.31 **Cyberspace** - Complex environment resulting from the interaction of people, software and

services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form. It also means interconnected digital environment of networks, services, systems, people, processes, organisations, and that which resides on the digital environment or traverses through it.

5.32 **Cyberspace Security** - Preservation of confidentiality, integrity and availability of information in Cyberspace.

5.33 **Cyber safety** - Condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or other types or consequences of failure, damage, error, accidents, harm or any other event in the Cyberspace which could be considered non-desirable. This can take the form of being protected from the event or from exposure to something that causes health or economic losses. It can include protection of people or of assets. Safety in general is also defined asthe state of being certain that adverse effects will not be caused by some agent under defined conditions.

5.34 **Chief Experience Officer** – An executive in the management who ensures positive interactions with an organization's customers.

5.35 **Distributed Control System** - Type of control system in which the system elements are dispersed but operated in a coupled manner. Distributed control systems may have shorter coupling time constants than those typically found in ICS systems. Distributed control systems are commonly associated with continuous processes such as electric power generation, oil and gas refining, chemical, pharmaceutical and paper manufacture, as wellas discrete processes such as automobile and other goods manufacture, packaging, and warehousing.

5.36 **Examination** – Examination is part of the assessment which measures a candidate's competence by one or more means, such as written, oral, practical and observational, as defined in the Certification Scheme.

5.37 **Examiner** - Person competent to conduct and score an examination, where the examination requires professional judgement.

5.38 **Framework** - Structure of processes and specifications designed to support the accomplishment of a specific task.

5.39 **Impartiality** - Objectivity with regard to the outcome of a conformity assessment activity. Objectivity can be understood as freedom from bias or freedom from conflicts of interest.

5.40 **Impartiality for Personnel Certification** - Presence of objectivity fairness equal opportunity for success provided to each candidate in the certification process.

5.41 **Invigilator** - Person authorized by the certification body who administers or supervises an examination but does not evaluate the competence of the candidate.

5.42 **Independence** - Freedom of a person or organisation from the control or authority of another person or organisation. Example: A conformity assessment body can be independent from the person who is the object of conformity assessment or from the organisation providing the object of conformity assessment

5.43 **Industrial Automation and Control Systems (IACS/ICS)** - Collection of personnel, hardware,and software that can affect or influence the safe, secure, and reliable operation of an industrial process.

5.44 **Industrial Control System (ICS)** - General term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures.
An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy) and can affect or influence the safe, secure and reliable operation of an industrial process/Operation.

5.45 **Information Security** - Preservation of confidentiality, integrity and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

5.46 **Information Technology** - Technology (computer systems, networks, software) usedto process, store, acquire and distribute information.

5.47 **Mark Holder**: Entities that are authorized to use the Scheme Mark which include the conformity assessment bodies namely, Certification Bodies, Inspection Bodies, Certification of Personnel and including its client base and, training bodies and consultancy organisation as the specialized professional bodies excluding its client base.

5.48 **Mark owner**: The person or organisation responsible for developing, issuing and managing of the Scheme Mark.

5.49 **Object of Conformity Assessment** - Entity to which specified requirements apply. Example: Product, process, service, system, installation, project, data, design, material, claim, person, body or organisation, or any combination thereof. The term “body” is used in this framework to refer to conformity assessment bodies and accreditation bodies. Theterm “organisation” is used in its general meaning and may include bodies according to thecontext.

5.50 **Off-Product:** Mostly publicity material, pamphlet, letterheads, other similar stationary, media for exchange of any communication are that detecting or causes a change through the direct monitoring and/or control of physical devices and systems, processes and events in the organisation.

5.51 **Personnel** - Individuals, internal or external, of the certification body carrying out activities for the certification body. These include committee members and volunteers.

5.52 **Principles of conformity assessment** - Conformity assessment is a series of three functions that satisfy a need or demand for demonstration that specified requirements are fulfilled:

5.52.1 selection;

5.52.2 determination; and

5.52.3 review and attestation.

Such demonstration can add substance or credibility to claims that specified requirements are fulfilled, giving users greater confidence in such claims. Standards are often used as the specified requirements since they represent a broad consensus of what is wanted in agiven situation. As a result, conformity assessment is often viewed as a standards-related activity.

5.53 **Protected System** - The Appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

5.54 **Qualification** - Demonstrated education, training and work experience, where applicable.

5.55 **Review** - Verification of the suitability, adequacy and effectiveness of selection and determination activities, and the results of these activities, with regard to fulfilment of specified requirements by an object of conformity assessment

5.56 **Scheme Mark**: The Scheme Mark is a protected mark owned by QCI (on behalf of NCIIPC), indicating that the Mark Holder is in conformity with specified requirements of the Scheme. The “Scheme Mark” is also commonly known as a “Logo”, however for the sake of aligningit with the international requirements the same will henceforth be referred to as the “Mark”.The Mark Holder is defined at no. 5.47.

5.57 **Scope of Attestation** - Range or characteristics of objects of conformity assessment covered by attestation.

5.58 **Security Components** - Assets such as firewalls, authentication modules, or encryption software used to improve the security performance of an information technology orindustrial automation and control system.

5.59 **Supervisory Control and Data Acquisition System (SCADA system)** - Type of loosely coupled distributed monitoring and control system commonly associated with electric power transmission and distribution systems, oil and gas pipelines, and water and sewagesystems. These definitions are specific to IT and ICS environment for ICS systems.

5.60 **Stakeholder** - Person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity.

5.61 **Surveillance** - Systematic iteration of conformity assessment activities as a basis for maintaining the validity of the statement of conformity.

5.62 **Suspension** - Temporary invalidation of the statement of conformity for all or part of the specified scope of attestation.

5.63 **Validity** - Evidence that the assessment measures what it is intended to measure, as defined by the Certification Scheme.

5.64 **Vulnerability** - Weakness of an asset or control that can be exploited by a threat.

5.65 **Withdrawal** – Revocation, cancellation of the statement of conformity appeal request by the provider of the object of conformity assessment to the conformity assessment body or accreditation body for reconsideration by that body of a decision it has made relating to that object.

6. Abbreviations

Abbreviation	Acronym
AB	Accreditation Body
AC	Accreditation Committee
ATC	Additional Technical Criteria
BIS	Bureau of Indian Standards
BTC	Basic Technical Criteria
CAB	Conformity Assessment Body
CAF	Conformity Assessment Framework
CB	Certification Body
CC	Certification Committee
CERT-In	Indian Computer Emergency Response Team
CII	Critical Information Infrastructure
CO	Consultancy Organisation
CSA	Cyber Security Agency
CSE	Critical Sector Entity
CSMS	Cyber Security Management System for IT and ICS
CXO	Chief Experience Officer
DA	Desktop Assessment
DCS	Distributed Control System
ENR	Energy
GRC	Governance, Risk and Compliance
IACS	Industrial Automation and Control System
IAF	International Accreditation Forum
IB	Inspection Body
ICS	Industrial Control System
IEC	International Electro technical Commission
IIoT	Industrial Internet of Things
IS	Indian Standards
ISMS	Information Security Management System

Abbreviation	Acronym
ISO	International Organisation for Standardisation
IT	Information Technology
ITAA	Information Technology Association of America
KM	Knowledge Module
MSC	Multi-stakeholder Committee
NABCB	National Accreditation Board for Certification Bodies
NABET	National Accreditation Board for Education and Training
NCIIPC	National Critical Information Infrastructure Protection Centre
NERC	American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NSAB	National Security Advisory Board
NSCS	National Security Council Secretariat
NTRO	National Technical Research Organisation
OA	Office Assessment
OT	Operational Technology
PLC	Programmable Logic Controller
PrCB	Certification Body for Persons
QCI	Quality Council of India
QMS	Quality Management System
RA	Re-Accreditation
RFP	Request for Proposal
RTI	Right to Information
SA	Surveillance Assessment
SC	Steering Committee
SCADA	Supervisory Control and Data Acquisition
SPB	Specialised Professional Body
SM	Skill Module
SO	Scheme Owner
STC	Supplementary Technical Criteria
TB	Training Body
TC	Technical Committee
WA	Witness Assessment

SECTION 2

GOVERNING STRUCTURE

1. Objective

The objective of this section is to define the governing structure of the Scheme and the roles and responsibilities of various organisations and committees involved in the design, development, operation and management of the Scheme. It also elaborates the handling of complaints and disposal of appeals.

2. Scheme Owner and Scheme Manager

NCIIPC is the Scheme Owner (SO) and QCI is the Scheme Manager, who will operate the Scheme on behalf of the SO.

2.1 Roles and Responsibilities of the Scheme Owner:

2.1.1 Provide vision, overall guidance, and direction to achieve the objectives of the Scheme.

2.1.2 Integrate the capabilities and outcomes of the Scheme into policies and guidance being provided to the critical sector entities and other stakeholders responsible for critical information infrastructure.

2.1.3 Work with the ministries, sectoral regulators and other government / private bodies to popularise the scheme, thereby improving cyber resilience in critical sectors.

2.1.4 Delegate authority to the Scheme Manager to ensure that the day to day and routine operations related to the Scheme are handled smoothly. Following activities/ decisions are delegated:

a. Ensure that information about the Scheme is made publicly available, ensure transparency, understanding and acceptance.

b. Create, control and maintain adequate documentation for the operation, maintenance and improvement of the Scheme. The documentation should specify the rules and the operating procedures of the Scheme and in particular the responsibilities for governance of the Scheme.

c. Ownership of the “Scheme Mark” (logo), to get it duly registered with the appropriate authority. The certification bodies and certified entities shall be required to obtain formal approval for the use of the Mark.

d. Handle complaints at all levels (stakeholders, public) regarding the quality of products as well as the scheme operation.

2.1.5 Participate in all meetings of Committees - Steering, Technical, and Certification Committees, as needed for the development and management of the Scheme.

2.2 Roles and Responsibilities of the Scheme Manager.

2.2.1 Responsible for all activities related to the up keep of scheme documents. Information regarding the schemes will be continuously updated on its website.

2.2.2 Responsible for establishing, implementing, and maintaining scheme requirements.

2.2.3 Ensure that sufficient evidence is maintained to justify that the activity and the criteria selected for the approval of the CO.

2.2.4 Ensure that the Scheme documents, including the criteria and process to assess activities pertaining to accreditation of COs, are publicly available.

2.2.5 Whenever the Scheme Manager provides any clarification about the Scheme to any interested party, ensure that the information is also made available to all the bodies within the Scheme.

2.2.6 Have a legally enforceable agreement with CO to ensure that the CO and its clients use the Scheme as published, without any additions or reductions, and comply with rules for applying the symbol/ statement/ mark, as applicable.

2.2.7 As the provider of approval, mandate the accredited COs to provide reasonable access and cooperation as necessary to enable the QCI assessment team, which includes assessors, technical experts, observers, and regulatorsto assess conformity with the Agreement and per the relevant standard(s).

2.2.8 Have a procedure for dealing with complaints relating to the Scheme, to ensure that complaints of the clients of COs are processed expeditiously.Investigation and decision on complaints shall not result in any discriminatory actions. The detailing of the activities of the Scheme Manager shall be such that it would independently operationalise the Scheme taking due care of issues such as impartiality, free from any conflict of interest etc.

Note: A description of the complaints handling process will be publicly available with or without request.

2.2.9 Monitor the development and review of the standards and other normative documents, whether their own or external, which define the specified requirements used in the Scheme. Any changes in the normative documents to be placed to the Steering Committee for making necessary changes in the Scheme.

2.2.10 Oversee the implementation of the changes (e.g., transition period) made by the COs, wherever necessary, and other parties interested in the Scheme.

2.2.11 Include all the necessary components like describing responsibility and independence for handling and decision making; receiving complaints; gathering all necessary information for establishing the validity of complaints; and deciding what actions are required to be taken in response to the same. Mandate the organisations to ensure that specific information related to the identity of the complainant, wherever the nature of the complaint is sensitive, is handled with confidentiality.

2.2.12 Seek formal approval from NCIIPC if any changes are to be carried out based on the recommendations of the MSC or any notifications issued by the Government which impact the operationalisation of the Schemes.

3. Governing Structure

3.1 The governing structure of the Scheme consists of a multi-stakeholder Steering Committee (SC) at the apex level, supported by a Technical Committee (TC), and a Certification Committee (CC). The Secretariat will be provided by QCI (being the National Accreditation Body and Scheme Manager) on behalf of NCIIPC (being the Scheme Owner).

3.2 The governing structure is depicted schematically in Fig. 2.1.

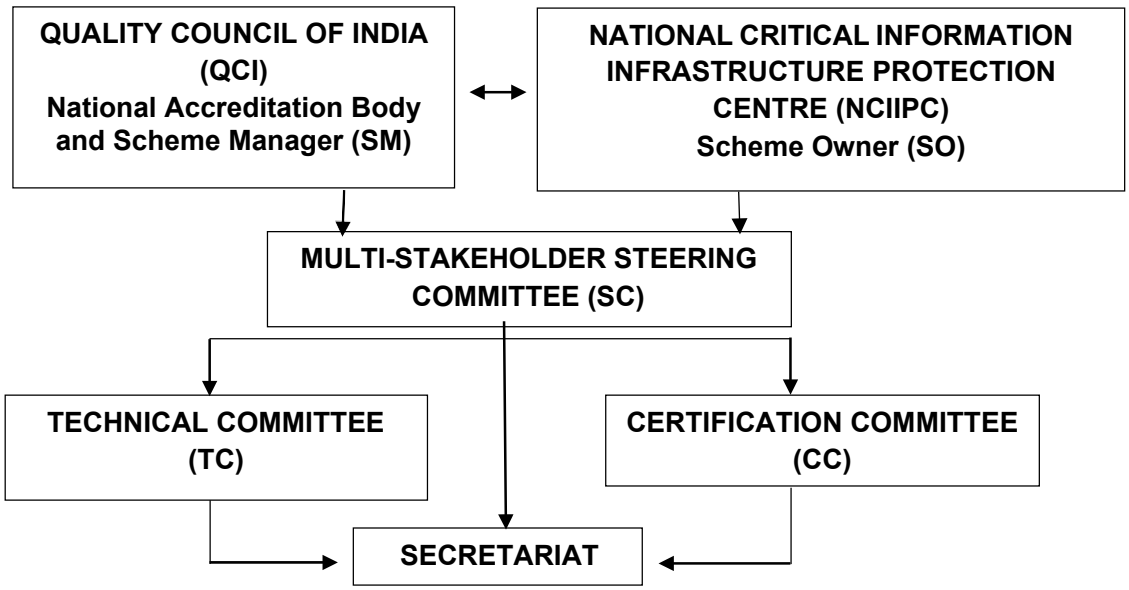

Figure 2.1: Governing Structure

3.3 Appointment of Committees – General Rules

In the appointment of various committees, the following general principles shall be keptin mind:

3.3.1 Representation of the balance of interests such that no single interest predominates.

3.3.2 Stakeholder interests include NCIIPC, relevant ministries, regulatory bodies and other governmental agencies, government departments, CSEs, ABs, PrCBs, COs, training bodies, testing laboratories, user associations, academic/ research bodies, manufacturers of products, providers of services and representatives of organisations working in related areas.

3.3.3 Offer of membership to individual experts shall be made with great caution and only when a suitable person is not forthcoming as a representative of an organisation.

3.3.4 Except when a member is appointed in personal capacity, a person vacates membership upon leaving his/ her organisation, and a fresh nomination is sought from the member organisation.

3.3.5 The member organisations shall nominate a principal and an alternate representative on the committee(s).

3.3.6 All committees shall be reconstituted every two years to provide representation to different stakeholder organisations by rotation, wherever necessary.

3.3.7 While there would be organisations as members with a definitive term, the Secretariat may invite one or more organisations/entities as special invitees.

3.3.8 A minimum of one-third of the members shall constitute the quorum of each committee meeting.

3.3.9 Minutes of the meeting are to be issued by the Secretary of the committee with consent of the Chair of the respective Committee.

3.3.10 Attendance of the committee meetings shall be logged in hard/ soft copies.

3.3.11 The committee chair is authorised to approve the minutes and the relevant scheme documents based on consensus.

3.3.12 The Secretariat will compile and put together the document of the respective Committee for their review, inputs and consent so that it is approved by the respective Chair of the Committee.

3.3.13 The Chair of TC and CC may present the results of the deliberations of their respective committees to SC for information. SC may advise/ guide only on policy-related matters.

4. Multi-stakeholder Steering Committee (SC)

4.1 Membership

The SC shall comprise of the following:

4.1.1. Chairperson – Seasoned professional considered to be well respected by Government and Industry alike, can be in individual capacity.

4.1.2. Nominees from the concerned Ministries – Representative from the Ministries responsible for the critical sectors, namely Banking, Financial Services & Insurance, Telecom, Government, Power & Energy, Transport, Strategic Enterprises and Healthcare, representative from the regulatory bodies responsible for the critical sectors, such as Central Electricity Authority (CEA), Reserve Bank of India (RBI) etc.

4.1.3. Government Agencies – Representative from government agencies, namely NCIIPC, National Security Advisory Board (NSAB), and National Security Council Secretariat (NSCS).

4.1.4. Chairperson SC may co-opt more members in consultation with Scheme Owner and Manager.

4.1.5. Secretariat – Quality Council of India

4.2 Terms of Reference

The SC is responsible for the following:

4.2.1. Overall development, modification and supervision of the Scheme.

4.2.2. Receiving recommendations of the TC/ CC and deciding on them.

4.2.3. Constituting any committees as and when required.

4.2.4. The SC may note approvals of the Chair TC and/ or CC and, if required, give a general direction for any course correction.

4.2.5. A minimum of one-third members shall constitute the quorum of the committee meeting.

4.2.6. Minutes of meetings of the Committees will be issued by the committee's Secretary with consent of the Chair of the respective committee.

4.3 Meetings

The SC shall meet at least once every year.

5. Technical Committee (TC)

5.1 Membership

The TC shall comprise of members/ representatives from the following stakeholdergroups:

5.1.1. Chairperson – a person of eminence, can be in individual capacity.

5.1.2. Ministries and regulatory bodies with oversight responsibility on the critical sectors.

5.1.3. National nodal agencies for Cyber security.

5.1.4. Critical sector entities.

5.1.5. Industry Associations focused on critical sectors.

5.1.6. Knowledge Bodies/ Labs/ COs working in Cyber security.

5.1.7. Chairperson TC may co-opt more members in consultation with Scheme Owner and Manager. Further representatives of similar organisations may be called by rotation as per requirement and mutual agreement by Chairperson TC, Scheme Owner and Manager.

5.1.8. Secretariat – Quality Council of India

5.2 Terms of Reference

The Technical Committee is responsible for the following:

5.2.1. Defining the accreditation criteria for the Scheme and resolving related issues.

5.2.2. Providing overall direction and guidance on the knowledge and skills that are requiredfor each Cyber security domain and expertise level.

5.2.3. Providing direction and guidance on the appropriate technical assessment methodologies for assessing COs.

5.2.4. Assisting the CC in finalizing the Quality Assurance Protocol for controlling the processes of the Scheme.

5.2.5. Defining and formulating the technical requirements of the Scheme.

5.2.6. Deliberations on any other applicable technical requirements.

5.3 Meetings

The TC shall meet at least once every year. Initially, the meetings could be held more frequently until the Scheme stabilises.

6. Certification Committee (CC)

6.1 Membership

6.1.1. Chairperson - A person of eminence, can be in individual capacity.

6.1.2. Government Organisations.

6.1.3. Critical Sector Entities.

6.1.4. Industry associations.

6.1.5. Academic Institutions/ Training Bodies.

6.1.6. Chairperson CC may co-opt more members in consultation with Scheme Owner and Manager. Further representatives of similar organisations may be called by rotation as per requirement and mutual agreement by Chairperson CC, Scheme Owner and Manager.

6.1.7. Secretariat – Quality Council of India

6.2 **Terms of Reference**

The Certification Committee is responsible for the following:

6.2.1. Developing, maintaining, and revising the Scheme, as appropriate.

6.2.2. Developing, maintaining and revising as appropriate the documents for the COs as per the defined scope.

6.2.3. Developing, maintaining, and revising as appropriate the documents for COs to apply for accreditation.

6.2.4. Developing, maintaining, and revising as appropriate the process for permitting approved entities for the use of Scheme mark, if any.

6.2.5. Deliberations on any other issue relating to accreditation of COs.

6.3 Meetings

The CC shall meet at least once every year. Initially, the meetings could be held more frequently until the Scheme stabilises.

7. Roles of Organisations

7.1 NCIIPC is the Owner of the Scheme and shall maintain oversight on the overall efficacy of the operationalisation of the Scheme by QCI.

7.2 Quality Council of India is the National Accreditation Body and Scheme Manager and will

operationalise the Scheme as per the established norms on behalf of the Scheme Owner. It shall establish the MSC in consultation with the Scheme Owner and shall be responsible for the overall management of the Scheme. QCI shall provide the Secretariat to the Scheme.

7.3 National Accreditation Board for Education and Training (NABET), a constituent Board of the QCI, shall be responsible for accrediting COs desirous of participation in the Scheme. NABET shall, through a legally enforceable agreement with the accredited COs, ensure that the COs shall offer NABET and its representatives, including assessors, experts, observers, and regulators appointed in the assessment teams, such reasonable access and cooperation, as necessary, enable NABET assessment team to monitor conformity with the Agreement and the relevant standard(s). The accredited COs shall also provide access to NABET assessors, experts and observers, to its premises to conduct assessment activities. The access to NCIIPC personnel or any personnel nominated by them will be similar to that of NABET.

8. Complaints

8.1 A complaint is an expression of dissatisfaction, other than an appeal, by any person or organisation to COs or AB relating to the activities of that body, where a response is expected.

8.2 The entire system has provisions for accepting complaints from any stakeholder against any component of the Scheme. The COs and ABs are required to have a complaints system in place as per standards applicable to them. Anyone having a complaint is encouraged to utilise the available mechanisms.

8.3 Any complaint received directly by the NCIIPC shall be referred to QCI, who shall refer to the appropriate body against which the complaint is made and monitor it until it is decided upon and reported back to the NCIIPC.

8.4 Any complaint received by QCI shall be similarly handled.

8.5 A statement on complaints as received above with their status shall be reported to the MSC in each meeting.

9. Appeals

9.1 An appeal is a request by COs or AB for reconsideration of a decision made by that body.

9.2 Provisions for addressing appeals from the applicant/ certified persons/ accredited COs under the Scheme shall invariably be utilized.

9.3 In case anyone is aggrieved by the TC/CC decision related to the appeal, the SC shall handle it.

9.4 In case anyone is aggrieved by the decision of SC regarding the appeal, the Chairperson of SC shall appoint an independent appeals panel to investigate and recommend necessary action(s).

9.5 While handling appeals, the fundamental principle of maintaining independence from the personnel involved in the initial decision shall be maintained.

9.6 A statement of appeals received by the NCIIPC will be forwarded to QCI, that shall process the same and may wish to place it before the MSC in each meeting.

10. Review of the Scheme

The scheme will undergo an annual review for three years following its launch and subsequently every five years or sooner, as needed, to ensure its relevance to the current environment. The review process will also encompass an examination of past performance data of accredited COs and consulted clients, along with the status of complaints, appeals, RTIs, and other pertinent information.

SECTION 3

ACCREDITATION CRITERIA

1. Objective

1.1 The Conformity Assessment Framework for Cyber Security of Critical Sector Entities, hereafter referred to as the 'Scheme', has a component that accredits Consultancy Organisations (COs), for rendering consultancy services to the critical sector entities, and others, all termed as client or client entities. The consultancy providers are called IT/ICS Cyber Security Consultancy Organisations (COs). They are required to comply with all the criteria prescribed in the Scheme to obtain a formal accreditation. This document sets out the accreditation criteria to be fulfilled by the COs to be granted accreditation for operating under the Scheme.

1.2 The objectives of the accreditation criteria defined in this document are as follows:

1.2.1 Serve as a reference for the COs to abide by the laid down requirements for obtaining accreditation.

1.2.2 Enable all COs to follow a standard set of accreditation criteria for demonstrating their competence in terms of processes and personnel for the scope of consultancy services being offered by them so that their audit can be done in a uniform way.

1.2.3 Serve as a reference document for auditors to provide the basis for auditing the applicants' COs.

2. Scope

This document specifies the accreditation requirements to be implemented by COs that want to provide one or more than one consultancy services defined in this document for accreditation under the scheme.

3. Intended Stakeholders

3.1 CO providing/supplying consultancy services.

3.2 CSEs, as a requirement, to document the development of RFPs to select a CO.

3.3 CSEs, to get consultancy services from accredited COs.

3.4 Accreditation Body.

4. References for Implementation Guidance

The following documents, in whole or in part, are normatively and informatively referenced in Accreditation Criteria for IT/ICS Cyber Security COs.

4.1. Normative references

4.1.1. IS/ISO 9001:2015 - Quality management systems – Requirements
4.1.2. IS/ISO/IEC 20700: 2017 - Guidelines for management consultancy services

4.2. Informative References

4.2.1. IS/ISO/IEC 27000 Family of Standards
4.2.2. IEC 62443 Family of Standards
4.2.3. NIST SP 800-82 Rev. 3: April 2022
4.2.4. Personnel Certification Scheme for IT and ICS Cyber Security Professionals

5. Document Structure and Approach

The 'Personnel certification scheme for IT/ICS Cyber Security Professionals' has defined 19 cyber security domains to cover the IT and ICS systems and infrastructure landscape of client entities and 10 cyber security functions that client entities are required to carry out to ensure the cyber security of their IT and ICS infrastructure. The cyber security domains of client entities are complex and dynamic and require a substantial depth and breadth of knowledge, expertise and skills to ensure that the associated cyber security functions are properly carried out to achieve cyber resilience. Cyber entities typically look for competent, capable and trustworthy COs, who can carry out the work required in different cyber security domains and cyber security functions of the client entities. Accreditation of COs will provide the client entities a pool of COs, who can provide them consultancy services that are aligned with their needs under different work heads.

Table 3.1 of Annex A of this section lists the cyber security domains and associated cyber security functions that are defined in the 'Personnel Certification Scheme for IT/ ICS Cyber Security Professionals'. The scope of consultancy services (Work Heads) under the Scheme are defined in Table 3.2 of Annex A of this section. An accredited CO can offer their services as a whole package or parts of it, depending on the scope chosen and the services sought by the client. During the accreditation process, the CO shall be attested for their capability, competence and level of expertise to provide consultancy service as per the work/ service defined and described in Table 3.3 of Annex A of this section.

The competence requirements of consultants of COs are defined in Annex B of this section.

The normative technical criteria checklist for COs is defined in Annex C of this section. The description given in column 2 of the checklist may also be used to design the processes by COs, self-assessment and 3rd party auditors of accreditation body for compliance audits.

Para 6 defines the Accreditation Criteria for the COs. The accreditation criteria are structured based on the following three principles:

5.1 **Fulfilment of client requirements:** Clients and the consultancy organisations are able to reach common understanding based on these criteria to identify and agree on the scope of consultancy services to ensure the effectiveness of the processes of IT / ICS security in line with the requirements.

5.2 **Deliverables to the client:** Services, as per the agreement, are delivered in a structured manner which follows a project management approach – clear baselining and professional execution, follow code of ethics and while maintaining the confidentiality of client entities, information and data.

5.3 **Competence of consultants of COs (refer to Annex B of this section):** Capability and technical competence of the consultancy service provider, access to / availability of the relevant IT/ICS security tools and infrastructure shall be up to date and in accordance with the services offered.

6. Accreditation Criteria for COs

The accreditation criteria for COs primarily comprise of following components:

6.1 General Requirements

6.1.1. **Legal Entity:** The COs shall be a legal entity or a defined part of a legal entity such that it can be held legally responsible for all its conformity assessment activities. A governmental consultancy organisation is deemed to be a legal entity based on its governmental status. In case a large organisation wants to be accredited for consultancy and training as a Conformity Assessment Body (CAB), the activities/functions and governance of the CAB shall be separate and distinctly identifiable within that organisation.

6.1.2. **Organisational Structure:** The COs shall define and document the duties, responsibilities and reporting structure of its personnel and any committee and its place within the organisation. When the consultancy organisation is a specified part of a legal entity, documentation of the organisational structure shall include the line of authority and the relationship to other parts within the same legal entity. The organisation should be in business of consultancy services in the area of cyber security for a minimum of 1 year. In case of 'Start Ups and similar initiatives' the policy of the Government of India will be applicable.

6.1.3. **Integrity:** The COs and their personnel shall maintain integrity at all times. The COs shall implement adequate measures to ensure integrity.

6.1.4. **Confidentiality:** The COs shall ensure the confidentiality of data and information obtained during their consultancy activities by having a suitable system. (refer to Annex E titled as 'NON-DISCLOSURE AGREEMENT – UNDERTAKING' in this section).

6.1.5. **Liability and Financing**

a. The COs shall evaluate its finances and sources of income and demonstrate that initially, and on an ongoing basis, commercial, financial, or other pressures do not compromise its operational integrity.

b. The COs shall be able to demonstrate that they have evaluatedthe risks arising from their consultancy activities and that they have adequate arrangements (e.g., insurance or reserves) to cover liabilities arising from their operations in each of their activities and the geographic areas in which they operate.

6.2 Quality and Information Security Management System

6.2.1. Fulfilment of client requirements and client satisfaction can be achieved through applying

a QMS addressing the 'design and delivery of consultancy services for cyber-security (or information security) of IT and ICS systems and infrastructure', which can be obtained by complying with the requirement of IS/ISO 9001:2015 or its current version. Therefore, CO shall be certified/complied to Quality Management System as per QMS IS/ISO:9001:2015 or its current version issued by a CB which is accredited by an IAF-MLA signatory such as by NABCB .

For ensuring that all assets of CO are protected from the perspective of cyber security, CO shall ensure its ISMS compliance/certification.

6.3 Requirements of Management Consultancy Services

As per the agreement with the client, deliverables by the consultancy organisations can be achieved in line with ISO 20700:2017, Guidelines for management consultancy services. The details are given in Annex C of this section. An informative template titled as 'cybersecurity consultancy agreement' is provided in Annex D of this section. Professional consultancy organisations can have their own templates as per their corporate practice, but they shall ensure that the requirements mentioned in Annex C and Annex D are broadly complied.

Note: There may be a case that with IS/ISO 9001:2015 certification, the client entity may be able to demonstrate compliance with all requirements of ISO 20700:2017 specified in this document. The accreditation body will take due cognizance of the same. The extent of audit in no. of man-days may get reduced accordingly. But being the accreditation process, the adequacy of technical competence of each member (knowledge, skill and experience) will still be assessed by an assessment team of the accreditation body.

6.4 Competency requirements and scope of accreditation

Technical competence is the paramount attribute for delivering consultancy services in the cybersecurity of the IT and ICS systems and infrastructure for CII. Therefore, the CO shall ensure that their consultants possess necessary professional qualifications, skills and experience in the relevant domains of IT/ICS cyber security (refer to Annex B of this section).

The applicant CO shall formulate its scope of accreditation by selecting 'Title of consultancy services' mentioned in Annex A of this section, as applicable, where CO has established capability, capacity and competence (knowledge, skill and experience) to deliver the same efficiently to the client organisation.

7. HR Requirements

7.1 Personnel (HR requirements)

7.1.1 The COs shall have, as part of their organisation, personnel, either employed or on contract, having sufficient competence for delivering the consultancy agreement as per the Scheme requirement.

7.1.2 The COs shall have defined processes for selecting, training, and formally authorising and monitoring the performance of its personnel involved in various consultancy activities and

for selecting technical experts, if needed, as per the requirements of the Scheme document.

7.1.3 The COs shall have a mechanism to keep their professional experts / consultants updated on the relevant contemporary issues in an appropriate manner such as by deputing them to participate in various seminars, workshops, by publishing papers, participation in standardization activities, etc. and similar capacity-building activities.

7.1.4 The infrastructure and staffing of the COs shall be proportional to the scope of activities applied to the Scheme manager.

7.1.5 Also, the COs shall only bid for the assignments once they have internally assessed the competence of their infrastructure and human resources.

7.1.6 The technical documentation by the consultancy organisation of their human resources shall align with the scheme requirements, including the competence profiles, wherever applicable.

7.1.7 Competence of Consultants: In addition to the requirement given above, every consultancy person shall have the appropriate qualification, training, experience,and skills to deliver the contracted services (as per Annex B of this section). They shall be able to make professional judgments about conformity with general requirements using assessment methodology and report thereon. They shall understand the significance of deviations found and their effect on protecting the critical sector entities and prescribe accurate interventions for safeguarding against the threats.

7.2 The domain area expertise, relevant certification/qualification, work experience, consultancy experience, and related training w.r.t scope are mentioned in Annex A and Annex B of this section.

8. Complaints and Appeal Handling

8.1 CO shall establish a documented procedure for the complaint handling process and disposal of the complaint within a reasonable period.

8.2 Complaints may be received from interested parties on any aspect, viz., course content, course delivery, administrative arrangements, pre and post-training activities and the evaluation result.

8.3 Various steps in the complaint-handling process shall include the following:

8.3.1 Providing complaint handling process information that is accessible to the public.

8.3.2 Complaints may be written or oral, in physical or electronic form, oral complaints shall be documented by the person who receives the same with details of the complainant.

8.3.3 Acknowledgement of the complaint.

8.3.4 Investigation for redressal of the complaint.

8.3.5 Communication with the complainant for closure of the complaint.

8.3.6 Informing the complainant of the higher appellate authority or accreditation body(AB) if not satisfied with the outcome.

8.3.7 A record of all complaints and actions taken shall be maintained.

8.3.8 CO shall have a documented appeal handling mechanism for handling appeals against its decisions and for the disposal of appeals within a reasonable time.

8.3.9 The documented procedure shall include provision for applicable correction and corrective and/or preventive action to be taken, if required, as a result of any complaint or appeal. In addition, the procedures shall include the potential involvement of AB in unresolved complaints or appeals.

8.3.10 CO shall inform all interested parties of the right to make a complaint or an appeal and shall make it publicly available without request.

Annexure A

Scope of Work: Cyber Security Consultancy Organisation (for accreditation purposes)

The Cyber Security Consultants shall as per the scope and ensuing agreement - identify baseline and problems associated with the same, evaluate security relevant issues, assess risk, offer measures / options to handle the relevant technical / process / people related issues, monitor the implementation of the finalized measures to defend against threats to CSEs' networks and computer systems. (OT infrastructure and its interfaces with relevant IT systems, with external networks)

The scope of consultancy services as described below are for demonstration of capabilities for a particular work head which are linked with a cyber-security domain as defined in clause 5.3.4 in Table 3.2 of document titled as 'Personnel certification scheme for IT/ICS Cyber Security Professionals (CyberPros)', and associated Cyber Security Functions. The cyber security domains (19 in number) are bundled under different Work Heads (WH) which are 11 in number (refer to Table 3.2 of this annexure) based on the common themes. The ICS specific work heads include work items related to securing ICS. COs are required to demonstrate to the AB their capability for execution of these work that is sought by any CSE.

Table 3.1: Cyber Security Domains

S. No.	Cyber security Domain Type	Cyber security Domain	Associated Cyber security Function
1	Organisational	Governance, Risk and Compliance	Govern & Administer (GA)
2	Technical	Technology & System Security Architecture	Acquire & Provision (AP)
3	Technical	Secure Software Development	Acquire & Provision (AP)
4	Technical	Application Security Testing	Acquire & Provision (AP)
5	Technical	Security Product Testing	Acquire & Provision (AP)
6	Technical	Network Security Administration	Operate & Maintain (OM)
7	Technical	System Security Administration	Operate & Maintain (OM)

S. No.	Cyber security Domain Type	Cyber security Domain	Associated Cyber security Function
	Technical	Applications & Data Security Administration	Operate & Maintain (OM)
9	Technical	Security Support Services	Operate & Maintain (OM)
10	Technical	Security Performance Management	Operate & Maintain (OM)
11	Technical	ICS Cyber Security	Operate & Maintain (OM)
12	Technical	ICS Cyber Risk Assessor	Govern & Administer (GA)
13	Technical	ICS Cybersecurity design, & Implementation	Acquire & Provision (AP)
14	Technical	ICS Cybersecurity Operations & Maintenance	Operate & Maintain (OM)
15	Technical	Cyber Defence	Analyse & Investigate (AI) [Identify (ID), Protect (PR)]
16	Technical	Cyber Vulnerability, Threat & Risk Management	Analyse & Investigate (AI) [Identify (ID), Protect (PR)]
17	Technical	Security Operations	Analyse & Investigate (AI) [Detect (DE), Respond (RP)]
18	Technical	Cyber Forensics & Investigation	Analyse & Investigate (AI) [Identify (ID), Protect (PR), Recover (RC)]
19	Organisational	Cyber Training & Awareness	Train & Enable (TE)

Table 3.2: Scope of Consultancy Services (Work Head) with Cyber Security domain and functions

WH-Id	Title of Consultancy Service (Work Head)	Related Cyber Security domain (indicative)	Related Cyber Security function
WH-1	Designing and facilitation of implementation of CSMS (L1/L2/L3) with focus on Governance, Risk and Compliance Requirements	Domain 1 (Governance, Risk and Compliance)	Govern & Administer (GA)
WH-2	IT Cyber Security, Architecture, Design, Engineering and Implementation	Domain 2 (Technology & System Security Architecture)	Acquire & Provision (AP)
		Domain 3 (Secure Software Development)	Acquire & Provision (AP)
		Domain 4 (Application Security Testing)	Acquire & Provision (AP)
		Domain 5 (Product Security Testing)	Acquire & Provision (AP)
WH-3	IT Cyber Security Administration and Management	Domain 6 (Network Security Administration)	Operate & Maintain (OM)
		Domain 7 (System Security Administration)	Operate & Maintain (OM)
		Domain 8 (Applications & Data Security Administration)	Operate & Maintain (OM)
		Domain 9 (Security Support Services)	Operate & Maintain (OM)
		Domain 10 (Security Performance Management)	Operate & Maintain (OM)
WH-4	ICS Cybersecurity Risk Assessment	Domain 12 (ICS Cyber Risk Assessor)	Govern & Administer (GA)
WH-5	ICS Cybersecurity Architecture, Design, Engineering and Implementation	Domain 13 (ICS Cybersecurity design, & Implementation)	Acquire & Provision (AP)
WH-6	ICS Cybersecurity Operations & Maintenance	Domain 14 (ICS Cybersecurity Operations & Maintenance)	Operate & Maintain (OM)
WH-7	Cyber Defence	Domain 15 (Cyber Defence)	Analyse & Investigate (AI)
WH-8	Cyber Security Monitoring and Assessment	Domain 16 (Cyber Vulnerability, Threat & Risk Management)	Analyse & Investigate (AI)

WH-Id	Title of Consultancy Service (Work Head)	Related Cyber Security domain (indicative)	Related Cyber Security function
WH-9	Cyber Security Operations	Domain 17 (Security Operations)	Analyse & Investigate (AI)
WH-10	Cyber Security Forensics & Investigation	Domain 18 (Cyber Forensics & Investigation)	Analyse & Investigate (AI)
WH-11	Cyber Training & Skill Gap Assessments	Domain 19 (Cyber Training & Awareness)	Train & Enable (TE)

Note: The mapping of domains against each of the WH Id is done in manner that it addresses the requirement of CXOs for consultancy services related to the associated cyber security functions. It may be noted that:

a) Domain 1 is related to IT/ ICS GRC under the CISO,

b) Domains 2 to 5 & 13 are related to design, engineering and implementation of IT/ ICS systems by project engineering teams,

c) Domains 6 to 10 & 14 are related to cyber security aspects for consideration by the IT & ICS teams under the CIO, ICS Head

d) Domains 12, 15 to 18 are exclusively related to cyber security functions by the IS & SOC teams under the IT / ICS CISO, and

e) Domain 19 is related to training under Head HR.

Table 3.3: Scope of Consultancy Services: Description of the Work / service {(Work Heads(WH)}

Description	Level of Expertise*
WH-1: Designing and facilitation of implementation of CSMS (L1/L2/L3) with focus on Governance, Risk and Compliance Requirements	
1. Status Audit and Gap Analysis 1.1 Review of existing CSMS/ISMS policy, process and procedure 1.2 Identify gaps and analyse the same. 1.3 Comprehensive Report on the Gaps Identified 1.4 Comprehend/Report activities and tasks for mitigating the gaps in terms of organisational, people, physical and technological control requirements and provide a cost estimation. 2. Facilitation of designing and preparation of Policy, Process & Procedures document for CSMS/ISMS 2.1 Designing Cyber Security Policy for CSE (in terms of Policy, Process, Procedure) considering business environment, threat and vulnerabilities, result of risk analysis, risk appetite of CSEs their organisational goals and objectives, and applicable technical criteria. The advice on the security policies at different policies such as program, issue, system specific policies.	1. Auditing Skills and knowledge ofvarious IS/ISO/IEC 27000 family of standards. 2. Technical criteria (BTC Level 1, STC Level 2 and ATC L3, as applicable. 3. Knowledge of business environment and operations of specific critical sector entity. 4. Skills to establish and communicate organisational cybersecurity policy. 5. Expertise in defining cyber security roles and responsibilities in an aligned way and the role of CISO and risk owners. 6. Equipped with the knowledge of legal and regulatory requirements regarding cybersecurity, including privacy. 7. Understanding of governance and risk management processes with the ability to address cybersecurity risks. *Power sector specific requirements(additional)* 1. Knowledge and auditing skills and IS16335 2. Knowledge of IT and ICS convergence 3. Knowledge of security issues andconcerns in the power Sector. 4. Knowledge of various IEC 62443 families of standards and IS 16335 and IS/ISO/IEC 27019, if applicable.

Description	Level of Expertise*
2.2 Work closely with CISO to obtain management constraint with policy and local level capacity building to spread the contextualized awareness at various levels. Drive cybersecurity policies, standards and guidelines aligned to the organisation's risk management framework, legislation and regulation. Responsible for establishing and approving ISMS policies, standards and guidelines to effectively manage cybersecurity risks, integrate and align the cyber risk management framework in the organisation's context. 2.3 Designing CSMS/ISMS (conceptual/ principle level/ blueprint) and obtaining management consent while working with CISO. This shall include preparation of Statement of Applicability (SoA), scope and boundaries of CSMS/ISMS. 2.4 Design & Review of supporting Standard Operating Procedures (SOPs) for realizing and implementing of policies in accordance to function in different areas in the Organisation. 2.5 Facilitate the implementation of these procedures and carry out a mock compliance audit. 2.6 Advice/Support for framing Request for Proposal (RFP). 3. GRC specific consultancy services: Strategies, design IT GRC framework and ISMS/CSMS for organisations and drive projects and investments for	5. Knowledge of business environment and operations of specific criticalsector entity. 6. Ability to dispense the documentation and its implementation in an ICS and SCADA environment. 7. Knowledge of NIST SP 800-82: Guide to Industrial Control System Security and North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards.

Description	Level of Expertise*
cybersecurity of the organisation. 3.1 Governance: Identification and recommendations of mitigation controls based on the results of Risk analysis, creation of implementation roadmaps for various policies at different levels, assessment of performances and compliances. The consultant shall advise on the structure and process based on IS/ISO/IEC/IEC 27014:2020 Information security, cybersecurity and privacy protection — Governance of information security. 3.2 Risk: Defining and setting up risk management frameworks based on industry best practices and standards such as IS/ISO/IEC 27005/ IS/ISO/IEC 31000 along with regular risk assessment with changing threat landscape. Conduct risk assessment to help identify cybersecurity risks and determine appropriate controls to ensure that IT and ICS systems perform within acceptable limits of risks. Monitor, track and manage risk mitigations and exceptions to ensure compliance with cybersecurity standards and policies. 3.3 Compliance Assurance: Compliance with regulations (IT Act, DPA etc. by defining processes for continuous monitoring of applicable controls by defining KPAs and KRAs for reporting to governing board for their compliance status)	

Description	Level of Expertise*
Power sector specific requirements, (if applied for) bythe CO. Review Existing CSMS Policy, Process, Procedure in the context of power sector with focus on STC L2 criteria advice on additional requirements, ENR requirements and enhanced requirements as specified in Annex A of STC Level 2.	
WH-2: IT Cyber Security, Architecture, Design, Engineering and Implementation	
1. The CO shall facilitate to: 1.1 Develop IT/ICS cybersecurity architecture and maintain oversight. 1.2 Advice on maintenance IT/ICS cybersecurity system integration 1.3 Advice quality and continuous improvement of OT cybersecurity architecture 1.4 Improvement and maintenance of cybersecurity posture of IT/ICS systems 1.5 Advice on response to IT/ICS cybersecurity incidents 1.6 Advice on discovery organisation's IT/ICS assets 1.7 Conceptualize, design, engineer, integrate and implement the security and security management aspects in IT and ICS systems of both on-premises and cloud infrastructure of organisations, 2. Development of procedures and process design for the following:	1. The CO shall have proficiency in business needs and analysis, emerging technologies, network security and segmentation, application security management, product security. Power sector specific requirements 1. The CO should be well versed with the various guidelines issued by CEA and enhance IT/ICS/IIoT collaboration with various actors for the national power systems.

Description	Level of Expertise*
2.1 Secure system architecture, mitigate cyber threats and vulnerabilities, periodic review and system security. 3. Implementation and configuration of the IT/ICS network controls to protect the IT/ICS environment.	
WH-3: IT Cyber Security Administration and Management	
1. The CO shall facilitate designing of the following processes: 1.1 Network Security Administration 1.2 System Security Administration 1.3 Application and Data Security Application 1.4 Security Support Services 1.5 Security Performance Management. 2. Capacity building of the respective roles of Cyber Security Professionals in the above areas and prepare these roles for executing their existing responsibilities for complying with CSMS/ISMS controls applicable to them.	The CO shall have expertise and skill in: 1.1 network security planning and management, identifying network security risk and potential control areas, technical vulnerability management, identification and authentication. 1.2 network audit logging and monitoring, intrusion detection and prevention. 1.3 protection against malicious code, cryptographic based services. 1.4 network technical security architecture, design principles and design sign off. 1.5 implementation aspects of network security such as criteria for network component, product / vendor selection. 1.6 network management including logging, monitoring and incident response, documentation etc. 1.7 securing communications between networks using security gates etc. 1.8 enhanced collaboration services, network segmentation and understanding of catalogue of threads 1.9 host access control mechanisms (e.g., access control list, RBAC, ABAC). 1.10 cyber threats and vulnerabilities. 1.11 specific operational impacts of cyber security lapses.

Description	Level of Expertise*
	1.12 authentication, authorization, and access control methods. 1.13 application firewall concepts and functions (e.g., Single point of authentication/ audit/ policy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, data loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing). 1.14 current and emerging data encryption (e.g., Column and Table space Encryption, file and disk encryption) and security features in databases (e.g. built-in cryptographic key management features). 1.15 current and emerging data remediation security features in databases.
WH-4: ICS Cybersecurity Risk Assessment	
1. The CO shall facilitate to: 1.1 Perform cyber risk assessment in the ICS environment, identify ICS assets and categorise them based on risk criticality, risk analysis methodology, categorise risk and build risk matrix and document risk analysis results. 1.2 Knowledge of processes of ICS systems in the organisation 1.3 Knowledge of cyber threat libraries and stages of cyberattacks. 2. Development of procedures and process design for the following:	The CO shall have proficiency in business needs and analysis, emerging technologies, network security and segmentation, application security management, product security. Skill in interconnectivity and communication paths of assets in the ICS environment. The CO should have proficiency in IEC 62443 family of standards specially on IEC 62443-3-2 and IEC 62443-3-3. *Power sector specific requirements* The CO should be well versed with the various guidelines issued by CEA and enhance IT/ICS/IIoT collaboration with various actors for the national power systems.

Description	Level of Expertise*
2.1 Cyber risk assessment techniques for the ICS environment 2.2 Security risks, threats and vulnerabilities in the organisation's ICS environment 2.3 Operational, safety and business risks and implications from cyber security loopholes and possible treatments of ICS cyber risks 2.4 Key requirements and objectives of various ICS cyber risk assessments and pros and cons of various risk mitigation treatment approaches	
WH-5: ICS Cybersecurity Architecture, Design, Engineering and Implementation	
The CO shall develop ICS Cybersecurity Design, & Implementation procedures and process covering: 1. ICS security architectures and systems design 2. Emerging trends and potential impacts on enterprise architecture and security controls 3. Key criteria for determining required level of security controls. 4. New and emerging ICS security system design methodologies, tools and techniques 5. Interdependencies and impact of changes on ICS systems	The CO shall have capability in ICS cybersecurity architecture and maintain oversight, maintenance of cybersecurity system integration, improving and maintaining the cybersecurity posture of ICS systems. The CO shall be proficient in NIST 800-82 and IEC 62443 family of standards.
WH-6: ICS Cybersecurity Operations & Maintenance	

Description	Level of Expertise*
The CO shall develop ICS Cybersecurity Operations & Maintenance scope, policies and procedures covering: 1. Range of patch management configuration techniques and embedded devices. 2. Threats posed by relevant stakeholders provided with access and privilege to ICS systems or embedded devices. 3. Types of interactions and possible conflict during patch deployment by internal and external stakeholders. 4. Tools and techniques for safe deployment of patches in ICS systems or embedded devices host architectures (Appliances, mobile devices, laptops, firmware) and interdependencies with ICS systems for patch updates. 5. Vulnerability and patch management techniques and strategies and their implications on ICS system operations and legacy systems. 6. Trade-offs between patch security, usability and availability of ICS systems, Industry best practices in fault detection, isolation, and recovery in the context of network administration in the ICS environment.	The CO shall have capability of conduct threat hunting in the ICS environment provide threat intelligence. Integration and maintenance service providers shall comply with IEC 62443-2-4.
WH-7: Cyber Defence	
	The CO shall have competencies in hacking methodologies, social dynamics of computer attackers in a global context, anti-forensics tactics, techniques and procedures, malware analysis concepts and methodologies, signature implementation impact for viruses,

Description	Level of Expertise*
	malware, and attacks, incident reporting and dissemination procedures, procedures used for documenting and querying reported incidents, problems and events and identification of software communications vulnerabilities. The CO shall also have ability to conduct the incident response and root cause analysis of any incident.
WH-8: Cyber Security monitoring and Assessment	
1. Development of procedures and process design for the following: 1.1 Monitoring of IT/ICS systems for cybersecurity 1.2 Improvement and maintenance of cybersecurity posture of IT/ICS systems 1.3 Respond to IT/ICS cyber incidents. 1.4 Advice on performing threat hunting activities by proactively scanning logs, network traffic SIEMs and other channels for suspicious behaviours and indicators of compromise. 1.5 Facilitate identifying IT/ICS assets prone to cyber threats and attacks. 1.6 Train the responsible person on monitoring for potential threats actors/groups/individuals capable of	1. The consultant should have capability and experience on the process and technologies for security monitoring and assessment including: 1.1 Design of processes and local capacity building of the client CSEs 1.2 Capable of recommending various technological options including instrumentation, tools and techniques and cost estimations to client CSEs. 1.3 The consultant should have adequate infrastructure and capability to advise on VAPT as specified in S No. 6 of the Description for WH-3. 1.4 Ability to conduct the Incident Response and Root Cause Analysis of any Incident.

Description	Level of Expertise*
attempting cyber-attacks. 2. Conduct research on new and existing threats that may impact existing IT/ICS systems and transfer this knowledge to the client CSEs. 3. Document new threats and establish threat profile based on a core set of attributes to assist in development of threat mitigation protocols. 4. Provide evaluation and feedback to improve intelligence productions, reporting, collection requirement and operations. 5. Advice and develop emerging technology synthesis, process for CSEs. 6. Advice and ability to conduct Vulnerability Assessment and/or Penetration Testing, formulating the procedures, test methods, report formats, instrumentation, tools and costing. 7. Advice on formulating procedures and methods for Security Product Testing based on global standards such as common criteria (IS/ISO/IEC 15408 and Crypto module validations).	

Description	Level of Expertise*
WH-9: Cyber Security Operations	
1. The CO shall facilitate in designing processes and preparing processes for the following: 1.1 Manage IT/ICS system control and remote access 1.2 Improve and maintain cybersecurity posture of ICS systems. 1.3 Network Security Administration 1.4 System Security Administration 1.5 Applications & Data Security Administration 1.6 Security Support Services Security Performance Management 2. The CO shall prepare the client for different roles, which typically can be broken into tiers according to their involvement in an incident'stimeline and severity. E.g., the common roles and responsibilities of a SOC team can be: 2.1 Security Analyst (Tier One) – Responsible for vulnerability monitoring, triaging identified incidents and escalating those that warrant it. 2.2 Security Analyst (Tier Two) – In charge of investigating and responding to incidents, then	1. The CO shall have proficiency in: 1.1 Access and Control Management 1.2 Application Security management 1.3 Business continuity and recovery 1.4 Cryptography and Encryption 2. The CO shall have expertise in designing and operating SOCs. 3. The CO shall advise Security Operation Centre (SOC) not merely a control room where cybersecurity professionals monitor a company's IT infrastructure but a synthesis of operations, technologies, and best practices that work together to form a comprehensive cybersecurity strategy. The CO shall have the ability to drive on-site counselling and capacity building on the above and advise on the applicable tools and techniques, environment, knowledge, and skills. Design, implementation, and provisioning of the following: 1. SOC Requirement assessment 2. SOC Monitoring solution, design for policy, process & procedures 3. SOC Technology selection 4. SOC Component implementation

Description	Level of Expertise*
executing response and recovery processes to remediate incidents' impact. 2.3 Threat Hunters (Tier Three) – Responsible for 2.4 assessing IT security infrastructure according to the latest threat intelligence to determine unexpected or stealthy means of network entry. 2.5 Manager (Tier Four) – Responsible for overseeing the entire team and reporting findings, action plans, and threat notifications to the organisation's CISO. 2.6 Engineer/Architect – Works alongside other members of SOC teams, designing, developing, and maintaining security infrastructure.	5. SOC Personnel hiring / provisioning
WH-10: Cyber Security Forensic and Investigation	
1. The CO shall facilitate in preparing the procedure for monitoring the Cyber Security Incidents, providing the response and improving the posture of IT/ICS system. 2. Facilitate in preparing CCMP and conduct of Cyber drills. 3. Digital Forensics: 3.1 Advice on embedding advanced digital forensics and incident response capabilities to fend off advanced persistent threats.	The CO shall have capabilities of Business Continuity and Recovery, Cyber Forensics, Cyber Incident Response and Management, Supply Chain Management, Stakeholder Management and Requirements of IT Act 2000.

Description	Level of Expertise*
3.2 Develop process so that CSE can seamlessly identify, collect, analyse and utilise digital evidence to determine the root cause of security breaches adopt corrective and predictive recommendations to mitigate sophisticated threats. 3.3 Advice on required technologies to address the challenges of cyber-crimes security breach and digital fraud. This shall help organisations to predict, detect and mitigate security incidents. 3.4 Advising on processes and technologies for detecting malware suspicious events in PII risks by combining intrusive analysis with fall content inspection. 3.5 Ministry of electronics and information technologies requirements. 3.6 Application of fencing laboratories as examiner of electronic evidence under section 79 A of Information Technology Act 2000.	
WH-11: Cyber Training and Skill Gap Assessment	
1. The CO shall carry out: 1.1 Skill gap assessment by collaborating with broader cyber security stakeholders and teams and recommend to optimally utilization of resources. 1.2 development of learning road maps for teams and functions after identifying the skill gaps	The CO shall have competencies in analyzing human psychology and behavior to address Cyber Risks and Threats by internal employees and other professionals. The CO shall be an expert in Human Resource Development and management of personnel specific to Cyber Security. Cyber Security experts of CSEs needs to follow highest level of

Description	Level of Expertise*
1.3 established performance indicators to benchmark effectiveness of learning and development for program against best practices. 2. The CO shall consider requirements of: 2.1 Critical core skills like global perspective, creative thinking, problem-solving, decision-making collaboration, trans-disciplinary thinking, communication sense making etc. 2.2 Technical skills and competencies requirement in emerging technologies synthesis, learning and development. 2.3 Other technical and analytical skills such as programming and scripting managing and securing systems networks applications management and securing information, SW development life cycle cyber defense others such as cyber security governance and program management, stakeholder management, threat analysis and defense, threat intelligence and detection vulnerability assessment.	codes of conduct while carry out their responsibilities. Generally, cyber security professionals have access to sensitive data and knowledge about the networks of their clients, which gives them power that can be abused. The consultant shall do the counselling of professionals on this issue to sensitize that impact and repercussions of the issues involved in cyber security.

Annexure B

Competence of Consultants of COs

The CO shall be responsible for ensuring and maintaining appropriate capability throughout the assignment and shall only seek and accept only those assignments that it is capable of fulfilling. These capability includes the following:

a. Managed staff, including contractors (expertise, training and personal skills);

b. Other resources, including technical information center (for standards and other technical literature) access to specialised knowledge, methodologies, tools and technology and other relevant resources like outsourced staff and specialist, maintenance team and system integrators etc.

c. Processes and mechanism exist to depute staff for training, capability building program etc. and maintenance of relevant records.

Educational qualifications and experience of a candidate consultant working in a CO is described below in Table 3.4:

Table 3.4: Educational qualification and experience requirement of consultant

Parameters	Description
Educational Qualification	Graduate in computer science, computer engineering, telecommunication engineering, cyber security, electronics and information technology, instrumentation, software engineering, information systems etc.
Overall experience	At least of 7 years
Professional experience in Industry/ Educational Institute	At least of 5 years
Cyber security relevant experience (in years)	Minimum of 3 years as a part of overall experience
Consultancy Experience (in years)	1 year+ is desirable

The CO shall have at least one in-house consultant with the above qualification and experience for a particular WH. For big and complex projects, generally consultants have a team. The size of the team is agreed at the time of execution of the contract. The consultants should possess the highest level of competency as per Advanced / Master Level or equivalent of applicable modules for which accreditation is sought as per personnel certification Scheme for IT/ICS Cyber Security Professionals (CyberPros).

Knowledge and Skill requirements for CO

The CO can assure to the AB that their consultants/professionals are competent with related knowledge and skill modules as mentioned below (Table 3.5). The demonstration could be as a team or as an individual. The evidence of compliance as well as test of knowledge and skills could be global certification/ teachings / professional arena of work equivalent to the body of knowledge as required by the combinations of KMs and SMs referred in the table. The detailed description of KM and SM given in Annexure 1A of Scheme for CyberPros.

Table 3.5: Work Head related Knowledge and Skill Modules of Personnel Certification Scheme for IT/ ICS Cyber Security Professionals (refer to Annexure 1A in Section 3 of CyberPros)

Work Head	Description	Domain	Related Module of personnel certification Scheme of CyberPros
WH-1	Designing and facilitation of implementation of CSMS (L1/L2/L3) with focus on Governance, Risk and Compliance Requirements	Domain 1 (Governance, Risk and Compliance)	KM 0601 M, KM 0701 A, KM 0601 F, KM 0601 A, KM 0701 F SM 0602 F, SM 0602 A, SM 0603 A
WH-2	IT Cyber Security, Architecture, Design, Engineering and Implementation	Domain 2 (Technology & System Security Architecture)	KM 0401 F, KM 0401 A, KM 0801 F, KM 0801 A, KM 0802 F, KM 0802 A, KM 0803 F, KM 0803 A SM 0101 F, SM 0301 A, SM 0602 F, SM 0602 A, SM 0603 A
		Domain 3 (Secure Software Development)	KM 0501 F, KM 0501 A SM 0401 F, SM 0401 A
		Domain 4 (Application Security Testing)	KM 0502 F, KM 0502 A SM 0401 F, SM 0401 A
		Domain 5 (Product Security Testing)	KM 0201 F, KM 0201 A, KM 0202 F, KM 0202 A SM 0401 F, SM 0401 A
WH-3	IT Cyber Security Administration and Management	Domain 6 (Network Security Administration)	KM 0101 F, KM 0101 A, KM 0102 F, KM 0102 A, KM 0201 F, KM 0201 A, KM 0202 F SM 0101 F, SM 0601F, SM 0201 F, SM 0102 A
		Domain 7 (System Security Administration)	KM 0101 F, KM 0102 F, KM 0201 F, KM 0201 A, KM 0202 F, KM 0202 A SM 0101 F, SM 0201 F, SM 0601 F

Work Head	Description	Domain	Related Module of personnel certification Scheme of CyberPros
		Domain 8 (Applications & Data Security Administration)	KM 0301 F, KM 0301 A, KM 0302 F, KM 0302 A SM 0301 F, SM 0301 A
		Domain 9 (Security Support Services)	KM 0101 F, KM 0101 M, KM 0102 F, KM 0201 F, KM 0201 A, KM 0202 F, KM 0202 A, KM 0803 F, KM 0803 A
		Domain 10 (Security Performance Management)	KM 0101 F, KM 0102 F, KM 0201 F, KM 1001 F, KM 0102 F, KM 1001 A
WH-4	ICS Cybersecurity Risk Assessment	Domain 11 (ICS Cyber Security) Domain 12 (ICS Cyber Risk Assessor)	KM 1301 F, KM 1302 F, KM 1302 A
WH-5	ICS Cybersecurity Architecture, Design, Engineering and Implementation	Domain 13 (ICS Cybersecurity design, & Implementation)	KM 1303 M, KM 1303 A
WH-6	ICS Cybersecurity Operations & Maintenance	Domain 14 (ICS Cybersecurity Operations & Maintenance)	KM 1304 A, KM 1304 M
WH-7	Cyber Defence	Domain 15 (Cyber Defence)	KM 0804 F, KM 0804 A, KM 0901 F, KM 0901 A, KM 0901 M SM 0101 F, SM 0501 F, SM 0501 A, SM 0602 F, SM 0602 A, SM 0603 A
WH-8	Cyber Security Monitoring and Assessment	Domain 16 (Cyber Vulnerability, Threat & Risk Management)	KM 0804 F, KM 0804 A SM 0602 F, SM 0602 A, SM 0603 A
WH-9	Cyber Security Operations	Domain 17 (Security Operations)	KM 0201 F, KM 0201 A, KM 0803 F, KM 0803 A
WH-10	Cyber Security Forensics & Investigation	Domain 18 (Cyber Forensics & Investigation)	KM 1101 F, KM 1101 A, KM 1101 M SM 0101 F, SM 0501 F, SM 0501 A
WH-11	Cyber Training & Skill Gap Assessments	Domain 19 (Cyber Training & Awareness)	KM 1201 F, KM 1201 A SM 0401 F, SM 0602 F SM 0602 A

Note: The knowledge and skill required for particular work head, mentioned in the table above, shall be in line with knowledge and skill required for master/ advanced level expertise in relevant domain, based upon its applicability.

Annexure C

Technical Criteria Checklist for COs (Normative)

(1)	(2)	Self Asst./ Auditor
Cl. No.	**DESCRIPTION**	
1	**Policies**	
	CO shall define the policies for the assignment delivery and apply them during the assignment.	
1.1	**Regulatory framework** The CO shall maintain an appropriate awareness of the relevant laws, policies, rules, regulations and standards that govern their services and those of the client. The CO shall: — engage in dialogue with the client entity to determine the relevant laws and regulations for the assignment. — manage any conflict between laws and regulations relevant to its general activities and those relevant to the specific assignment. If conflicts exist, the relevant laws and regulations for the assignment shall be identified in the agreement to ensure clarity.	
1.2	**Stakeholder/client entity engagement and commitment** The CO shall engage in dialogue with the client entity to identify the relevant stakeholder/client entity and agree on their involvement. The CO, together with the client entity shall, then engage with those relevant stakeholder /client entities to agree on their involvement. The stakeholder/client entity's role and relationship with the CO shall be described in the agreement. The agreement shall include the following: — access to information; — consultation; — communication; — roles and responsibilities. An effective strategy and policy shall exist for communicating with stakeholder/client entity for the duration of the assignment.	
1.3	**Code of ethical and professional conduct** A code of conduct shall be observed to guide the ethical and professional conduct of the CO during the assignment. This code of conduct shall include significant topics such as: — professional behaviour; — sustainability; — social responsibility; — conflict of interest; — integrity.	

(1)	(2)	Self Asst./ Auditor
Cl. No.	**DESCRIPTION**	
1.4	**Project governance** An appropriate system for project governance shall be agreed upon. The project governance system shall include the following: — scope of work and deliverables; — management structure (including client entity representatives); — policies, processes, and methodologies to be used; — limits of authority for decision-making; — stakeholder/client entity responsibilities and accountabilities; — interactions such as reporting; — process for escalation of issues; — process for identification and management of risks; mechanisms and controls to monitor, support, and enforce ethicalbehaviour; — mechanisms to facilitate the reporting of unethical behaviour without fear of reprisal. — The governance of the project shall be carried out jointly by the CO, the client entity and the recipient.	
1.5	**Capability** The CO shall be responsible for developing and maintaining appropriate capability throughout the assignment and shall only seek and accept those assignments that it can fulfil. Capability includes: — managing staff, including contractors (expertise, consultancy and personal skills); — qualification of employees for various domains — other resources, including access to specialized knowledge, methodologies, tools and technology and other relevant non-staff resources.	
1.6	**Communication** An effective strategy and policy shall exist for communicating with relevant stakeholder/client entity for the duration of the assignment.	
1.7	**Data protection and confidentiality** The communication policy shall encompass confidential data and information and intellectual property rights, such as benchmarks, for all stakeholder/client entities. The CO shall safeguard the privacy rights of all the stakeholder/client entities by limiting the types of information gathered and how such information is obtained, stored, used, reported and secured. The CO shall not use the stakeholder/client entity' data or information without permission for any reason, particularly to demonstrate the capacity of the CO to execute an assignment. The CO shall maintain their credibility and the confidence of the clients. The CO shall be responsible for the confidentiality of data and information received from clients even after the closure of the assignment.	

(1)	(2)	Self Asst./ Auditor
Cl. No.	**DESCRIPTION**	
1.8	**Protection of intellectual property** For intellectual property rights arising from the outcome/deliverables of the assignment (ownership, right to use or right to refer to), the ownership shall be agreed upon during the contracting phase and shall apply after the closure of the assignment.	
1.9	**Social responsibility** The CO shall endeavour to achieve socially responsible outcomes that consider the interests of the stakeholder/client entity. Considerations could include the following: — demonstration of the CO's contribution to stakeholder/client entity; — contribution to sustainable development; — ethical project governance, including transparency; — alignment with norms and standards that relevant organisations document.	
1.10	**Health and safety** The CO shall engage in dialogue with the client entity to continually assess and mitigate the assignment-related risks to the health and safety of the consultants and other relevant stakeholder's /client entities.The agreement shall provide information on the scope, the resources and the facilities relevant to health and safety risk consideration within and with which the CO shall identify, analyse, assess and prioritize the nature of potential risks, coordinating and applying the required resources to minimize, monitor and control the probability and impact of unforeseen events.	
1.11	**Risk and quality management** The CO shall continually anticipate, evaluate, prioritize and manage risks and quality issues associated with the assignment. Both commercial and project-related risks shall be considered. The CO shall coordinate and apply the required resources to minimize, monitor and control the probability and impact of unforeseen events.	
1.12	**Guarantees** COs shall negotiate and agree on the conditions of any guarantee of the services to be provided.	
2	**Contracting**	
2.1	**General** The structure for the contents of an agreement shall include sub-clauses 2.2 to 2.4. The client entity and the CO shall perform the contracting phase together.	
2.2	**Purpose** The CO shall define the contract's purpose considering and protecting the client entity's interests and the CO.	

(1)	(2)	Self Asst./ Auditor
Cl. No.	**DESCRIPTION**	
2.3	**Input** The CO shall identify the inputs to the contracting phase, including the client entity's perceived needs, expectations and desires, the potential constraints and risks involved in the assignment, and any significant changes beyond the scope of the change control process.	
2.4	**Outcome** The outcome of the contracting phase shall determine the services and the deliverables to be provided and establish rights and obligations for each of the parties.	
2.5	**Contents**	
2.5.1	**General** The agreement shall include: — context; — services and deliverables; — approach and work plan; — roles and responsibilities; — acceptance criteria; — terms and conditions.	
2.5.2	**Context**	
2.5.2.1	**Background information, assumptions, scope and limits** The agreement shall contain relevant facts, such as an accurate description of the organisation's current situation, the client's objectives, why the work needs to be done, the assumptions and their impact, and the scope and limits of the assignment.	
2.5.2.2	**Constraints and risks** The agreement shall specify the constraints and risks associated with the assignment to the extent that they are known and identified, referring to policies.	
2.5.2.3	**Stakeholder/client entity** The agreement shall specify any agreement negotiated with the stakeholder/client entity.	
2.5.3	**Services and deliverables** The agreement shall contain a description of the services to be provided, the expected outcomes, the assignment deliverables, and the conditions and process for acceptance. The services shall be able to be evaluated with formal evaluation criteria.	
2.5.4	**Approach and work plan** The agreement shall include a work plan. The following elements shall be considered: a) objectives, scope and expected outcomes; c) approach and methodology; project governance (changes to the scope, escalation procedures,etc.); d) contents; e) documentation; f) data, information and technological resources;	

(1)	(2)	Self Asst./ Auditor
Cl. No.	**DESCRIPTION**	
	g) project organisation; h) CO's human resources and their responsibilities; i) client's, recipient's and other stakeholder/client entity' human resources and their roles and responsibilities; j) timetable and milestones; k) project budget; l) project management methods; m) communications (channels, methods, etc.); n) client entity and/or recipient capacity building; o) knowledge transfer; p) quality and risk methodology; q) deliverables.	
2.5.5	**Roles and responsibilities**	
2.5.5.1	**General** This agreement shall specify the roles, responsibilities and all the resources (including client's, recipient's and other stakeholder/client entity' people, data and documentation) involved in the assignment.	
2.5.5.2	**Assignment monitoring and control** The agreement shall specify the assignment's decision-making, direction and control processes, including the designation of a project 'sponsor' or project 'leader' for the project governance role.	
2.5.5.3	**Evaluation of the assignment** The agreement shall specify how the evaluation will be carried out, for example, measurable milestones, how objectives shall be evaluated and to whom interim and final evaluation results shall be reported.	
2.5.6	**Acceptance criteria** The agreement shall specify the acceptance criteria, such as key performance indicators (KPIs).	
2.5.7	**Terms and conditions**	
2.5.7.1	**Commercial terms** The agreement shall specify terms and conditions relevant to billing, such as fees/charges, payment schedule, expenses, etc.	
2.5.7.2	**Contracting standard terms and conditions** The agreement shall specify any information pertinent to relevant legal and regulatory requirements and statutory obligations, such as ownership of material and deliverables, user rights, licensing, intellectualproperty rights, liability limits, etc. This may also include reference to applicable professional standards. The CO shall have a process for dealing with claims and disputes. This process shall be communicated clearly to the client.	

(1)	(2)	Self Asst./ Auditor
Cl. No.	**DESCRIPTION**	
2.5.7.3	**Policies to be included in the agreement** The agreement shall specify any requirements, responsibilities and activities relating to policies and any other agreed item applicable to the assignment. COs shall assess their responsibilities and activities for all policies and declare if they are not applicable.	
3	**Execution**	
3.1	**General** Execution is the performance of the services agreed upon in the contracting phase. Beyond the delivery of the agreed services and the performance of the assignment, the ultimate aim of the execution phase is to fulfil the agreement.	
3.2	**Purpose** The CO shall define the purpose of this phase to deliver as per agreement.	
3.3	**Input** The CO shall start execution once there is an agreement. Significant changes in the context of the assignment that have an impact on the execution shall be addressed.	
3.4	**Outcome** The outcomes of the agreement shall be: — services and deliverables; — recommendations and approach for the future, if appropriate; — ongoing evaluation and improvement.	
3.5	**Contents**	
3.5.1	**General** The components of the execution phase shall include: — refining the agreed work plan; — implementing the work plan; — assignment management and monitoring; — approvals and acceptance.	
3.5.2	**Refining the agreed work plan** The work plan agreed upon in the contracting phase shall be refined in detail to reflect the actual conditions at the start of the execution phase. The CO shall involve the client entity and the recipient to gain approval for the refined plan.	

(1)	(2)	Self Asst./ Auditor
Cl. No.	**DESCRIPTION**	
3.5.3	**Implementing the work plan** The assignment shall be carried out in accordance with the refined work plan. The method of implementation shall consist of the following steps that the CO performs with the recipient: — Prepare: includes gathering the relevant data, analysing the data with reasonable hypotheses, reviewing business models and listing the issue(s); — Analyse options: includes analysis of different options to address the issues and short-listing the most appropriate option(s); — Recommend: includes recommending appropriate solutions from the existing situation along with an implementation roadmap and expected outcomes; — Obtain decision: includes presentation of recommendations to the client entity or the recipient for decision and acceptance; — Implement: includes execution of recommendations, monitoring the progress made and measuring the outcomes (applicable only when implementation is specified in the agreement).	
3.5.4	**Assignment management and monitoring**	
3.5.4.1	**General** Planning and continuous coordination between the client, the recipient and the CO following areas of activity shall be considered: — project governance; — project management approach; — resources management; — commitment of resources; — monitoring of progress and change control; — risk and quality management; — communication and reporting; — evaluation and feedback.	
3.5.4.2	**Project governance** The client shall make final decisions about the assignment. The CO shall make reasonable efforts to provide relevant information relating to the assignment to the client entity on an ongoing basis. Disputes between the client entity and the CO shall be handled in accordance with the terms of the agreement.	

3.5.4.3	**Project management approach** The CO shall adhere to the agreed project management approach and structure throughout the assignment. The CO shall ensure that the assignment is carried out effectively and efficiently.	
3.5.4.4	**Resource management** All resources involved in the assignment shall be made available and managed in accordance with the agreement between the CO and the client. The deployment by the CO of suitable human resources is the responsibility of the CO. Criteria for suitability shall include relevant domain experience, consultancy skills and people skills.	
3.5.4.5	**Commitment of resources** The CO shall foresee the needs and availability of the client's and the recipient's resources and plan resources in accordance with them.	
3.5.4.6	**Monitoring of progress and change control** The assignment's progress against the work plan shall be monitored and recorded formally using appropriate analysis and monitoring methods. There shall be a change control system or process, including management of the records, to deal with issues that have an impact on the assignment, such as: — deviations from the work plan; — changed the context of the assignment; — changes in the operating environment of the client entity or recipient; — changes in client expectations; — changes in the CO. There may be significant changes that are beyond the scope of the change control process. These shall be considered as new inputs to the contracting and/or execution phase. If required, the agreement shall be renegotiated between the client, the recipient, and the CO.	
3.5.4.7	**Risk and quality management** The client entity and the CO shall follow the agreed risk and quality management methodology to ensure that the agreed service is provided and the outputs are delivered.	
3.5.4.8	**Communications and reporting** The communication principles agreed upon the contracting phase shall be followed throughout the assignment and include regular reporting of progress and risks.	
3.5.4.9	**Evaluation and feedback** The CO shall follow the agreed ongoing evaluation methodology and feedback approach.	
3.5.5	**Approvals and acceptance** There shall be an agreed process to approve and accept all services delivered during the assignment. The commercial implications of acceptance or rejection shall be dealt within accordance with the agreement.	

4	**Closure**	
4.1	**General** The CO shall consider the assignment closed once the final closure topics have been addressed. These include: — legal and contractual matters; — final evaluation and improvement; — administrative matters, including payment of agreed fees where applicable; — communication; — intellectual property rights; — outstanding minor issues.	
4.2	**Purpose** The CO shall define the purpose of the closure phase as an orderly end to the assignment after the delivery of the service in accordance with the agreement.	
4.3	**Input** The closure process shall start when a decision is taken to complete the assignment when the agreed service has been provided and accepted. An assignment shall be terminated before the originally agreed service has been provided. In this case, the closure process needs to take place based on a revised agreement.	
4.4	**Outcome** The closure process shall result in several outcomes, including: — release of all parties from their obligations in the agreement; — a shared understanding of continuing obligations between all the stakeholder/client entity, particularly the CO and the client entity (e.g. guarantees, confidentiality, data protection, intellectual rights, outstanding issues, etc.); — financial settlement of invoices, expenses, etc.	
4.5	**Contents**	
4.5.1	**Legal and contractual matters** The CO shall have effective processes to ensure that all legal and contractual matters are dealt with in a timely and efficient manner, in accordance with the agreement. These processes include: — invoicing and payment; — reconciliation of expenses of the CO; — formal sign-off and acceptance; — release of resources (including subcontractors); — warranties and guarantees; — third party confidentiality; — ownership of intellectual property rights; — obligations that remain after closure (e.g. legal, confidentiality, protection of intellectual property rights, data protection, non-competition, outstanding issues, etc.)	

4.5.2	7.5.2 Final evaluation and improvement Even if no evaluation is included in the agreement, the CO shall have a process to gather feedback and learn from the work it undertakes so that the CO can record the information and knowledge created during the project and apply it for improvement. Evaluation may be required for contractual reasons to determine the fees paid. If this is the case, the CO and the client entity hall agree the most appropriate method of evaluation. Typical metrics may include: — innovation (development of new services); — process effectiveness; — process improvements; — new systems and behaviour; — methodologies; — team performance; — utilization of resources; — sales leads/references; — client satisfaction. The CO shall preferably maintain expertise in evaluation and shall have a systematic process for ensuring that strengths and opportunities for improvement are recorded and shared among the staff. The CO shall have processes to manage improvements such as: a) knowledge management; b) knowledge database; c) technology and methodology improvements; d) case studies; e) training, briefing; f) internal communication.	
4.5.3	**Administrative matters** The CO shall have effective processes to ensure that all administrative matters are dealt with in a timely and efficient manner. These processes can include: — indexing, filing, archiving; — backing-up data and records; — return of client entity property, equipment and facilities (e.g. files, records, data, security passes); — release/recruitment of subcontractors and internal resources; — completion of internal quality assurance procedures.	
4.5.4	**Communication** The CO shall ensure that any obligations regarding communication about the assignment are fulfilled (e.g. confidentiality agreements, preparation of case studies, articles, requests for references, etc.). The CO shall ensure that the client entity is debriefed at the end of the assignment.	
4.5.5	**Outstanding minor issues** The CO shall have a process, agreed upon with the client, for dealing with any outstanding minor issues after the completion of the assignment, so that closure can be achieved.	
5	**Ongoing evaluation and improvement**	

5.1	CO shall evaluate to assess and determine the effectiveness of the assignment. Evaluation shall also allow the client entity and the CO to: — diagnose the effectiveness of the assignment; — make recommendations for corrective action; — implement new processes and methods; — provide and receive feedback from each other; — evaluate added value. The CO and client shall agree on a suitable methodology for ongoing evaluation and feedback throughout the assignment. The CO shall establish a structured process for ongoing evaluation for the duration of the relationship between the client entity and the CO. The effectiveness of the assignment shall be assessed based on the evaluation criteria, the policies and strategies included in the agreement. Even if no evaluation is included in the agreement, the CO shall have a process to learn from the work it undertakes. If evaluation is required for contractual reasons to determine the fees paid, the CO and the client shall agree the most appropriate method of evaluation.	
6	**Claims and Disputes**	
6.1	CO shall have a process for addressing issues arising from disputes and claims. The process shall cover: —Steps for organisation (CO) to participate in dispute resolution process (which should be in congregation with customer satisfaction Code-of-Conduct) —Top management movement in, commitment to, dispute resolutions and deployment of adequate resources within the organisations. —The essential for fair, suitable, transparent and accessible dispute resolution —Monitoring, evaluating and improving the dispute resolutions —Need of intervention of dispute resolution and claim service providers (e.g. industry sector specific associations, ombudsmen and multisector organisations or a mutually agreed mediator)	

Annexure D

CYBERSECURITY CONSULTANCY AGREEMENT

Template

THIS CONSULTANCY AGREEMENT (this "**Agreement**") is made as of MONTH DATE, YEAR and is effective as of MONTH DATE, YEAR, by the NAME OF CO (herewith referred to CO) and between CLIENT ('the company'), a LEGAL ENTITY as per the Companies Act, 2013 of the GoI.

1. Engagement

1.1. The Company hereby engages Consultant to perform, and Consultant hereby agrees to provide advice and assistance to the Company and any of its affiliates related to the AS PER THE SCOPE DEFINED BELOW (the "**Services**").

2. Contracting

2.1. General
The agreement shall include the following:

2.1.1 Context

Background information, assumptions, scope and limits
The agreement shall contain relevant facts, such as an accurate description of the organisation's current situation, the client's objectives, why the work needs to be done, the assumptions and their impact, and the scope and limits of the assignment.

2.1.2 Services and Deliverables

The agreement shall contain a description of the services provided, the expected outcomes, the assignment deliverables, and the conditions and process for acceptance.
The contract between CO and clients will be based on the work items and scope defined in Annex D of this section.
The services shall be able to be evaluated with formal evaluation criteria.

2.1.3 Approach and work plan

The agreement shall include a work plan. The following elements shall be considered:

a. objectives, scope and expected outcomes;
b. approach and methodology;
c. project governance (changes to the scope, escalation procedures, etc.);
d. contents;
e. documentation;
f. data, information and technological resources;
g. project organisation;
h. CO's human resources and their responsibilities;
i. client's, recipient's and other stakeholders' human resources and their roles and responsibilities;
j. timetable and milestones;

k. project budget;
l. project management methods;
m. communications (channels, methods, etc.);
n. client and/or recipient capacity building;
o. knowledge transfer;
p. quality and risk methodology;
q. deliverables.

2.1.4 Roles and responsibilities
This agreement shall specify the roles, responsibilities and all the resources (including client's, recipient's and other stakeholders' people, data and documentation) involved in the assignment.

2.1.5 Evaluation of the assignment
The agreement shall specify how the evaluation will be carried out, for example, measurable milestones, how objectives shall be evaluated and to whom interim and final evaluation results shall be reported.

2.1.6 Acceptance criteria
The agreement shall specify the acceptance criteria, such as key performance indicators (KPIs).

2.1.7 Terms and conditions

a. Commercial terms
The agreement shall specify terms and conditions relevant to billing, such as fees/charges, payment schedule, expenses, etc.
b. Contracting standard terms and conditions

i. The agreement shall specify any information pertinent to relevant legal and regulatory requirements and statutory obligations, such as ownership of material and deliverables, user rights, licensing, intellectual property rights, liability limits, etc.

ii. This may also include reference to applicable professional standards.

iii. The CO shall have a process for dealing with claims and disputes. This process shall be communicated clearly to the client.

c. Policies to be included in the agreement
The agreement shall specify any requirements, responsibilities and activities relating to policies and any other agreed item applicable to the assignment.
COs shall assess their responsibilities and activities for all policies and declare if they are not applicable.

2.2. Definitions

2.1.1. Company Data: Company Data is any and all data that the Company has disclosed to the Contractor. For the purposes of this Agreement, Company Data does not ceaseto be Company Data solely because it is transferred or transmitted beyond the Company's immediate possession, custody, or control.

2.1.2. Data Breach: The unauthorized access and acquisition of computerized data that materially compromises the security of confidential and/or sensitive personal information maintained by the Company as part of a fact base of distinctive information regarding a range of individuals and/or that leads to a breach and/or the Company has sufficient reason to believe has to lead to loss or injury to any Company's properties.

2.1.3. System: A range of equipment that assists operations or drives a specific goal. This may consist of a distinct set of knowledge resources such as a server, software, andstorage devices arranged for the assembly, processing, treatment, application, sharing, dissemination, or constitution of information.

2.1.4. Change Management: A formal process to ensure that changes to a system are introduced, controlled, and coordinated. This reduces the possibility that unnecessarychanges will be introduced to a system, faults or vulnerabilities will be raised, or changes made by other users will be undone.

3. Disclosure of Company Data

The contractor shall not disclose Company Data in any manner that would lead to a violationof state or federal law or the terms of this Agreement, including, without limitation, using outsourcing, distributing, retransferring, or access, to any individual or entity, except:

3.1. Employees or agents who actually and legitimately need to access or use Company Data toperform Contractor’s duties to Company.

3.2. Such external mediators are approved by the Company in writing and in advance of anydisclosure, but only to the extent of such approval.

4. Usage Policy

The Contractor shall only use, store, or access Company Data in compliance with and only till the scope permissible under this Agreement. Any transmission, transportation, or storage of Company Data outside the [Region/State/Country] is prohibited except on prior written authorization by the Company.

5. Payment

The Company shall pay the Contractor as per the agreed amount. The payment will be made after the Company has sent the invoice. The Company will pay theService Provider within [number of days] days of the invoice date.

6. Safeguarding Company Data

6.1. The Contractor concurs that implementation, data storage, and access to Company Data shallbe executed with proficiency, care, and judgment in accordance with the general standards of quality adherence.

6.2. The Contractor shall implement and maintain the integrity of the Company Data.

6.3. The Contractor shall also implement and maintain any safeguards required to be implementedby applicable state and federal laws and regulations.

6.4. The System shall use secure protocols and encryption to safeguard Company Data in transit.

6.5. The Contractor understands that the System may be placed on a public network and shall implement safeguards reasonably necessary to protect its System from compromises and attacks.

6.6. The Contractor shall

6.6.1. Limit administrative access to the System

6.6.2. Limit remote access to the System

6.6.3. Limit permits and benefits to the minimum unless necessary for the proper functioningof company operations.

6.6.4. Withdraw or dismantle applications and services that are not needed for the properregulation of the system

6.6.5. Use official accounts and not shared accounts.

6.6.6. Use standard industry-compliant services for substantiation and authorization.

6.6.7. Facilitate an appropriate level of audit and log for the system and its applications.

7. Oversight

The Company reserves the right to request security information reasonably necessary to ascertain the Company's compliance with applicable rules and regulations.

8. Data Breach

8.1. If Contractor becomes aware that Company Data may have been accessed, disclosed, or acquired without proper authorization and contrary to the terms of this Agreement, Contractorshall bring this to the Company's notice within 6 hours, and shall process measures to preserve forensic evidence and eliminate the cause of the Data Breach.

8.2. The Contractor shall give the highest priority to immediately correcting any Data Breach and shall devote the resources as may be required to accomplish that goal.

8.3. The Contractor shall provide the Company information necessary to enable the Company to fully understand the nature and scope of the Data Breach, about what the Contractor has done or plans to do to mitigate any harmful effect of the unauthorized use or disclosure of, or access to, Company Data.

8.4. If a Data Breach requires the Contractor's assistance reinstalling software, such assistance shall be provided at no cost to the Company.

8.5. The Company may discontinue any services or products provided by the Contractor until theCompany, in its sole discretion, determines that the cause of the Data Breach has been sufficiently mitigated.

Annexure E

NON-DISCLOSURE AGREEMENT – UNDERTAKING*

I hereby accept the offer of <_____> to take part in consultancy services delegated assessments / assignments and undertake to comply with the following terms and conditions mentioned herewith:

1. Consultancy Services / Process

   I will perform the consultancy services / processes activities with true spirit, ethics and in accordance with the procedures and instructions of NABET, QCI.

2. Confidentiality

   I will not disclose to a third party any information of proprietary nature about the consultancy assignment bodies that I will get as part of the assignment, at any time even after leavingmy organisation.

3. Conflict of Interest

   I will declare to the authorities my association with any organisation in the past two years that can adversely affect the impartiality of the assignment processI shall also keep the authorities informed about the change in the status of my association with such organisations before every assignment.

4. Copyright of the Report

   The assignment report and the notes on assignment will be the property of the client entity and Iwill not disclose the same to any third party.

5. Breach of Conduct

   The client entity in its capacity can take any suitable action against me in the event of any breachof conduct or willful wrong information given by me.

6. Procedures, Rules and Regulation

   I shall maintain the “updated copy” of the procedures / documents of the contract and related documents, or any specific information provided by the client entity and shall abide by the procedures, rules and regulations as amended from time to time. I shall abide by the decision ofthe Head of the Client Entity.

7. Participation in Training or other activities of the Client Entity

   I shall make myself available to participate in the assessment as allocated and in the training andother activities organized by client entities specific to the assignment being undertaken.

Place: Signature (CO):_____
Date: Name
Seal

**This is a model contract; additional clauses may be inserted as per the COs‘internal requirements.*

SECTION 4

ACCREDITATION PROCESS

1. Background

1.1 Cyber Security of Critical Information Infrastructure has garnered importance in the recent times. CSEs are expected to comply with technical criteria of various strata in order to demonstrate the identified risks resolution capabilities, facilitating protection to their CII. This requires CSEs to obtain consultancy services to seek advice from experts to make their systems compliant. They look for COs which are reliable having competent consultants.

1.2 In view of the above, it is required to develop a credible Accreditation Scheme specifying the requirements for the accreditation of COs, operating in Cyber Security domain. The accreditation scheme has various components such as its Governance, Accreditation Criteria, Accreditation Process, Means of demonstrating accreditation (Rules for Use of Scheme Mark).

2. Scope

The scope of this document defines the lifecycle of activities associated with the accreditation process to be followed by COs imparting consultancy in the domains of cyber security.

3. Accreditation Process

3.1 Pre-requisite for Pre-Application Stage:

The requirements that an applicant CO should meet are defined in 'Section 3: Accreditation Criteria for COs'. The potential applicant shall study the same before initiating the application process.

3.2 Assessment Process

3.2.1 Application Process

a. Details of the accreditation scheme and the Application Form are available on the QCI - NABET website. Any institution/organisation desirous of acquiring accreditation, should assess their preparedness against the requirements and processes mentioned in the Scheme (accreditation criteria to identify the relevant shortcomings, if any, prior to applying

b. The duly filled Application Form in all respects should be sent as a soft copy along with the evidence of payment of the required fees). During application review by NABET, when necessary, the hard copy(s) of all relevant document(s) are to be made available.

3.2.2 Assessment Process

The Assessment life cycle comprises of three stages:

a. **Initial / Desktop / Office Assessment:** Completeness of application, technical evaluation of the submitted documents, access to the relevant infrastructure, resources, experts as part of the office review including knowledge and skill tests and interview with COs' expert(s) and concerned administrative staff to gain an understanding of the capabilities required for consultancy.

b. **Surveillance Assessment:** Same as stated above but with a brief assessment duration,

especial emphasis on the effectiveness of their engagements with CII clients to meet their IT/ICS cyber security requirements, timely delivery of the agreed scope including performance, quality of provided consultancy, up-to-date qualifications of the experts / consultants, compliance to accreditation conditions, carried out within 12 and 24 months of initial process of accreditation.

c. **Re-Accreditation**: Same as initial assessment, especial emphasis on the performance during the accreditation cycle, including client(s) feedback, after 3 years of initial accreditation.

3.2.3 Requirements for Initial, Surveillance and Re-accreditation

a. **Initial Assessment (IA)**

i. Application Completeness: Submitted application shall be reviewed by NABET's Secretariat for its completeness. Inadequacies in the application (if any) shall be informed to the applicant organisation. COs should submit their response(s) to the inadequacies within 30 days. Only applications which are in due compliance shall be further processed. COs should submit the filled self – assessment report in the format shared by NABET's Secretariat at the time of acceptance of application.

If inadequacies are found in the response(s), the same shall be communicated and an additional time of 30 days will be allotted to COs to respond. If COs fails to submit a satisfactory response in the allotted time, then the application may be considered inactive. The inactive period shall remain for 60 days. The COs may choose to reapply with the due payment of the requisite fees after this period.

ii. Desktop Assessment: NABET's assessor(s) conduct adequacy assessment(s) (application & technical assessments of documents submitted by COs). The Observation(s) and non-conformities (NCs), if any, shall be communicated by NABET Secretariat to the applicant CO(s). CO(s) shall have a time frame of 30 days to submit their response(s). Closure of NCs and Observations submitted by COs shall be verified by NABET assessors.

iii. Office Assessment: Post the review and acceptance of the documentation, and procedures submitted by the COs, NABET shall undertake full assessment at COs premises. It shall include interaction with each expert (in house and visiting)/ quality manager, concerned administrative staff etc., verification of infrastructure, implementation quality assurance system and client's feedback. Assessment reports[findings like observation(s) and NCs (if any)] shall be conducted by NABET assessors (placed at NABET Secretariat) and in turn be communicated to COs. Corrective measures shall be submitted by COs within 30 days. All COs assessment reports shall be reviewed by NABET Secretariat and forwarded to Accreditation Committee for the grant of accreditation. Decisions regarding grant/denial of accreditation would be communicated to COs by NABET Secretariat. NABET will conduct tests of requisite knowledge and skills required by experts in their specific fields, against which the COs have applied to provide consultancy.

'Accreditation Criteria for COs' document shall be used as reference while conducting desktop assessments and office assessments.

iv. Closure of NC's and Observations submitted by COs shall be verified by NABET assessors.

v. In cases when an applicant CO having branched offices, its assessment shall be conducted

during the Initial Assessment phase.

b. Surveillance Assessment (SA)

The SA shall be completed within 1 year of the Initial Assessment. It is, therefore, mandatory for the COs to apply for SA within 10 months post the IA is conducted, in order to complete all the SA formalities in the 1st year, starting from the date the grant of IA was achieved.

In cases when a change is brought to the list of experts, team composition, quality manual, infrastructure, modification of scope, etc., then the applicant shall submit the updated details along with the applicable fee to the NABET Secretariat. NABET Secretariat shall review the documents and proceeds, submitted by the applicant organisation, in due accordance to the specified process of surveillance assessment.

SA shall be conducted with particular emphasis on the performance, quality of consultancy delivery, client's feedback, implementation of CQAS and compliance to conditions of accreditation. The SA shall include the evaluation of documents as well as site visit(s).
In cases for an applicant CO having branched offices, the SA shall cover each one on a risk-based sampling method.

c. Re-Accreditation (RA)

The procedure is similar to initial assessment, where particular emphasis is given to the performance, clients' feedback, etc. The RA requires completion within a period of 3 years, starting from the date of accreditation. The RA application is to be submitted 3 months prior to the expiration date of the issued accreditation certificate. The RA process requires completion before the accreditation's date of expiry in order to avoid any form of discontinuation to the same.
Extra Visit (based on requirement): On the basis of risk factors, retrieved information / complaints from primary or secondary source, etc. surprise visit(s) / extra visit(s) may be planned and the nature of it could be unannounced or announced (as applicable to the case).

3.3 Criteria for Granting Accreditation

Desktop Assessment (DA), reporting by assessor(s) and satisfactory closure of NCs and Observations, and Office Assessment will be conducted by NABET assessor(s). Based on the office assessment report, NCs and Observations, if any, the necessary closure and compliance shall be communicated to the COs. The COs are required to submit evidence-based compliance of NCs and Observations not later than a month's period (30 days). If required, additional office(s) and witness(es) assessment shall be conducted in order to verify evidences for closures.

The accreditation period is of three years and shall be taken into consideration from the date of grant (of accreditation) by the Accreditation Committee (AC); however, the validity period is subjected to the satisfactory status of Surveillance Assessment (SA). Accreditation, under this criterion, shall be granted only against the fulfilment of all of the following stated conditions:

3.3.1 Submission of application with the requisite document(s)
3.3.2 Closure of all NCs at the DA stage
3.3.3 Successful completion of OA and closure of observed NCs, in the allotted time and as per the

satisfaction of the assessing team

3.3.4 Approval of accreditation by the NABET Accreditation Committee

4. Terms & Conditions to maintain accreditation

4.1 Compliance to the Conditions of Accreditation

4.1.1 Accreditation period of three years shall be counted from the date of grant of accreditation by the AC.

4.1.2 Accredited COs should submit annual reports and complete SA/RA application(s) three months prior to the due date (12/24/36 months from the date of accreditation) to maintain the accreditation.

4.1.3 Accreditation shall expire at the end of its validity unless renewal is sought as per the defined time.

4.1.4 All payments shall be made in advance.

4.1.5 Franchising, licensing, subcontracting of NABET Accredited COs is NON – permissible.

4.1.6 COs should submit a six-monthly report about the CSE's consultancy projects along with their status and the list of approved experts involved in the same.

4.1.7 Any change(s) subjected to list of experts, employment status, scope, etc. shall be informed to NABET within 10 days along with the relevant documents.

4.1.8 After acquiring 'Accredited' status, COs are required to sign the 'Code of Conduct' and send it to NABET Secretariat.

4.1.9 The accredited COs shall maintain relevant records for each of the consultancy projects conducted / provided.

4.1.10 The accredited COs are required to share the list of consultants with NABET, which NABET/QCI may choose to display on its website.

4.2 Suspension / Withdrawal of Accreditation

NABET may suspend or withdraw its accreditation on account of any one or more reasons during the accreditation cycle. The following list of clauses are the grounds for suspension / withdrawal:

4.2.1 Non-compliance, violation of the QCI / NABET requirements and conditions ofaccreditation.

4.2.2 Deviation from facts as stated in application and enclosures.

4.2.3 Submission of false or misleading information in the application or in subsequent submissions.

4.2.4 Improper use of NABET accreditation logo and Scheme Mark.

4.2.5 Carrying out changes in expert's/ quality procedures without NABET's approval

4.2.6 Failure to report any major legal (mandatory compliance) changes.

4.2.7 Using fraudulent practices by the accredited CO in respect of its submission/ interaction with NABET / QCI including, but not limited to, deliberate concealment and/or submission of false or misleading information, suppression of information, falsification of records or data, unauthorized use of accreditation, and non-reporting of complaints against COs to NABET / QCI.

4.2.8 Non- payment of applicable fees in timely manner to NABET / QCI.

4.2.9 Non- submission of SA/RA application in allotted time.

4.2.10 Franchising, licensing or subcontracting of consultancy / programs.

4.2.11 Any other condition deemed inappropriate by NABET / QCI.

4.3 Code of Conduct

All accredited COs are obliged to facilitate improvements in the professional standings by rigorous observation of the Code of Conduct. Failure to do so may result in the suspension or cancellation of accreditation.

The accredited COs are obligated to committed to the following conditions:

4.3.1 To act professionally, accurately and in an unbiased manner.
4.3.2 To be truthful, accurate and fair while conducting assigned work, without any hesitation or favourism.
4.3.3 To judiciously use the information provided by or acquired from the applicant, and to maintain confidentiality of information which is received or acquired in context with the assignment.
4.3.4 To avoid and/ or declare any conflict of interest that may affect the functionality of the work to be conducted.
4.3.5 Not to act in a detrimental manner which would hurt the reputation of the stakeholders, including NABET / QCI.
4.3.6 To fully co-operate in a formal procedural enquiry of NABET / QCI.
4.3.7 Not to employ active/involved NABET assessors. Any person involved in conducting assessments for NABET should not be hired as a Consultant with the COs for the domain of Cybersecurity(IT & ICS).

4.4 Complaint and Appeals

4.4.1 The accredited COs shall strive to establish documented procedural handling and disposal of complaints and appeals, within a reasonable time frame. The documented procedures shall include provisions for:

a. Providing information regarding complaint handling process to all the interested parties
b. Acknowledgement of complaints
c. For redressal of complaint/appeals.
d. Communication with the complainant/appellate for satisfactory closure of the complaint.
e. Involvement of NABET in unresolved complaints or appeals, if any.

4.5 The accredited COs shall strive to maintain records of all complaints & appeals, and also provide for their resolutions within a reasonable time frame.

4.6 All complaints and appeals are to be made assessable for NABET assessments.

4.7 Payment of Fee

The CO shall abide by the all commercials as applicable.

4.8 Governance

NABET / QCI reserves the rights with respect to accreditation scheme for COs for Cybersecurity (IT & ICS). NABET / QCI shall adhere to the following functions (but not limited to) in consultation with NCIIPC (Scheme Owner):

4.8.1 Changing/ modifying the criteria/ guidelines/ fee structure.
4.8.2 Suspension/cancelling of accreditation in case of violation of any clause of the Scheme.
4.8.3 Surprise visits/ extra witness assessments.

4.9 Confidentiality

4.9.1 All information, documents submitted by an applicant to NABET shall be used by NABET (including NABET Assessors and Members of Accreditation Committee) for the purposeof assessment & accreditation only. These may also be used for study/ research purpose or sharing with any ministry and other appropriate agency. However, the identity of the accredited CO would be protected for sensitive information related to business wheneverappropriate. In cases when a CO wants the information to be kept confidential, it shall be communicated to NABET citing the reasons for the same. NABET reserves the right to decide in such matters.

4.9.2 Accredited CO shall have adequate arrangements consistent with the applicable laws to safeguard confidentiality of all information provided by stakeholders.

4.9.3 The accredited CO should maintain confidentiality of their client-related information like location, products, processes, vendors, feedback form, personal details, etc.

SECTION 5

RULES FOR USE OF SCHEME MARK

1. Introduction

1.1 The accreditation scheme for COs is designed and developed as per best international practices.

1.2 The 'Scheme Mark' denotes the assigned mark to the accredited COs.

The 'Scheme Mark' is allowed to be used for promotional purposes only by accredited COs, who are authorized to display the mark in off-product(s) in alignment to the prescribed rules mentioned in the subsequent paras of the document.

1.3 Further, it is the collective responsibility of the NCIIPC, QCI and its constituent accreditation boards for keeping an oversight on the usage of 'Scheme Mark'.

2. Purpose

QCI and its constituent accredited boards may so be benefitted from visually identifying their status through the use of the 'Scheme Mark'. In doing so, the Mark Holders are provided guidance in a manner that requires organisations displaying the mark to desist from misleading anyone; to avoid positioning of incompatible marks that may lead to devaluation or degradation of other marks; to avoid their usage in violation to the associated legalities (protected under trademark rules); or to avoid their usage in contradiction to the recognised Scheme.

3. Objective

3.1 This document establishes rules for the use of Scheme Mark.

3.2 This document enlists the conditions that must be adhered by the accredited COs, permitted to use the logo and/or symbols.

3.3 This document establishes the process required to be adopted by the Scheme for granting the use of Scheme Mark to accredited COs.

4. Scope

4.1 The scope covers all the authorized Mark Holders.

4.2 This document covers the rules for use of the Mark and defines the misuse scenarios with respect to the requirements of the Scheme.

5. Prerequisites for Use of Scheme Mark

5.1. Organisations declared as Entities in the scheme:

5.1.1. Only the approved Mark Holders under the Scheme, are eligible to use Scheme Mark. An application is required to be submitted for getting authorization for the Use of Scheme Mark (refer to Annex A of this section).

5.1.2. As per the contract between the QCI and the Mark Holder, the Mark Holder shall be required to formally sign an agreement with QCI for the use of Scheme Mark. This shall be done immediately after the grant of approval.

5.1.3. The accredited COs, shall make provision in their management system to institutionalise this requirement for it to be legally enforceable.

6. Oversight Responsibility

6.1 The QCI secretariat in consultation with NCIIPC, is responsible to establish, implement and amend this procedure after approval from various committees like TC, CC, SC, etc. The Mark Holder are responsible to comply with the procedure, specifically undertaking surveillance or re- accreditation.

6.2 The Mark Holder should establish a strong market surveillance system for ensuring sustained compliance at all times.

6.3 By affixing the Mark, the Mark Holder commits to abide by the rules for use of Scheme Mark which should be independent of the oversight process.

7. Rules for Use of Scheme Mark

7.1 The Mark Holder(s) need total compliance with the applicable criteria.

7.2 The Scheme Mark is only allowed to be used by accredited COs.

7.3 For the purpose of promotional work, the marks may be used by the accredited COs. However, the same shall not be allowed to use while issuing consultancy documents to their clients.

7.4 In some cases, if a Mark Holder has acquired marks from different Scheme, he/she is required to seek prior approval(s) explicitly from QCI for affixation of multiple marks.

7.5 Mark Holder(s) who have been subjected to important changes or overhauls, and aim to modify the original mandate (post due approvals are secured), must apply de novo.

7.6 The Scheme Mark may be used as any photographic reduction or enlargement. The colour scheme used for the Marks should be same as described below. Varying combinations of colour scheme are not permitted.

7.7 During photographic reduction and enlargement of the Mark Scheme, sufficient care has to be exercised to ensure that no deviation exists while maintaining the ratio and colour coding.

7.8 The Mark Holder, upon suspension or withdrawal of its attestation, shall discontinue the use of the Scheme Mark, in any form.

7.9 The Mark Holder, upon suspension or withdrawal of its attestation, shall discontinue the use of all advertising materials that may contain any reference to its attestation status.

7.10 In case the Scheme Mark is observed to be used in contravention to conditions specified, suitable actions shall be taken by the approving body in accordance with the relevant requirements of Scheme, and those specified in the document “Accreditation Process”.

7.11 Depending upon the degree of violation, suitable action(s) may be taken up ranging from advice for corrective actions, to withdrawal of accreditation, especially in cases of repeated violations. In case the Mark Holder denies to take suitable action(s) for redressal of wrong usage of the Scheme Mark, QCI is authorized to issue suspension/withdrawal of its accreditation.

7.12 In cases when Mark Holders' accreditation is suspended/ its attestation cancelled, withdrawn or discontinued, it is responsibility of the Mark Holder(s) discontinue any future use of the Scheme Mark, post the date of accreditation suspension, cancellation and/or withdrawal or discontinuation has come into force. QCI, the Scheme Manager that has approved the use of Scheme Mark to the Mark holder, needs to ensure compliance as stated above.

7.13 The Mark Holder(s) has to sign a legally enforceable agreement with the QCI, only after which the use the Scheme Mark shall be allowed, after agreeing to all the relevant conditions as described in this document.

7.14 The Mark holders shall pay an annual fee to QCI, through their operational entities for the use of Scheme Mark as prescribed from time to time. This payment shall be made to its approving Mark holder for onward submission to QCI.

7.15 Misuse scenarios

7.15.1 The Mark should not be used while making a statement related to out-of-scope entities.

7.15.2 The NCIIPC's, QCI's and its constituent boards' logos/Marks are not permitted to be used by the Mark Holder. If required for temporary events such as collaborative training program, etc., a written permission needs to be sought from the respective organisation.

7.15.3 The Mark Holder shall desist from misleading anyone; avoid positioning of incompatible marks that may devalue or degrade other Marks; use them illegally (they are protected trademarks); or use them contrary to the recognised Scheme.

8. Conditions for use of Scheme Mark by COs

Following conditions shall apply for the use of Scheme Mark

8.1 The Scheme Mark(s) may be used in published material(s) such as pamphlet(s), letterhead(s), etc. for communication purposes or promotions or spreading awareness of the Scheme/the Scheme Mark, etc.

8.2 While using the above-mentioned documents, it should be ensured that the Mark only should be used in respect to the Mark Holder(s) and should not give the impression that the non-certified, other than scope of Scheme, locations/personnel from offices are not included in scope or a related companyare also certified/attested.

8.3 The Mark Holder(s) is not permitted to make any misleading claims in respect to the Scheme Mark.

8.4 The Scheme Mark(s) shall not be used in a manner which brings the Scheme Owner (NCIIPC) or QCI, any disrepute.

9. Conditions for Use of the Scheme Mark by COs (accredited COs)

9.1 The Scheme Mark shall be displayed only for domain for which COs has been accredited. The clients / consultants are not permitted to use or display the Scheme Mark elsewhere.

9.2 The consultants shall abide by all clauses as mentioned in Annex B of this section once certified, committing to the requirement of the Scheme through their accredited COs.

9.3 Once the Mark Holder is accredited by the QCI, it shall seek the clients / consultants to fill up in duplicates – the contractual form (enclosed as a template mentioned in Annex A of this section).

9.4 The accredited COs shall forward the filled contract form to QCI, for the purpose of signing and completing the contract formalities. Along with the contract form, the relevant conformity assessment body shall also forward the details of the Mark Holder, covering the following information as a bare minimum:

9.4.1 Name and address of the Mark Holder;
9.4.2 Legal entity Status (with evidence);
9.4.3 Names of the top management/ownership details;
9.4.4 Details of the consultancy granted – number, validity, etc.;
9.4.5 Scope of consultancy granted to the Mark Holder;
9.4.6 Any other significant detail(s) considered as relevant.

9.5 The consultants are required to submit an undertaking to the respective accredited COs for abiding by the Rules for Use of Scheme Mark.

9.6 Upon receiving the signed contract form from QCI, the attestation body shall be responsible for the issuance of the certificate, informing the Mark Holder(s) regarding the permissible use of the Scheme Mark, and to forward the signed contract form to them.

9.7 The contract validity between QCI and the Mark Holder, shall be for the period until the later holds valid accreditation under the Scheme or if is otherwise advised to do so.

10. Design of the Mark

Only the Scheme Mark mentioned below, shall be allowed to be used by the accredited COs, while issuing the statement of conformance.

GRAY: C-43, M-33, Y-35, K-2
BLACK: C-66, M-65, Y-60, K-56

Annexure A

Format for Application

APPLICATION FOR PERMISSION TO USE THE SCHEME MARK

1	**Name of the accredited CO**	
2	**Address**	
3	**Telephone No.**	
4	**Mobile No.**	
5	**Email**	
6	**Purpose of Usage**	
7	**Name of Mark Holder (for which Scheme Mark is to be applied)**	
8	**Signature and Date of authorised QCI personnel**	

Annexure B

Format for the agreement between QCI and the Mark Holder for use of Scheme Mark (Only for accredited COs)

AGREEMENT FOR USE OF SCHEME MARK

M/s_____(hereinafter referred to as **Mark Holder**) situated at_____has applied to M/s. Quality Council of India, 2nd Floor, Institution of Engineers Building, 2, Bahadur Shah Zafar Marg, New Delhi - 110002, India (hereinafter referred to as **QCI**), for permission to use **Scheme Mark** for the offices for which it has received accreditation from the ……
(name of approving/CAB) approved by QCI under the Conformity Assessment Framework for Cyber Security of Critical Sector Entities (hereinafter referred to as the **Scheme**) owned by the **QCI.** This agreement is entered in connection with granting of permission to use the Scheme Mark by QCI under the following terms and conditions agreed upon:

1. GENERAL CONDITIONS

1.1. The Mark Holder agrees to comply at all times with the requirements of the Scheme as applicable presently and as amended from time to time. The Mark Holder shall also agree to pay the annual fee to QCI.

1.2. The Mark Holder shall agree to comply with conditions of the accreditation as per its contract with QCI.

1.3. This Scheme aims to certify the Mark Holder for their ability to meet the applicable Scheme requirements.

1.4. The Mark Holder may use the Scheme Mark in publicity material, pamphlet, letter heads, other similar stationary; media for exchange of any communication, for promoting the awareness of the Scheme, the Scheme Mark, etc. The Mark Holder may also use the Scheme attestation issued by the conformity assessment body as part of publicity material. The Mark Holder, however, agrees to take care, while using the above documents to ensure that the Mark is used only with respect to the Mark Holder and it shall not give impression that the non-attested, other than attested scope, offices not included in scope or a related company are also carrying the Mark.

1.5. The Mark Holder agrees to use the Scheme Mark only with respect to the Mark Holder covered under accreditation granted to it and will continue to comply with the accreditation criteria.

1.6. The Mark Holder agrees that it would always fulfil the accreditation requirements as per the existing Scheme and as modified from time to time and shall use the Scheme Mark only during the validity period of the certificate and when its QCI approval is valid.

1.7. The Mark Holder agrees not to make use of the **Scheme Mark** or name of QCI which could be misleading or unacceptable to QCI.

1.8. The Mark Holder agrees to make claims of accreditation only for the scope which are specifically covered under accreditation.

1.9. The Mark Holder agrees not to use the marks in such a manner that would bring QCI or the Scheme into disrepute and/or lose public trust.

1.10. The Mark Holder agrees to inform QCI in writing of any significant changes in the Mark Holder's name, ownership or location for which the Mark Holder has obtained the accreditation.

1.11. The Mark Holder shall inform QCI, without delay, of matters that may affect its ability to conform to the accreditation requirements.

1.12. The Mark Holder agrees to provide any information sought by QCI regarding operation of the Scheme by the Mark Holder.

1.13. The Mark Holder agrees that its name, location and the scope of accreditation is included in the directory maintained and published by QCI.

1.14. The Mark Holder agrees for the conduct of announced/ unannounced / decoy assessments in order to verify the compliance of the Mark Holder with reference to the use of the Mark as allotted to it and with respect to the complaints received by QCI about the Mark Holder and to pay such charge within the time as communicated by QCI.

1.15. The Mark Holder agrees to discontinue the use of the Scheme Mark from the date from which the certificate stands suspended, cancelled, and withdrawn or discontinuation comes into force.

1.16. Upon suspension or withdrawal/cancellation of its accreditation, the Mark Holder shall discontinue use of all advertising material referring to the use of Scheme Marks with immediate effect and submit a declaration to this effect to QCI. It shall also refrain from making claim in any form regarding the accreditation under the scheme.

2. OTHER REQUIREMENTS

2.1. This agreement is entered for a period of the validity of the accreditation and shall be in force from the date of signing of this agreement.

2.2. All correspondence of QCI shall be in writing and shall be deemed to have been served/made when sent by courier/registered post or facsimile or email to the address of the Mark Holder as mentioned on the company information sheet or any change as subsequently communicated to QCI by the client in writing under QCI acknowledgement.

2.3. In case of any disputes/issues, Mark Holder agrees to go through the appeal procedure under the Scheme and accepts its decision as final.

2.4. Mark Holder agrees to indemnify QCI in case of any loss or liability incurred by QCI in connection with the Scheme or misuse of mark(s) by the Mark Holder.

2.5. Disputes, if any, arising out of the terms and conditions of the agreement between QCI and the Mark Holder, shall be governed by laws of India and subject to the jurisdiction of competent courts located in Delhi.

2.6. Mark Holder shall nominate the chief executive or an authorized signatory for the agreement as the point of contact with QCI.

The Mark Holder hereby accepts and agrees to the above terms as documented in this agreement.

1. **Signature :**

Name of Mark Holder: _____

(the chief executive of the organisation or an authorized signatory)

Title : _____

Address : _____

_____

_____

Date : _____

2. **Quality Council of India**

QCI hereby accepts the above application and agrees to the terms thereof.

Authorized Signatory: _____

Name : _____

Title : _____

Date : _____