Issue No. 1.
Feb 2024

NCIIPC – QCI Initiative

Conformity Assessment Framework for Cyber Security of Critical Sector Entities (CAF_CS_CSE)

Accreditation Scheme for IT/ICS Training Bodies (TBs)

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 document details the requirements for accreditation of IT/ICS Training Bodies herein after referred to as TBs**.**

ACKNOWLEDGEMENT

Quality Council of India (QCI) would like to thank NCIIPC (a unit of NTRO) 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 cyber security 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 assessment documents 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, PADD, in terms of his dedication, commitment and hard work. 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	Sh. 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. Praveen Kumar Goyal	Noida Power Company Limited
9	Sh. Ashutosh Bahuguna	Indian Computer Emergency Response Team
10	Prof. Faruk Kazi	Veermata Jijabai Technological Institute
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	Sh. 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 To enhance the confidence of the cyber security of Critical Information Infrastructure (CII), it is imperative to equip the professionals working in Critical Sector Entities (CSEs) with required knowledge and skill-sets. An extensive training in Cyber Security is essential in today's digital world to combat the growing threats to critical assets in any Information Technology (IT) and Industrial Control System (ICS) environment.

1.2 This necessitates a nationwide programme on capacity building in entire cyber security ecosystem. There are many training institutes that offer comprehensive programs and certifications to help these professionals in augmenting their skills and expertise in cyber security. These training institutes and their certifications cater to different knowledge and skill levels aligned with varied career goals among professionals. It's desirable to assess one's specific needs and objectives before selecting a training program from the list of offered courses. Additionally, being at par with the latest developments in cyber security through continuous training is crucial for marking a successful professional transition.

1.3 Training bodies (TBs) as a part of this Scheme will provide the training and hands on requirement related to various specialised domain of cyber security and help CSEs to implement Cyber Security Management System (CSMS) through competent trained professionals by TBs. The TBs working in this area have an important role to play in cyber security ecosystem both as a knowledge and competence center for building capacities as well as to address the challenges faced by the CSEs.

1.4 Interested CSEs that wish to obtain the CSMS certification struggle to get proper direction, and technical guidance to stand out among their competitors. They indulge in an evasive exploration of competent and recognized TBs. It is known fact that, at present, our education system does not address implementation of the requirements specified in the global standards in the field of cyber security. This necessitates to strengthen a mechanism of recognition of competent and reliable TBs.

1.5 There is an emergent need to put in place a system of oversight and due diligence so that only bonafide TBs impart training to the potential trainees to ensure both qualitative and quantitative training service delivery in different cyber security domains.

1.6 In view of the above, and to cater to the existing market necessity, a national accreditation Scheme is designed and developed detailing the requirements for accreditation of IT/ICS Training Bodies hereinafter referred to as TBs. This Scheme will provide confidence to the users of cyber security training services that their services are credible and dependable.

1.7 This Scheme will enable the TBs to impart knowledge and skill set through various training modules which are aligned to national and international standards. The Scheme also aims to supplement the requirements of recognition of Cyber Security Professionals where competency profiles are developed for various cyber security domains and evaluation of a candidate's professional knowledge and skills is carried out through an examination and review process.

1.8 The designing of the accreditation Scheme involves establishing accreditation criteria, process and related lifecycle activities.

1.9 This document introduces a framework which will assist the CSEs to establish a resilient CSMS and other technical support in the whole life cycle of the system concerning cyber security issues while maintaining acceptable system performance, cost and reliability. This will come in force by enhancing the abilities of their professionals to implement various processes and controls which are necessary and sufficient as well as mechanisms which are correct and reliable.

2. Objective

The objective of this document is to define Accreditation Scheme for TBs to:

2.1 Ensure that the training processes and infrastructure of TBs are aligned with the requirements of Personnel Certification Bodies (PrCBs) Scheme;

2.2 Facilitate CSEs to develop training plan for strengthening knowledge and skill of their workforce and implement the same by availing the services of accredited TBs as competence center.

2.3 Help individual professionals to enhance their potential and ability by acquiring knowledge and skill in the area which requires augmentation for compliance with competency profile(s) of their interest and need.

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 ISO/IEC 27000 and IEC 62443 its family of standards. In case of any differences in terminology the definitions in the IT 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 **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.

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

5.5 **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.

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

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

5.8 **Complaint** - Expression of dissatisfaction, other than appeal, by any person or organization to a conformity assessment body or accreditation body, relating to the activities of that body, where a response is expected.

5.9 **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.

5.10 **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.

5.11 **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.

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

5.13 **Cyber Security** - Safeguarding of people, society, organizations and nations from cyber risks. The objective of adequate cyber security 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, cyber security aims to reduce cyber risks to a tolerable level.

Areas of concern for cyber security include:

5.13.1 Stability and continuity of society, organisations and nations.

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

5.13.3 Human lives and health.

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

5.15 **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.

5.16 **Cyberspace Security** - Reservation of confidentiality, integrity and availability of information in Cyberspace.

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

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

5.19 **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.

5.20 **Information Technology** - Technology (computer systems, networks, software) used to process, store, acquire and distribute information.

5.21 **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

5.22 **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.

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

5.24 **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 training bodies as the specialized professional bodies excluding its client base.

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

5.26 **Operational Technology -** Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices and systems, processes and events in the organization.

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

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

5.29 **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

5.30 **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 aligning it with the international requirements the same will henceforth be referred to as the “Mark”.

Note: A conformity assessment Scheme under NCIIPC-QCI initiative for CABs {Certification Body (CB), Inspection Body (IB), Personnel Certification Body (PrCB)}, organisational entities {Critical Sector Entity (CSE), Consultancy Organisation (CO), Training Body (TB)}, and individuals {Cyber Security Professionals (CSPs)}.

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

5.32 **Stakeholder** – A person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity.

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

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

5.35 **Trainee- Person engaged in training-** Beneficiary acquiring and developing competence using an educational service (Source: ISO 21001:2018)

5.36 **Training -** Acquiring knowledge, behavior, skills, values, preferences or understanding

5.37 **Training body -** Organization of any size or individual providing training services, including any associates involved in the provision of the training service

5.38 **Training Resource -** Material, environment, human resource, information or other asset that can be drawn on by the training service provider in order to facilitate training effectively.

5.39 **Training Service -** Processes or sequence of activities designed to enable training

5.40 **Training Management System -** Training management system (TMS) is defined as a formalized system that documents processes, procedures, and responsibilities for achieving quality policies and objectives for conducting various training courses/programs and enables the organization to ensure adhering to it to achieve desired results.

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

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

5.43 **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
ABAC	Attribute-based access control
AC	Accreditation Committee
BIS	Bureau of Indian Standards
CAB	Conformity Assessment Body
CAF	Conformity Assessment Framework
CB	Certification Body
CC	Certification Committee
CCMP	Cyber Crisis Management Process
CERT-In	Indian Computer Emergency Response Team
CII	Critical Information Infrastructure
CMMI	Capability Maturity Model Integration
CO	Consultancy Organisation
CSA	Cyber Security Agency
CSE	Critical Sector Entity
CSMS	Cyber Security Management System for IT/ ICS
DA	Desktop Assessment
FDP	Faculty Development Program
FIPS	Federal Information Processing Standard
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
ISO	International Organisation for Standardisation
IT	Information Technology
JSON	JavaScript Object Notation
KM	Knowledge Module
LAN	Local Area Network
MSC	Multi-stakeholder committee
NABET	National Accreditation Board for Education and Training
NCIIPC	National Critical Information Infrastructure Protection Centre
NDA	Non-disclosure Agreement
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
PBX	Private Branch Exchange
PLC	Programmable Logic Controller
PrCB	Certification Body for Persons
QCI	Quality Council of India
QMS	Quality Management System
RA	Re-Accreditation
RBAC	Role-based Access Control
RFP	Request for Proposal
SA	Surveillance Assessment
SAML	Security Assertion Markup Language
SC	Steering Committee
SCADA	Supervisory Control and Data Acquisition
SM	Skill Module
SO	Scheme Owner
SPML	Services Provisioning Markup Language
TB	Training Body
TC	Technical Committee
TDP	Trainer Development Program
TMS	Training Management System
TOR	The Onion Router
WA	Witness Assessment
WAN	Wide Area Network

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 organizations 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 the 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 the activity and the criteria selected for the approval of the IT/ICS Training Bodies.

2.2.4 Ensure that the Scheme documents, including the criteria and process to assess activities pertaining to accreditation of TBs, 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 IT/ ICS TBs to ensure that the TB 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 IT/ ICS TBs to provide reasonable access and cooperation as necessary to enable the QCI assessment team, which includes assessors, technical experts, observers, and regulators to assess conformity with the Agreement and 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 IT/ ICS TBs are processed expeditiously. Investigation and decision on complaints shall not result in any discriminatory actions.

Note 1: 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 TBs' clients, 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 organizations 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.

2.2.13 The Scheme Manager shall brief the Steering Committee for activities pertaining to the Scheme.

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.

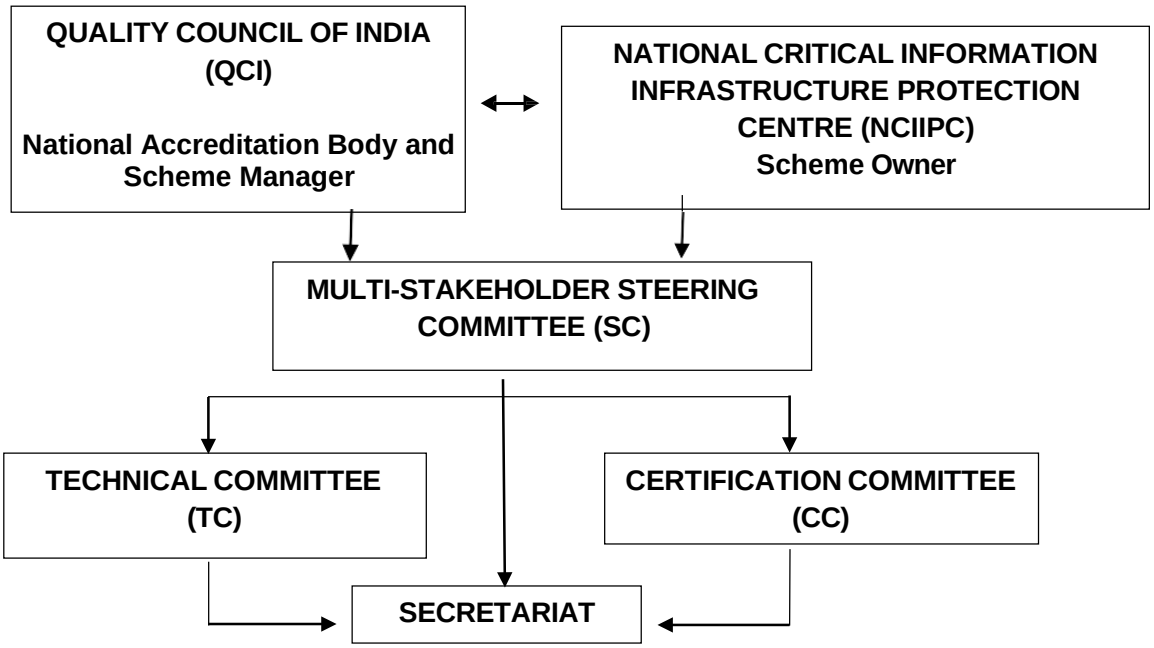

Figure 2.1: Governing Structure

3.3 Appointment of Committees – General Rules

In the appointment of various committees, the following general principles shall be kept in 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, consultancy organisations, training bodies, testing laboratories, user associations, academic/ research bodies, manufacturers of products, providers of services and representatives of organizations 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 organization.

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

3.3.5 The member organizations 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 organizations by rotation, wherever necessary.

3.3.7 While there would be organisations as members with a definitive term, the Secretariat may call 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 & Public Enterprises and Healthcare, representatives 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**

4.2.1 The SC is responsible for the following:

4.2.2 Overall development, modification and supervision of the Scheme.

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

4.2.4 Constituting any committees as needed.

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

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

4.2.7 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 stakeholder groups:

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/ Training bodies 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 Defining the criteria for IT/ICS Training Bodies w.r.t essential knowledge and skills for different expertise levels in different Cyber security domains.

5.2.3 Providing direction and guidance on the knowledge and skills that are required for each Cyber security domain and expertise level for IT/ICS TBs.

5.2.4 Providing direction and guidance on the appropriate technical assessment methodologies for accreditation criteria for IT/ICS TBs.

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

5.2.6 Defining and formulating the technical requirements of the Scheme.

5.2.7 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 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

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 TBs as per the defined scope.

6.2.3 Developing, maintaining, and revising as appropriate the documents for TBs 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 TBs.

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 Organizations

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 who will manage and operationalise the Scheme as per the established norms on behalf of Scheme Owner. It shall establish the MSC in consultation with 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 TBs desirous of participation in the Scheme. NABET shall, through a legally enforceable agreement with the accredited TBs, ensure that the TBs 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 TBs 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 organization to a TBs 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 TBs 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 a TBs or AB for reconsideration of a decision made by that body.

9.2 Provisions for addressing appeals from the applicant/ certified persons/ accredited TBs 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 In handling appeals, the broad principle that the appeal is handled independently, of the personnel involved in the 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 TBs 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 Training Bodies (TBs), for training CyberPros necessary to critical sector ecosystem including rendering training services to the critical sector entities, and others, all termed as client or client entities in the area of cybersecurity. The IT/ICS Training Bodies, for the purpose of this document, are termed as TBs. They shall need to comply with all the accreditation criteria prescribed in the Scheme. In order to be formally accredited by the accreditation body, the training body, even if already accredited to any similar international standard, would need to undergo an office assessment and a witness assessment and actual evaluation under the Scheme. All requirements of these criteria are generic in nature and are intended to be applicable to all TB, regardless of type, size, nature and sector.

1.2 The objectives of accreditation criteria are as follows:

1.3 To enable the TBs to define and implement their learning management system for providing training services as per the scope defined in this document.

1.4 To enable TBs to follow a set of 'Accreditation Criteria' for demonstrating their competence in terms of processes, personnel and technological requirements for the scope of training services being offered by them.

1.5 To assist assessors with a reference document for carrying out assessment activities related to accreditation of the TBs in a harmonised way across various TBs.

1.6 To enable training bodies to design their training programme which will assist the CSEs to obtain certifications as per CSMS certification Scheme requirements.

2. Scope

This document specifies the accreditation requirements to be implemented by Training Bodies that wants to offer one or more of the training services for accreditation under the scheme.

3. Intended Stakeholders

3.1 TB providing/supplying training services.

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

3.3 Cyber Security Professionals for acquiring knowledge to foster his technical acumen.

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 TBs.

4.1. Normative references

4.1.1 IS/ISO 9001:2015 - Quality management systems – Requirements
4.1.2 IS/ISO/IEC 21001:2018 - Educational organisations Management systems for educational organizations - Requirements with guidance for use

4.2. Informative References

4.2.1 IS/ISO/IEC 10015: 2015 - Quality Management - Guidelines for Training
4.2.2 Personnel Certification Scheme for IT and ICS Cyber Security Professionals

5. Document Structure and Approach

The dynamic landscape of cyber-security of IT and ICS systems and infrastructure requires a substantial depth and breadth of knowledge, expertise and skills to comprehend risks (threats and consequences) that may potentially impact organisations and society at large. To keep pace with rapidly changing developments in these areas, the client entities look for accredited TBs so that they acquire knowledge and skill from accredited TBs. The accreditation criteria for TBs are structured based on the following three principles:

5.1 **Fulfilment of client requirements:** CyberPros are satisfied with the training services which are as per their agreed scope of technical requirements.

5.2 **Deliverables to the client:** Services, as per the domain requirements of the competency level (Foundation / Advanced / Master) chosen , are delivered in a structured manner which combines both theoretical and practical hands on approach, follow code of ethics while in line with changing cyber security environment / technology.

5.3 **Competence of trainers of TBs:** The capability and technical competence of the training provider, access to / availability of the relevant IT/ICS security tools and cyber security of IT and ICS and infrastructure shall be up to date and in accordance with the services offered.

This document has been structured on the above three principles, which TB will follow while imparting its training services. The accreditation criteria for TB primarily comprise of following components which are described in para 6 of this section:

- Organisational Requirements
- Process Requirements
- People Requirements
- Technological Requirements

6. Accreditation Criteria for TBs

These requirements specify criteria pertaining to general requirements along with management of quality and information security in a TB.

6.1 General Requirements

a. **Legal Entity:** The TBs shall be a legal entity or shall be a defined part of a legal entity, such that it can be held legally responsible for all its training activities. A governmental training organisation is deemed to be a legal entity based on its governmental status.

   Note: A training body can be a part of an educational institute or a corporate which are themselves legal entities.

b. **Organisational Structure:** The TBs shall define and document the duties, responsibilities and reporting structure of its personnel, any committee and its place within the organisation. When the training body is a defined 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 to eliminate any conflict of interest.

   The applicant TB shall define POC (Point of Contact) for each vertical.

c. **Integrity**: The training bodies and its personnel shall always maintain integrity. The training bodies shall implement adequate measures to ensure integrity. The TB should have a committee that conducts periodic review to ensure that adequate measures are implemented in the organization to maintain integrity.

d. **Code of ethical and professional conduct:** A code of conduct shall be documented and maintained in order to guide the ethical and professional conduct of the training body during the assignment. This code of conduct shall include major topics such as professional behaviour, sustainability, social responsibility, conflict of interest, integrity.

   The TBs shall have a committee that conducts periodic review to ensure that adequate measures are implemented in the organization to maintain code of ethical and professional conduct.

e. **Liability and financing:** The training bodies shall evaluate its finances and sources of income and demonstrate that initially, and on an ongoing basis, and ensure that commercial, financial or other pressures do not compromise its operational integrity.

   The training bodies shall be able to demonstrate that it has evaluated the risks arising from its training/training activities and that it has adequate arrangements (e.g., insurance or reserves) to cover liabilities arising from its operations in each of its field of activities and the geographic areas in which it operates.

f. **Communication:** An effective strategy and policy shall exist for communicating with relevant stakeholders for the duration of the assignment.

g. **Transparency:** Training organisations shall have mechanism to improve transparency and understanding with clients in order to achieve better results from training projects. This includes elements of continual improvement, ethical behaviour and interoperability

h. **Data protection and confidentiality:** The communication policy shall encompass

confidential data and information as well as intellectual property rights, such as benchmarks, for all stakeholders.

i. The TB shall safeguard the rights of privacy of all stakeholders by limiting the types of information gathered and the ways in which such information is obtained, stored, used, reported and secured.

ii. The TB shall not use stakeholders' data or information without permission for any reason, particularly to demonstrate the capacity of the TB to execute an assignment.

iii. The TB shall maintain their credibility and the confidence of the clients.

iv. The TB shall be responsible for the confidentiality of data and information received from clients even after the closure of the assignment.

v. The TB must ensure that a duly signed mutual NDA is in place with the client. The training bodies shall ensure confidentiality of information obtained in the course of its training/training activities by having a suitable system.

vi. The TB must ensure that sensitive data is accessed only by authorized parties in the organization. The access of such information should be properly logged.

vii. Use of authentication process like username and password may be used before allowing.

viii. the users to access sensitive information.

i. **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 also apply after the closure of the assignment.

The TB must aim to protect the intellectual property (IP) and prevent others from wrongly using the IP.

j. **Health and safety:** The TB shall have a mechanism to engage in a dialogue with the client to continually assess and mitigate the assignment related risks to the health and safety of the trainers and other relevant stakeholders.

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 TB shall identify, analyse, assess and prioritise the nature of potential risks, coordinating and applying the required resources to minimise, monitor and control the probability and impact of unforeseen events.

This scenario is generally applicable for on-site training.

k. **Infrastructure:** Training bodies for Cyber security (IT & ICS) applying for accreditation under this Scheme should have the following facilities:

i. Office setup, suitable meeting/ discussion room(s). The space could be owned or rented.

ii. Experts room or workstations

iii. Contemporary discussion rooms / training aids (as Digital boards, projectors, white board, markers, flipchart, audio, video facilities etc.) including requisite software for their staff or clients.

iv. TB should have library facilities or appropriate subscriptions to update their knowledge about the latest developments in the area of cyber security training.

v. Applicable cyber security software and tools along with IT support equipment to carry out the work of training shall be available and used adequately.

vi. If TB has offices at multiple locations, the same should be mentioned in application with details of experts, infrastructure etc.

vii. A Single Point of Contact (SPOC) must be appointed for each office location.

l. **Quality Management System and Information Security Management System (QMS and ISMS):** The IS/ISO 9001:2015 is the commonly used standard for Quality Management System (QMS) by any TB in almost all sectors in India and is also prescribed by major procurers. The implementation of QMS requirements ensures that:

i. the TBs have ability to consistently provide services that meet customer and applicable statutory and regulatory requirements, and,

ii. The TB shall aim to enhance customer satisfaction, higher operating efficiency, greater employee engagement, better process integration, better supplier relationships through the effective application of the system.

The training body shall demonstrate compliance with IS/ISO 9001:2015 or the current version with scope 'design and development and delivery of training courses in the area of cyber security'. This can be demonstrated by obtaining an IS/ISO 9001:2015 certification from an accredited certification body.

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

6.1 Process requirements

Process requirements address Training Body service requirements. The training body service provisioning process shall consist of the following activities:

6.1.1 General information provided by the TB

Prior to enrolment, trainees and interested parties need information about the training services in order to make an informed decision.

Information provided by the TB shall be accessible, up-to-date, accurate and legible. This information shall include at least the following elements:

a. name, address of headquarters, contact details, and locations where the training services are provided;
b. key management staff;
c. description of the main training services offered by the TB;

d. qualification and experience of trainers
e. teaching methods;
f. description of training environment and training resources;
g. full syllabus to be covered during training and no. of hours allotted to various sections
h. Details of facility/Lab providing Hands on training and skill
i. any certifications, awards, qualification and accreditation offered.

6.1.2 Proposal development

a When provided, a proposal enables the trainees or sponsors to make an informed decision regarding the acquisition of the training service.

b Prior to developing the proposal, TB shall take appropriate steps to understand the training request, its context and any logistical factors. This proposal shall include at least the following:

i. the objectives and targets of the proposed training services;

ii. the capacity of the TB to address the client's needs (e.g. client references, technical characteristics, trainers' profile, example of similar programs);

iii. the teaching and assessment methods including the batch size to be used by the TB in delivering the training service;

iv. the price, terms and conditions.

6.1.3 **Information provided by Training Body prior to acquisition of the training services by the Trainee Organisations**

Before agreeing to the acquisition of the training service, the interested parties shall be provided with the following information, as applicable:

a. the title and objectives of the training service;

b. any prerequisites, technical or otherwise, such as a required level of competence;

c. dates, location, duration and timetable, batch size: minimum and maximum no. of participants;

d. the proposed number of hours of instruction and how these are divided between different modes of training (e.g. face-to-face training, blended training, IT-supported training);

e. the teaching methods and the means of assessment to be used;

f. required software licenses and technical equipment;

g. tuition fees, examination fees, the purchase of training materials (e.g. books, software, worksheets),

h. any other charges and terms and conditions of payment. cancellation, withdrawal and refund policies;

i. the procedures used for obtaining feedback about the satisfaction of trainees (and, where applicable, of their sponsors), as well as for handling their requests, suggestions and complaints;

j. the profile of the trainers assigned to the training service, such as their teaching qualifications, teaching experience and background.

6.1.4 Needs analysis

a. Understanding the needs of trainees is a key factor in the training service as it ensures that the objectives, programme, content and assessment methods meet those needs. Prior to delivering training services, *the training needs shall be analysed by qualified* staff in order to orientate training services effectively within the specified scope of the training service.

b. The intended outcomes of the training services shall:

i. be detailed, measurable and understandable to the trainee (and, if applicable, to the sponsors);

ii. refer to a widely-known national or international scale, if available.

c. The needs analysis shall determine:

i. the goals and requirements of trainees and sponsors;

ii. the desired level of competence and the preferred time frame;

iii. the purposes for which, and contexts in which, the trainee requires the desired level of competence after the completion of the course (e.g. in the domain of work or study);

iv. the trainee's current level of competence;

v. other aspects of the trainee's background and situation (e.g. age, relevant education and training history, prior training, professional experience, language, culture, literacy level, cognitive and physical abilities).

d. In the context of work-related training, interested parties shall be consulted on how the competences acquired are expected to be applied in the workplace and what they consider possible indicators of success

e. The results of the needs analysis shall be disclosed and agreed upon between the interested parties before the design and delivery of the training service.

f. Trainers shall be fully informed about the results of the needs analysis.

g. Information gathered about trainees shall be only used for the purpose of providing the training service. Information shall only be disclosed with the trainee's consent.

6.1.5 The TB can offer standard training courses or custom-built courses which are tailored made as per specific requirements of the trainees/training organisations.

a. Standard training programs/courses

To help Cyber Security Professionals to enhance their abilities to qualify a certification programme as per their need. The outline of standard training programs for short term and extensive courses are given in Annex 1A and Annex 1B of 'Section 4 : Accreditation Process' respectively.

These courses are pre-announced and generally have trainees from various organisations.

b. Custom-built training programs/courses

To build tailored programs which are generally for a specific organisation designed to meet their objectives and goals. The TB shall define its policies / procedures in this regard.

6.1.6 Design of the training service

Following the needs analysis, the design of the training service consists of developing a curriculum, training materials and means of assessment and evaluation.

Curriculum design and development shall be carried out by trainers who are experienced or trained in the design and development of curriculum for training services.

In the design of the training service, the following shall be taken into account:

a. the results of the needs analysis
b. the agreed-upon goals
c. the proposed intensity and duration of the course, and the modes of training (e.g. face-to-face training, blended training, IT-supported training);
d. the intended training outcomes;
e. the intended means of assessment;
f. the ratio of trainers to trainees;
g. the methods, resources, and responsibilities to optimize the transfer of training, if applicable;
h. the type and content of a certificate of completion to be issued;
i. any relevant contractual elements;
j. the intended procedure of monitoring and evaluation

6.1.7 Training materials shall be:

a. in line with the designed curriculum and with the selected modes of training;
b. authentic and up-to-date reflecting current application of the subject being learned, outside the course;
c. selected taking into account social and cultural needs, as well as the background of the trainees. The curriculum, training resources, the means of assessment and evaluation shall be disclosed to trainees or the interested parties, and to trainers.

6.1.8 The roles and responsibilities of the TB, the trainees and the interested parties relating to the delivery of the training service and to the monitoring and assessment of training shall be clearly specified.

6.1.9 The curriculum, training and assessment materials shall be reviewed at least annually.

6.1.10 The design shall take into account the results of evaluations of any prior similar training services delivered by the TB.

6.1.11 Sources and copy rights of training resources used or developed by the TB shall be cited

or acknowledged.

6.1.12 Information about the training service for enrolled trainees or their sponsors.

Commencing with, or prior to delivery of the training service, trainees (or, where applicable, their sponsors) shall be informed in writing of the details, terms and conditions of the training service. Additional information may include the following:

a. the responsibilities of each party (e.g. the trainees, TBs, trainers);

b. the processes and schedule for assessing training;

c. the TB's designated contact person(s);

d. procedures for complaints, suggestions and dispute resolution;

e. support for training, such as access to library, self-directed computer-assisted training, help desk, counselling services, dictionaries, reference books and mentoring.

6.1.13 Service delivery

Staff engaged in the delivery of training services:

a. The service shall be delivered by trainers who are qualified and trained in delivering the training service in question and are trained in the use of the methods and materials.

b. Other staff engaged in the delivery of the training service shall have the competence and qualifications required to accomplish their tasks.

c. If a substitution is required, arrangements shall be made to ensure that qualified trainers with desired level of skill are available, and that such trainers are guided in the preparation and delivery of the training service.

6.1.14 Training material

a. Training materials shall be available to trainees in sufficient quantity. Trainees or their sponsors shall be guided in the purchase of those that are needed. (Eg: standards and other reference books)

b. Trainers and trainees shall be informed of relevant rules about the photocopying and use of printed and digital materials.

c. TBs should ensure the desired training material is also made available to trainees in Soft Copies

d. Videos and soft copy of materials to be made available to trainees which are pre-requisite to conduct any training.

e. TBs should make their best effort to upload the training videos for referral by trainees during the training period. A TB should be allowed to impart any similar training third time only after uploading of at least 75% syllabus to be accessed by trainee during training period.

6.1.15 Training environment

a. The applicant TB shall have in-house facilities/access to external facilities such as laboratories, test bed etc., in order to impart the training services as per the

scope of the Scheme.

b. In cases where the TB is responsible for providing or selecting the training environment, the TB shall ensure that it is conducive to training. If the TB does not have control over the training environment, the TB shall specify minimum requirements for it.

c. The training environment shall be ergonomic and well-maintained. It shall also be:

i. large enough to accommodate the number of trainees enrolled in the groups as well as their trainers;

ii. laid out in such a way as to facilitate interactive training, taking into account the needs of the trainees concerned;

iii. well-lit and clean;

iv. heated or cooled, if necessary, and well ventilated;

v. protected or insulated from noise interference;

vi. equipped with training aids and tools (e.g. as audio, video, projection devices, information technology equipment, flip charts, flash cards, models etc.) relevant to the curriculum.

d. The necessary safety facilities and equipment shall be put in place and maintained, and potential safety hazards in the training environment shall be minimized. Procedures for dealing with emergencies and security issues shall be made known to trainers, to other staff and to trainees.

6.1.16 Trainers

Trainers shall be either:

a. experienced and have qualifications/training in teaching that are/is recognized within the country where the TB offers its services; or

b. supervised by experienced trainers with qualifications/training.

c. All trainers shall have the necessary competence in the relevant subject or skill areas to undertake the teaching and related duties assigned to them.

d. Trainers shall participate in professional development. Professional development can include:

i. training and teaching principles, sound practice and latest research in training and teaching methods relevant to the curriculum;

ii. teaching competences, resources relevant to the curriculum, including instructional and informational technologies;

iii. competence in using training resources relevant to the training services;

iv. practical experience in subject matter;

v. competence in classroom management;

vi. assessment for the subject being learned.

e. Professional development plans shall be established. These shall take into account (but not be limited to) assigned tasks and responsibilities, the results of the evaluation of the training service and the trainers' own views about their professional development needs.

6.1.17 Assessment of training

a. In designing or selecting assessments, the following aspects shall be considered:

i. intended use of the assessment;

ii. knowledge, skills and abilities to be measured;

iii. standards to be measured against;

iv. methods of assessment;

v. scoring and reporting;

vi. interested parties involved in or affected by the assessment.

b. Prior to, or at the beginning of the course, an assessment shall be made of the trainee's level of competence in the subject to be learned.

c. The progress of trainees shall be assessed throughout and at the end of the course.

d. Trainees or their sponsors shall, upon request, receive a certificate of completion, which shall include (but not be limited to) the following information:

i. title and objectives of the training service;

ii. number of hours of instruction;

iii. level of achievement.

e. Access to assessment results shall be given only to those with established authority or legitimate consent to view the information with regard for principles of fairness, transparency and confidentiality.

6.1.18 Monitoring and evaluation of the training service

a. Regular monitoring and evaluation shall be carried out in order to determine whether the training service is meeting its objectives.

b. In designing the processes for monitoring and evaluation, the following aspects shall be considered:

i. scope;

ii. goals;

iii. means of monitoring and evaluation, including rationale, criteria, instruments and schedule;

iv. interested parties involved in or affected by monitoring and evaluation.

v. logistics and organization of the training service.

c. Service evaluation shall include (but not be limited to) the following:

vi. fulfilment of training needs;

vii. training and teaching methods;

viii. adequacy of training material and other resources;

d. Procedures for monitoring and evaluation shall include:

ix. periodic observation of teaching and training for quality assurance purposes;

x. review of assessment results and the alignment of these results with the agreed-upon goals of the training service, as developed in the needs analysis. For this purpose, assessment of training shall allow the compilation, comparison and analysis of assessment results;

xi. analysis of the level of satisfaction of trainees and sponsors with the training service, as well as their feedback and suggestions for improving the quality of the training service;

xii. analysis of enrolment, attendance and attrition.

e. Such monitoring and evaluation shall be conducted by qualified persons.

xiii. Data sets and reports resulting from monitoring and evaluation shall be clear and transparent. Reports shall clearly describe the findings and the rationale in light of the training service objectives.

xiv. Any complaints and claims shall be dealt with within an agreed timeframe to provide redress or explanation.

xv. The results of monitoring and evaluation shall be taken into account in implementing improvements and changes to the training service, such as in the curriculum, course programs, teaching methods and professional development.

6.1.19 Invoicing

a Invoices for the training service shall be clear and shall contain all the details needed to enable trainees (or, where applicable, their sponsors) to understand precisely what is being invoiced.

b The TBs shall provide the trainee or the sponsor with proof of payment if requested.

6.2 People Requirements

6.2.1 Personnel (HR requirements)

a. As per the scope, the training bodies shall have, as part of its own organisation, personnel, either employed or on contract, having sufficient competence for delivering the training / training according to the Scheme requirement.

b. The training bodies shall have defined processes for selecting, training, and formally authorising and monitoring the performance of its personnel involved in carrying out the various training/training activities and for selecting technical experts, if needed, as per the requirements of the Scheme.

The TBs must take feedback from training participants regularly to monitor the performance of its personnel involved in carrying out the various training/training activities and the effectiveness of the training program.

c. The training bodies shall have a mechanism to keep their human resource updated to the contemporary issues by deputing them to participate in various seminars, workshops, access to latest versions of standards, testing tools, participations in standards development activities, publishing research papers, mentoring aspiring candidates and similar capacity building activities. They should maintain a record of

the same.

d. The infrastructure and staffing of the training bodies shall commensurate to the scope of activities applied to the Scheme manager.

e. Also, the training bodies shall accept the assignments in line with the available capabilities of human resources and capacities of their infrastructure.

f. Competence on Technical Rationale:

In addition to the requirement given above, every trainer shall have the appropriate level of experience and should understand the requirements (What, Where, When, Why, Who and How) to deliver the services. The trainers need to be conversant with the new pedagogy tools available with the training body.

The TBs must carry out Faculty/Trainer development program (FDP/TDP) after fixed intervals.

6.2.2 Competence of trainers of TB

The TBs shall be responsible for developing and maintaining appropriate capability throughout the assignment and shall only seek and accept those assignments that it is capable of fulfilling. Capability includes:

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

b. other resources, including access to specialised knowledge, methodologies, tools and technology and other relevant non-staff resources.

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

d. Education

i. The TBs shall ensure that the trainer have at least a graduate degree in engineering discipline from a university recognized by the Government for such purposes.

OR

ii. Diploma in Engineering from a Board or Institute recognized by the Central Government or the State Government, as the case may be, for such purposes.

e. Work Experience

The trainers shall have at least 5 years (7 years for diploma in engineering discipline) of full-time post qualification experience in cyber security life cycle (such as product development, engineering, manufacturing, integration, installations, operations, inspection, certification or testing, or the equivalent industry).

Minimum 2 years as a trainer (which is a part of 5 years) in information security/cyber security aspects from an IT, software/firmware related to IT or IoT products or CII products under the supervision of a qualified personnel with 5 years of experience in the Information Technology (IT) same field.

f. Trainings of Trainers and Evaluators (internal evaluators) of TB

The training bodies shall ensure that trainers and evaluators have participated in any or all of the trainings on relevant international standards such as IS/ISO/IEC 17021, IS/ISO/IEC 27001, IS/ISO/IEC 27019, IEC 62443-2-1, IEC 62443-3-3, ISA/IEC 62443 Cyber Security Fundamentals Specialist, IEC 62443 - Cyber security Risk Assessment Specialist, ISA/IEC 62443 - Cyber security Design Specialist, ISA/IEC 62443 - Cyber Security Maintenance Specialist, ISA/IEC 62443 - Cyber security Expert, ISO 31000 and standards for Cloud and Digital Personal Data Protection Act 2023, as applicable.

The trainer should have adequate knowledge of subject areas defined in the course curriculum / elements of the applicable modules of competency profiles along with control elements of Level 1, Level 2 and Level 3, as applicable depending on the applied scope of accreditation.

The trainer shall have gained experience in the entire process of information security /cyber security management system, including review of documentation and risk management of CSEs, identification of root cause and reporting/implementing preventing and correction actions to add value in the training pedagogy by sharing his experience and delivery of case studies. The trainer shall have the experience to articulate the performance of the trainees at the end of the day/ session while evaluation.

TBs providing training services related to certification of Cyber Security Professionals should themselves have a few PrCB certified personnel. For guidance, following certifications (or equivalent) may be required. This table mentioned below can be used for inference of minimum Knowledge and Skill required for the trainers. Refer to Annex 1A of 'Section 4: Accreditation Process'.

Table 3.1: Cyber Security Domain and Certification Id

S. No.	**Cyber security domain**	**Certification Id** (refer to Table 3.3: Cyber Security Domain Certification Codes and Titles under the Scheme in Section 3 of Certification Scheme for CyberPros)
1	Governance, Risk and Compliance	S No. 3 GRC-M
2	Technology & System Security Architecture	S No. 6 TSA-M
3	Secure Software Development	S No. 8 SSD-A
4	Application Security Testing	S No. 10 AST-A
5	Product Security Testing	S No. 12 PST-A
6	Network Security Administration	S No. 14 NSA-A
7	System Security Administration	S No. 16 SSA-A
8	Applications & Data Security Administration	S No. 18 ADS-A
9	Security Support Services	S No. 20 SSS-A
10	Security Performance Management	S No. 22 SPM-A
11	ICS Cyber security	S No. 23 ICS-F
12	ICS Cyber Risk Assessor	S No. 25 ICR-A

13	ICS Cyber security design, & Implementation	S No. 27 ICD-M
14	ICS Cyber security Operations & Maintenance	S No. 29 ICM-M
15	Cyber Defence	S No. 32 CYD-M
16	Cyber Vulnerability, Threat & Risk Management	S No. 34 CRM-A
17	Security Operations	S No. 36 SCO-A
18	Cyber Forensics & Investigation	S No. 39 CYF-M
19	Cyber Training & Awareness	S No. 41 CTA-A
20	Documentation, Implementation and Auditing of CSMS (BTC-L1, STC- L2 and ATC -L3 as applicable)	S No. 03 GRC-M and/or S No. 23 ICS-M and S No. 25 ICR-A

6.3 Technological requirements

The training body shall have provisions of sufficient infrastructure to deliver its services effectively and efficiently. This includes but not limited to:

6.3.1 Access to Cyber security simulator

a. Access to Cyber Security simulator and / or suitable hardware**:** The TB shall have access to globally recognised catalogue of on-demand cyberattacks simulation scenarios so that trainees can recognise and respond to any attacker technique, tactic and procedure.

b. The simulator shall provide trainees with a suite of commercial tools which they shall actually using on the job for performing investigations, incident detections and response. Trainees shall experience advanced attackers' behaviours which they may encounter on the job (e.g. PING sweeps, lateral movement and data ex filtration).

c. This simulator shall meet the requirement of global practices such as National Institute of Standards and Technology (NIST) Incident Response framework, Council of Registered Security Testers (CREST), MITRE ATT&CK (Adversary Tactics, Techniques and Common Knowledge) framework etc.

The applicant training body shall study in detail the requirements of competency profile documented in certification criteria TBs and prepare a compliance matrix specifying how they are equipped to meet the K&S requirements for delivering the same to trainees. Refer to Annex 1A, 1B and 1C of 'Section 4: Accreditation Process'.

The procedures and listing of tools to be used for the conduct of IT and ICS assessment shall be in place.

Note: The applicant TB shall have in-house facilities/access to external facilities such as laboratories, test bed etc., in order to impart the training services as per the scope of the Scheme.

6.3.2 Training Management System (TMS)

a. The training body shall possess the training management system which is designed to identify training and training gaps, using analytical data and reporting and are focused on online training delivery but support a range of uses, acting as a platform for online content, including courses, both asynchronous based and synchronous based.

b. A TMS may offer classroom management for instructor-led training or a flipped classroom. It is recommended that TMSs include intelligent algorithms to make automated recommendations for courses based on a user's skill profile as well as extract metadata from training materials to make such recommendations even more accurate. It is desired that TMS should be integrate able with the Cyber security simulator and / or suitable hardware.

c. Access to international standards

The training body shall have mechanisms to have access to domestic regulations, guidelines and international standards:

i. NCIIPC and CERT-In guidelines as published.
ii. ISO/IEC standards on cyber security published by JTC 1 SC 27, IEC TC 65E
iii. Other IS/ISO/IEC standards on cyber security published by various sub committees which are generally domain specific.
iv. All applicable and relevant NIST standards.

d. Process for Continuous professional development for trainers and experts:

The training body shall have necessary infrastructure such as technical information centre, library, documentation centre etc. consisting of access to journals, technical reports, policy documents etc. relevant to cyber security in critical infrastructure for continuous professional development for trainers and experts.

The training body shall have the procedure for evaluating, selecting, appointing and monitoring expert for the Cyber security (IT & ICS) Training through:

- Prescribing qualifications, experience, competence requirements for Cyber security (IT & ICS) experts/resource persons (in-house/ external).
- Assessing competence of a Cyber security (IT & ICS) expert/resource person prior to appointment.
- Assessing performance/ monitoring Cyber security (IT & ICS) expert after appointment and during/after training. Identifying training areas of improvements for Cyber security (IT & ICS) expert/resource person.

Note: This is an internal standard of the training body. This standard refers to the internal standard/criteria of the training body as a policy.

7 Complaints and Appeal Handling

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

7.2 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.

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

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

7.3.2 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.

7.3.3 Acknowledgement of the complaint.

7.3.4 Investigation for redressal of the complaint.

7.3.5 Communication with the complainant for closure of the complaint.

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

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

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

7.3.9 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.

7.3.10 TB shall inform all interested parties of the right to make a complaint or an appealand shall make it publicly available without request.

SECTION 4

ACCREDITATION PROCESS

1. Background

1.1 A credible accreditation Scheme specifies the requirements for the accreditation of Training Bodies, operating in Cyber Security for IT and ICS. Along with the requirements, a robust accreditation process needs to be defined and implemented to generate a reasonably a good level of confidence on the system.

1.2 The accreditation process workflow focuses on the compliance of the requirements along with other supporting activities like suitable infrastructure, qualified & competent human resource, Cyber security expert, system-oriented working system, sustainable and ethical working as well as risk assessment and its management.

1.3 The defined accreditation process is dynamic in nature and modifications and update may take place periodically, as it is ought to be for continual improvement of the delivery and effectiveness of the training services.

2. Scope

2.1.1 The requirements that an applicant TB should meet, are defined in 'Accreditation Criteria for TBs'.

2.1.2 The scope of this document defines lifecycle activities of the accreditation process.

2.1.3 It also prescribes training programme addressing training objectives of training course including training course (title) no. of days, training outcome and mode of delivery.

2.1.4 It provides reference for curriculum development for a training course including training course (title), modules along with description mapping with competency profiles.

2.1.5 For defining the scope of accreditation for training bodies, the following should be considered:

a. Annex A (Table depicting domains for selection of Scope by TB) defines short term training programs with targeted towards CSEs' capacity building which may eventually assist in obtaining certification.

b. Annex B (Detailed training programs with extensive coverage) defines the extended training programs with targeted towards professionals interested in enhancing their knowledge and skill levels in the area of cyber security which may eventually assist in obtaining personnel certifications of various levels. Annex IB should be read in conjunction with Annex 1C (Reference for Curriculum Development for a Training Course).

Note
1: TBs are advised to start with a scope commensurating to their current capabilities, market requirements and gradually enhance the same over a period of time.
2: The accreditation of TBs is the demonstration of technical capabilities and delivery process to the AB. The scope recommended in Annex 1A, 1B and 1C should be followed in intent and the principles. There could be a situation where the contents of the established training programs will be at variance with the prescribed contents but if objectives and outcomes are similar in nature, the AB shall consider the established modules of the TBs complied with the scope.

3. Accreditation Process

3.1 Pre-requisite for Pre-Application Stage

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

3.2 Assessment Process

3.2.1 Details of the accreditation Scheme and the Application Form are posted on the QCI-NABET website. Any institution/organization desirous of accreditation under this Scheme should carefully go through the requirements of the Scheme, processes and assess their own readiness. The prospective applicant TB must take care of shortfalls, if any, before applying.

3.2.2 The applicant training body shall define their scope of accreditation depending on their capability and result of the business analysis & market needs. They shall refer to Annex 1A, Annex 1B and Annex 1C of this section during for finalising the scope. For defining scope, the following should be considered:

Scope can be chosen from 19 domains (S No. 1-19 of Annex 1A of this section) as per requirement of CSEs or individuals. Training is always associated with Knowledge, Skills and Expertise, which may be relevant to one or more Cybersecurity domains.

a. (Since TB is expected to be at higher echelon of competency than the trainees they shall appreciate the relationships of KM and SM bundling for a particular domain therefore for obtaining the accreditation, the unit is 'A Domain'. However, for delivering the training services, it can be any module depending on market/ client needs)

b. For S No. 20, TB can choose L1, L2 and L3 sequentially in a progression for accreditation.

c. Training Bodies which are a part of educational institutions or training division of corporates / PSUs and their existing training programs are in line with prescribed scope with common principles, common philosophy, similar (or more) content can be described in their application form so that their existing training programs can be considered for recognition if a satisfactory degree of equivalence is established. However, they have to meet other requirements of accreditation criteria.

d. There is no provision for accreditation of training bodies for Basic level.

e. Interested TBs that wish to conduct these courses (as accredited courses) shall obtain accreditation of the domain where these modules are covered.

f. Application form, complete in all respects, giving relevant details of application fee can be sent in a soft copy.

g. Hard copy of any other relevant document may have to be submitted if asked for by NABET, subsequently. NABET Secretariat will inform the TB of any clarification/additional information that may be required for completeness of the

application.

3.3 Assessment Process

Assessment Process comprises of three stages:

3.3.1 **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 test, interview with TBs' expert(s) and concerned administrative staff to gain an understanding of the capabilities required for imparting trainings.

3.3.2 **Surveillance Assessment:** Same as stated above but with a brief assessment duration, especial emphasis on the effectiveness of their engagements with trainers to meet their IT/ICS cyber security requirements, timely delivery of the agreed scope including performance, quality of imparted trainings, up-to-date qualifications of the experts / trainers, compliance to accreditation conditions, carried out within 12 and 24 months of initial process of accreditation.

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

3.3.4 Requirements for Initial, Surveillance and Re-accreditation

a. Initial Assessment (IA)

Application Completeness: Submitted application shall be reviewed by NABET secretariat for its completeness. Inadequacies in application (if any) shall be informed to applicant organization. TBs should submit response to the inadequacies within 30 days*. Only completed applications will be processed further. TBs should submit the filled self-assessment report in NABET format shared by NABET Secretariat at the time of acceptance of application.

If inadequacies are found in the response, the same will be communicated and the TB will have additional time of 30 days to respond. If TB fails to submit satisfactory response even after this additional time, then the application can be made inactive. The inactive period will be for 60 days. The TB may reapply with requisite fees after this period.

i. Desktop Assessment (DA): NABET assessor conducts adequacy assessment (application & technical assessments of documents submitted by TBs). Observation(s) and non-Conformities (NCs), if any, would be communicated by NABET secretariat to the applicant TB. TB will have time of 30 days to submit the response. Closure of NCs and observations submitted by TB will be verified by NABET assessor. During desktop assessment, the auditor will also audit the training course of a domain specified in the scope of accreditation. Document evaluation include their quality manual, ISMS manual, procedures and processes and compliance report (mentioning references linking to their documents to indicate adequacy of their defined system) submitted by applicant w.r.t 'Accreditation Criteria'. During DA, audit team shall indicate about adequacy of

documentation.

The technical expert of the audit team reviews the training course material for its completeness, correctness and comprehensiveness, and complying with the requirements of accreditation criteria. This is done for each domain for which accreditation is sought. The auditor of the audit team checks for the following:

ii. TBs has to make it clear that the training module doesn't substitute any applicable legislature and/or national/international standard and the same is only for provision of training course. Prescribed training courses doesn't substitute any subject/module falling under the ambit of National Education System.

iii. Each training course defines

- Purpose
- Training objective (K & S) which the trainee must achieve after successful completion of the training
- Prerequisite (may be defined by training body)
- Broad contents
- Need of the training after proper need assessment.
- Procedure for assessment of trainees
- Procedure for evaluation of training and its intended outcome
- Duration and mode of training

iv. TBs has made it clear that It is a voluntary initiative wherein the professional is free to undertake any course based on his professional requirement. It is not mandatory to complete any training programme for certification of personnel (PrCB) or getting certification for CSMS (L1, L2 and L3)

v. TBs has defined course attendance policy, ratio of trainers to trainees including maximum trainees permitted in a programme, and stipulated the possible causes that may be generated for each trainee.

b. **Office / Site Assessment (OA):** Following the review and acceptance of the documentation and procedures submitted by the TB, NABET shall undertake full assessment at TB premises to ensure effective implementation of the documentation. It shall include interaction with each expert (in-house and visiting)/ quality manager, concerned administrative staff etc. verification of infrastructure, client's feedback etc. The audit team will carry out witness audit where witness of the training course will be checked for proficiency of training service delivery and compliance with the requirements.

'Accreditation Criteria for TBs' shall be used as a reference document to carry out desktop assessment and office assessment.

c. Witness Audit (WA): During witness audit NABET subject matter experts are also involved. Witness audit is done as per the scope of accreditation sought which is aligned with the Annexure1A and 1B and will be done for every domain which is included in the scope. Assessment report [findings like observation(s) and NCs (if any)] would be reported by NABET assessors to NABET secretariat and in turn communicated to TB. Corrective measures shall be submitted by TB within 30 days.

Witness Audit Criteria:

The technical expert of NABET, based on his evaluation of ability and capacity of a training body provides knowledge and skill training and resource to the ecosystem. His recommendations are based on informed judgement which are qualitative in nature indicating TB's ability to deliver and transfer Knowledge and Skill to a domain function.

Accreditation Committee for granting accreditation. Decision regarding grant/denial of accreditation would be communicated to TB by NABET secretariat.

'Accreditation Criteria for TBs' shall be used as a reference document to carry out desktop assessment and office assessment.

Note 1: Closure of NC's and observations submitted by TB will be verified by NABET assessor. In case an applicant TB has branch offices, all branches will be assessed during Initial Assessment.

Note 2: TB can refer to annex 1A for selecting a domain for demonstration of their capability.

d. Surveillance Assessment (SA)

i. If there is no change in approved experts, training quality manual, infrastructure, etc. since the initial accreditation then accredited TB shall pay surveillance fee and inform NABET for surveillance due. The Surveillance Assessment shall be completed within 365 days (1 year) of the Initial Assessment. It is therefore mandatory for the TB to apply for SA within 10 months of the IA so that all SA formalities are completed with completion of 1 year from the date of grant of IA.

ii. If there is any change in experts, team composition, quality manual, infrastructure, modification of scope etc. then applicant with updated details and applicable fee shall submit the details to NABET Secretariat. NABET Secretariat will review the documents and proceed with the process of surveillance assessment of applicant organization.

iii. SA will be conducted with particular emphasis on performance, quality of training delivery, client's feedback, compliance to conditions of accreditation. Two SA to be carried out within 12 and 24 months from the date of accreditation. The SA will involve evaluation of documents as well as Site Visit.

iv. In case an applicant TB has branch offices, branches shall be covered during each SA on risk -based sampling. During SA, the focus is on complaints, appeals, misuse of marks, analysis of the customer satisfaction records and continual improvement programme of the training body.

e. Re-Accreditation (RA)

i. To confirm that TB operations are in steady state and continue to comply with the accreditation criteria, re-accreditation audit is done. Process shall be similar to initial assessment, with particular emphasis on performance, feedback by clients, etc. The RA needs to be completed within three years from the date of accreditation. RA application shall be submitted 3 months prior to date of expiry of accreditation certificate issued. RA process shall be completed before the expiry of accreditation to avoid any discontinuation

of accreditation.

ii. Extra Visit if needed: On the bases of risk factors, received information or complaint from primary or secondary source, surprise Visit / extra visit may be planned unannounced or announced as the case may be.

*Note: The time framed specified are maximum and training body shall have their own service levels as per their policies which should be stringent than this.

f. Criteria for granting Accreditation

On the basis of desktop assessment (DA), report by assessor(s) and satisfactory closure of NCs and observations, office assessment will be conducted by NABET assessor(s). Based on office assessment report, NCs and observation, if any, shall be communicated to the TBs for the necessary closure and compliance. TBs shall submit evidence-based compliance of NCs and observations at the earliest but not later than a month (30 days). If required, additional office and witness assessment may be carried out for verification of evidences for closures.

Accreditation period of three years will be counted from the date of grant of accreditation by the Accreditation Committee (AC); however, this validity period is subject to satisfactory Surveillance Assessment (SA).

Accreditation under this criterion will be granted under fulfilment of all of the following:

i. Submission of requisite documents with application.
ii. Closure of all NCs at the DA stage.
iii. Successful completion of OA and closure of observed NCs in required
iv. Time and to the satisfaction of the assessing team.
v. 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 TBs 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 in defined time.
4.1.4 All payments shall be made in advance.
4.1.5 Franchising, licensing, subcontracting of NABET Accredited training organizations is NOT permissible.
4.1.6 Accredited Training Bodies (ATB) should submit a six-monthly report about the CSE and/or individuals training projects taken up and list of approved experts involved along with the status of project.
4.1.7 Any change in expert, employment status, scope etc. shall be informed to NABET within

10 days with relevant documents.

4.1.8 Accredited TB just after accreditation shall sign the 'Code of Conduct' and send it to NABET Secretariat.

4.1.9 The accredited TB shall maintain relevant records of each training conducted / provided.

4.1.10 The accredited TB shall share list of trainers with NABET which NABET/QCI may display on its website.

4.2 Suspension / Withdrawal of Accreditation

NABET will suspend or withdraw accreditation on account of any one or more grounds during accreditation cycle as per the following clauses:

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

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 TB in respect of its submission/ interaction with NABET / QCI which would include, 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 TB to NABET / QCI.

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

4.2.9 Not submission of SA/RA application in defined time.

4.2.10 Franchising, licensing or subcontracting of training / programs.

4.2.11 Any other condition deemed appropriate by NABET / QCI.

4.3 **Code of Conduct**

All accredited TB's are obliged to improve the standing of the profession by rigorously observing the Code of Conduct. Failure to do so may result in the suspension or cancellation of accreditation.

The accredited TB is committed:

4.3.1 To act professionally, accurately and in an unbiased manner.

4.3.2 To be truthful, accurate and fair to the assigned work, without any fear or favour.

4.3.3 To judiciously use the information provided by or acquired from the applicant and to maintain the confidentiality of information received or acquired in connection with the assignment.

4.3.4 To avoid and/ or declare any conflict of interest that may affect the work to be carried out.

4.3.5 Not to act in a manner detrimental to the reputation of any of the stakeholders including NABET / QCI.

4.3.6 To co-operate fully in any formal enquiry procedure of NABET / QCI.

4.3.7 Not to employ active NABET assessors. Any person who is conducting assessments for NABET should not be a trainer with the Training Body for Cyber security (IT & ICS).

4.4 Complaint and Appeals

4.4.1 The accredited TB shall establish documented procedures for handling and disposal of complaints and appeals within a reasonable time. The documented procedure shall include provision for:

a. Providing information regarding complaint handling process to all interested parties
b. Acknowledgement of complaints
c. Complaint analysis/ investigation for redress 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.

4.4.2 The accredited TBs shall maintain records of all complaints & appeals, and their resolutions including actions taken.

4.4.3 All complaints and appeal to be assessable to NABET assessment.

4.5 Payment of Fee

The TBs shall abide by the commercials as applicable.

4.6 Governance

NABET / QCI reserves the rights with respect to accreditation Scheme for TBs for Cyber security (IT & ICS). NABET / QCI will have following functions (but not limited to):

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

4.7 Confidentiality

4.7.1 All information, documents submitted by an applicant to NABET shall be used by NABET (including NABET Assessors and Members of Accreditation Committee) for the purpose of 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 TBs would be protected for sensitive information related to business whenever it is called for/ appropriate. In case a TB wants the information to be kept confidential, a communication shall be sent to NABET citing reasons for the same. NABET reserves the right to take decision in this regard.

4.7.2 Accredited TBs shall have adequate arrangements consistent with applicable laws to safeguard confidentiality of all information provided by stakeholders.

4.7.3 The accredited TBs should maintain confidentiality of their client's related information like location, products, processes, vendors, feedback form, personal details etc.

Annexure 1A

Table depicting domains for selection of Scope by TB

(Short term courses)

S. No.	Cyber security domain	Related modules* (Refer to Annex 1C)	No. of Days**	Training Objectives	Training Outcome	Code for mode of delivery (Online 1/F2F 2/Hybrid 3)
1	Governance, Risk and Compliance	*(GRC-M)* KM 0601 F KM 0601 A KM 0601 M KM 0701 F KM 0701 A SM 0602 F SM 0602 A SM 0603 A	4	To acquire knowledge on: i) IT/ICS Governance, Risk and Compliance frameworks and its requirements. ii) Risk Management covering Risk Scenarios, Source, Criteria, internal, external, appetite, likelihood, consequences and level of risks as per ISO 27005:2022 and ISO 31000:2018. To acquire skill on: i) Written Communication Skills	i) Capability to formulate and drive cyber security policies, standard operating procedure (SoP) on GRC ii) Perform cyber security risk management activities such as risk assessment and treatment and generate a report ii) Able to present a conformance and performance status report to the governing board.	All modes

S. No.	Cyber security domain	Related modules* (Refer to Annex 1C)	No. of Days**	Training Objectives	Training Outcome	Code for mode of delivery (Online 1/F2F 2/Hybrid 3)
2	Technology & System Security Architecture	*(TSA-M)* 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 F SM 0301 A SM 0602 F SM 0602 A SM 0603 A	4	To acquire knowledge on: i) Design, development and implementation of Secure Systems Architecture for IT/ICS environment. ii) Identification of Cyber Security needs of the organisation and translating them into security, designs and principles. iii) Adoption of new technological advances and best practices in IT/ICS systems to mitigate security risks. To acquire skill on: i) Technical Skills on security architecting ii) Written Communication Skills	i) Capability enhancement in design rules and architecture models and their implementations ii) Capable to design and architecture review. iii) Document Technology and Systems Security Architecture	All modes

S. No.	Cyber security domain	Related modules* (Refer to Annex 1C)	No. of Days**	Training Objectives	Training Outcome	Code for mode of delivery (Online 1/F2F 2/Hybrid 3)
3	Secure Software Development	*(SSD-A)* KM 0501 F KM 0501 A SM 0401 F SM 0401 A	2	To acquire knowledge on: i) Secure Software Design & Development as per global practices such as Open Worldwide Application Security Project (OWASP) To acquire skill on: i) Software Development & Testing Skills	Understanding the requirements of secure software development and its implementation	1,2,3
4	Application Security Testing	*(AST-M)* KM 0501 F KM 0502 F KM 0502 A SM 0401 F SM 0401 A	3	To acquire knowledge on: i) Software Security Testing as per global standards such as OWASP. ii) Security Code Review as per OWASP or equivalent. iii) Formulating test objectives, test specifications, creation of testing goals and scenarios, validation rules and creation of test reports. To acquire skill on:	i) Setting up of a security test laboratory consisting of test tools, test environment etc. ii) Capable of formulating test procedures and defining responsibilities of different roles such as test manager, test lead / test engineer, tester and analyst. iii) Capable of conducting security testing, generation of test reports and its validation	2 or 3

S. No.	Cyber security domain	Related modules* (Refer to Annex 1C)	No. of Days**	Training Objectives	Training Outcome	Code for mode of delivery (Online 1/F2F 2/Hybrid 3)
				i) Software Development & Testing Skills		
5	Product Security Testing	*(PST-A)* KM 0201 F KM 0201 A KM 0202 F KM 0202 A SM 0401 F SM 0401 A	3	To acquire knowledge on: i) Secure Software Design & Development ii) Product Security Testing requirements as per global frameworks such as common criteria (ISO 15408) and crypto model validation programme (CMVP), Crypto Algorithm Certification Programme (CACP) as per FIPS -140 -2 and FIPS 140-3 requirements and ISO 19790 requirements To acquire skill on: i) Software and System Development & Testing Skills	Understanding the requirements of Security Product Testing including maturity levels their applicability and tasks involved	2 or 3

S. No.	Cyber security domain	Related modules* (Refer to Annex 1C)	No. of Days**	Training Objectives	Training Outcome	Code for mode of delivery (Online 1/F2F 2/Hybrid 3)
6	Network Security Administration	*(NSA-A)* 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 0201 F SM 0201 A SM 0601 F	2	To acquire knowledge on: i) Network Infrastructure and Administration requirements ii) Network Security requirements iii) Standards on Network Security To acquire skill on: i) Managing & Securing Skills	Capable (documentation and implementation) to configure hardware, software, services (e.g. Cloud services) systems to ensure integrity and reliability of network infrastructure incorporating uses of appropriate protection, detection and response mechanism to confine and detects security incidents.	1 or 3
7	System Security Administration	*(SSA-A)* 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	2	To acquire knowledge on: i) Systems Infrastructure and Administration ii) System Security requirements, its hardening and management To acquire skill on: i) Managing & Securing Skills	i) Capable to design process and its operation including log reviews / monitoring for System Security Administration ii) To generate standard template and baselining of secure configurations	2 or 3

S. No.	Cyber security domain	Related modules* (Refer to Annex 1C)	No. of Days**	Training Objectives	Training Outcome	Code for mode of delivery (Online 1/F2F 2/Hybrid 3)
8	Applications & Data Security Administration	*(ADS-A)* KM 0301 F KM 0301 A KM 0302 F KM 0302 A SM 0301 F SM 0301 A	2	To acquire knowledge on: i) Software and Platform Operations Security and requirement analysis ii) Cyber Threats and Vulnerabilities To acquire skill on: i) Managing & Securing Skills	Capable to design process and its operation for Application and Data Security Administration addressing Cyber Threats and Vulnerabilities	2 or 3
9	Security Support Services	*(SSS-A)* KM 0101 M KM 0101 F KM 0102 F KM 0201 F KM 0201 A KM 0202 F KM 0202 A KM 0803 F KM 0803 A	2	To acquire knowledge on: i) Network Infrastructure and Administration requirements ii) Network Security requirements iii) System Infrastructure and Administration iv) Software and Platform Operations iv) In case of ICS Security program requirements, training on IEC 62443-2-4 is preferred To acquire skill on: i) Managing & Securing Skills	i) Capable to design process and its operation for Application and Data Security Administration ii) Security for ICS System as per IEC 62443-2-4 iii) Capable to design RFP/tenders for identifying capable service provider vendors as specified in ii) above.	All modes

S. No.	Cyber security domain	Related modules* (Refer to Annex 1C)	No. of Days**	Training Objectives	Training Outcome	Code for mode of delivery (Online 1/F2F 2/Hybrid 3)
10	Security Performance Management	*(SPM-A)* KM 0101 F KM 0102 F KM 0201 F KM 0202 F KM 1001 F KM 1001 A	2	To acquire knowledge on: i) Data Science, Data Analytics, AI/ML ii) Process of security performance, measurement and management To acquire skill on: i) Managing & Securing Skills	i) Enhancement in the ability for Security Performance Management ii) Capable to define matrix, KPAs and KRAs.	2 or 3
11	ICS Cyber security	(ICS-F) KM 1301 F	4	To acquire knowledge on: i) ICS operations and components ii) Specific additional risk in ICS environment and their consequences iii) Patch Management, Security Programme, Architectures, System Security Requirements and Product Development Life cycle iv) Network Segregating and Zoning	Enhancement in ability in Risk Management in ICS environment. Developing security architecture of ICS, specific cyber security controls of ICS and establishment of Security Management programmes.	2 or 3

S. No.	Cyber security domain	Related modules* (Refer to Annex 1C)	No. of Days**	Training Objectives	Training Outcome	Code for mode of delivery (Online 1/F2F 2/Hybrid 3)
12	ICS Cyber Risk Assessor	*(ICR-A)* KM 1302 F KM 1302 A	2	To acquire knowledge of techniques to perform cyber risk assessment in the ICS environment with focus on EHS and Business Continuity Management.	Capable of performing Risk Analysis and Mitigation in ICS environment	2 only
13	ICS Cyber Security design, & Implementation	*(ICD-M)* KM 1303 M KM 1303 A	2	To acquire knowledge of design and implementation techniques for the ICS environment.	Capable of performing design and implementation techniques for the ICS environment including proficiency in critical design review	2 only
14	ICS Cyber Security Operations & Maintenance	*(ICM-M)* KM 1304 A KM 1304 M	2	To acquire knowledge of vulnerability and patch management configuration tools and techniques To acquire knowledge for formulating and documenting procedures incorporating controls and performance matrix.	Capable of designing and implementing process of operation and maintenance including techniques such as failure mode and effect analysis and faulty analysis. Deploy mitigation techniques in order to effectively defend against cyber threats and vulnerabilities. Verify assets, asset enquiry, commissioning and decommissioning.	2 only

S. No.	Cyber security domain	Related modules* (Refer to Annex 1C)	No. of Days**	Training Objectives	Training Outcome	Code for mode of delivery (Online 1/F2F 2/Hybrid 3)
15	Cyber Defence	*(CYD-M)* KM 0804 F KM 0804 A KM 0901 F KM 0901 A KM 0901 M SM 0101 M SM 0501 F SM 0501 A SM 0602 F SM 0602 A SM 0603 A	4	To acquire knowledge on: i) Enterprise Cyber Defence, Network Infrastructure, Security and Administration, System Infrastructure, Security and Administration, Software and Platform Operations. ii) To build a robust security infrastructure layer by layer across hybrid environment and implementing a zero trust defensible security architecture. To acquire skill on: i. Programming & Scripting Skills ii. Managing & Securing Skills iii. Written Communication Skills To acquire knowledge for formulating and documenting procedures incorporating	i) Enhancement in the ability of designing, developing and implementing cyber defense system for enterprise (CSEs) ii) Technical knowledge, insight and hands-on training to confidently defend network iii) Intelligently examine network traffic to identify emerging threats to perform large scale correlation for threat hunting and reconstructing network attacks.	All modes

S. No.	Cyber security domain	Related modules* (Refer to Annex 1C)	No. of Days**	Training Objectives	Training Outcome	Code for mode of delivery (Online 1/F2F 2/Hybrid 3)
				controls and performance matrix.		
16	Cyber Vulnerability, Threat & Risk Management	*(CRM-A)* KM 0804 F KM 0804 A SM 0602 F SM 0602 A SM 0603 A	3	To acquire knowledge on: i) Enterprise Cyber Vulnerability, Threat & Risk Management ii) Specific issues and requirements of CII iii) Testing and hardening techniques To acquire skill on: i) Written Communication Skills	Enhancement in the skills and abilities in Cyber Vulnerability Threat and Risk Management and vulnerability analysis	All modes
17	Security Operations	*(SCO-A)* KM 0201 F KM 0201 A KM 0803 F KM 0803A	3	To acquire knowledge on: i) Enterprise IT and Info Security Operations requirements ii) Enterprise IT Security Strategy and Design iii) SoC Management To acquire skill on: i) Written Communication Skills	Capable to design process for security operations Enhancement in ability in *pro-active Incident identification*	2 or 3

S. No.	Cyber security domain	Related modules* (Refer to Annex 1C)	No. of Days**	Training Objectives	Training Outcome	Code for mode of delivery (Online 1/F2F 2/Hybrid 3)
18	Cyber Forensics & Investigation	*(CYF-M)* KM 1101 F KM 1101 A KM 1101 M SM 0101 F SM 0501 F SM 0501 A	3	To acquire knowledge on: i) Cyber Forensics & Investigation ii) Software and Platform Operations iii) Practices and processes of digital forensic data, its collection analysis and relation with digital evidence to determine root cause of cyber breaches. iv) Hardware reverse engineering techniques To acquire skill on: i) Written Communication Skills	Capable to design and document process for Cyber Forensics and Investigation Advice on required technologies and capabilities to address the challenges of cyber-crime, security breach and digital fraud which should help CSEs to predict, detect and mitigate security incidents. Understand the requirements of notification of forensic labs on 'examiner of electronic evidence' u/s 79A of IT Act	2 or 3
19	Cyber Training & Awareness	*(CTA-A)* KM 1201 F KM 1201 A SM 0401 F SM 0602 F SM 0602 A	2	To acquire knowledge of principles and processes addressing What, How and Why, objective and correlation with Cyber Security, its potential effects (positive or negative).	Capable to design and document training and awareness mechanisms Capable to design object oriented, result based training program for information security awareness and education	All modes

S. No.	Cyber security domain	Related modules* (Refer to Annex 1C)	No. of Days**	Training Objectives	Training Outcome	Code for mode of delivery (Online 1/F2F 2/Hybrid 3)
					while addressing policy procedures and controls.	
Miscellaneous						
20	Documentation, Implementation and Internal Auditing of CSMS (BTC-L1, STC- L2 and ATC -L3 as applicable)***	N/A	3-4	To acquire knowledge on Technical Criteria of CSMS (BTC-L1, STC- L2 and ATC -L3) with focus on: i) Enterprise Supply Chain ii) ICS requirements iii) Enterprise Cyber Vulnerability, Threat & Risk Management iv) Enterprise IT Governance, Risk and Compliance v) Enterprise Cyber Defence To acquire skill on: i) Written Communication Skills	Enhancement in ability of design of applicable controls and operational effectiveness, measurement and auditing of CSMS (BTC-L1, STC- L2 and ATC -L3)	All modes

S. No.	Cyber security domain	Related modules* (Refer to Annex 1C)	No. of Days**	Training Objectives	Training Outcome	Code for mode of delivery (Online 1/F2F 2/Hybrid 3)
21	Implementation/Execution of Cyber Crisis Management Process (CCMP)	N/A	2	1. To understand the concept of incident, event and crisis 2. Activities (anticipation, assessment, prevention and preparedness) of Cyber Crisis Processes and levels of CCMP 3. Mechanism for conducting Cyber Drill. 4. To improve the cyber security posture of the CSEs.	Broad understanding of CCMP and conduct of Cyber Drill by simulation during delivery of training by utilising the concept of purple teaming. The purple teaming is the collaborative approach to cybersecurity that brings together red and blue teams to test and improve the security posture. The purple team changes the team dynamic and culture, maximizing the contribution of each set of skills.	All modes

*Note 1: The related modules are in reference to Annex 1A in Section 3 from Certification Scheme for IT/ ICS Cyber Security Professionals (CyberPros). In this column, both Foundation and Advanced Level are mentioned to make it comprehensive as they complement each other and facilitate TBs to design their training program by using this information. TBs can use other information also based on their customer requirements.

**Note 2: The time duration (each day considered as 8 working hours) for the training programme is indicative in nature, with the assumption that training group has a basic knowledge of the topics. This is basically a journey time traversed to appreciate and connect all the topics in a structured way. For arriving to the actual number of training days, the TBs shall work with the customer for agreeing to a duration based on the knowledge, maturity, abilities and experience. While calculating the time duration, the TBs shall appreciate the distinction between the training programme and education system.

Note 3: In second column cyber security domains are specified which defines the theme and not the title of the training program. TBs can define title of the training program depending on the requirements of the customers. It may be noted that the training programs are from one to many vis-à-vis CO which is one to one and expected to provide a solution of the stated problem and handholding for implementation.

Note 4: Module of higher echelon (mentioned *in italics*) has been chosen to ensure the sufficient maturity of the trainers.

*** Note 5: This will be required by micro CSEs. The micro and medium CSEs struggle for trainings on procedural formulations and on implementation guidance. In these training programs, templates/sample SoPs are provided which are not protected or have copyright issues. This training will accelerate the knowledge creation in these segments and facilitate for rapid compliance.

Annexure 1B

Detailed training programs with extensive coverage

S No.	KM/ SM ID	Level	Title of Module	No. of days
			Knowledge Modules	
	KA-01		Knowledge Area: Network Infrastructure & Network Security (Technical)	
1.	KM-0101F	Foundation	Network Infrastructure and Administration	7
2.	KM-0101A	Advanced	Network Infrastructure and Administration	12
3.	KM-0102F	Foundation	Network Security	7
4.	KM-0102A	Advanced	Network Security	10
	KA-02		Knowledge Area: Systems (HW, VM, OS) Security (Technical)	
5.	KM-0201F	Foundation	System Infrastructure and Administration	7
6.	KM-0201A	Advanced	Systems Infrastructure and Administration	10
7.	KM-0202F	Foundation	System Security and Security Administration	5
8.	KM-0202A	Advanced	System Security and Security Administration	10
	KA-03		Knowledge Area: Software and Platform Operations Security (Technical)	
9.	KM-0301F	Foundation	Software and Platform Operations	7
10.	KM-0301A	Advanced	Software and Platform Operations	10
11.	KM-0302F	Foundation	Software and Platform Operations Security	7
12.	KM-0302A	Advanced	Software and Platform Operations Security	5
	KA-04		Knowledge Area: Secure Systems Engineering (Technical)	
13.	KM-0401F	Foundation	Secure Systems Engineering	7
14.	KM-0401A	Advanced	Secure Systems Engineering	10
	KA-05		Knowledge Area: Secure Software Design & Development (Technical)	
15.	KM-0501F	Foundation	Secure Software Design & Development	7
16.	KM-0501A	Advanced	Secure Software Design & Development	8
17.	KM-0502F	Foundation	Software Security Testing	5
18.	KM-0502A	Advanced	Software Security Testing	10
	KA-06		Knowledge Area: Enterprise Governance, Risk and Compliance (Organisational)	

S No.	KM/ SM ID	Level	Title of Module	No. of days
19.	KM-0601F	Foundation	Enterprise IT Governance, Risk and Compliance	7
20.	KM-0601A	Advanced	Enterprise Governance, Risk and Compliance	10
21.	KM-0601M	Master	Enterprise Governance, Risk and Compliance	15
	KA-07	Knowledge Area: Enterprise Supply Chain (Organisational)		
22.	KM-0701F	Foundation	Enterprise Supply Chain	5
23.	KM-0701A	Advanced	Enterprise Supply Chain	10
	KA-08	Knowledge Area: Enterprise IT and Information Security (Technical)		
24.	KM-0801F	Foundation	Foundation Module: Enterprise IT Strategy & Design	5
25.	KM-0801A	Advanced	Enterprise IT Strategy & Design	10
26.	KM-0802F	Foundation	Enterprise Info Security Strategy & Design	5
27.	KM-0802A	Advanced	Enterprise Info Security Strategy & Design	10
28.	KM-0803F	Foundation	Enterprise IT and Info Security Operations	5
29.	KM-0803A	Advanced	Enterprise IT and Info Security Operations	10
30.	KM-0804F	Foundation	Enterprise Cyber Vulnerability, Threat & Risk Management	5
31.	KM-0804A	Advanced	Enterprise Cyber Vulnerability, Threat & Risk Management	14
	KA-09	Knowledge Area: Enterprise Cyber Defence (Technical)		
32.	KM-0901F	Foundation	Enterprise Cyber Defence	7
33.	KM-0901A	Advanced	Enterprise Cyber Defence	10
34.	KM-0901M	Master	Enterprise Cyber Defence	21
	KA-10	Knowledge Area: Data Science, Data Analytics, Machine Learning (Technical)		
35.	KM-1001F	Foundation	Data Science, Data Analytics, AI/ML	5
36.	KM-1001A	Advanced	Data Science, Data Analytics, AI/ML	14
	KA-11	Knowledge Area: Cyber Forensics (Technical)		
37.	KM-1101F	Foundation	Cyber Forensics & Investigation	7
38.	KM-1101A	Advanced	Cyber Forensics & Investigation	10
39.	KM-1101M	Master	Cyber Forensics & Investigation	21
	KA-12	Knowledge Area: Cyber Security Training & Awareness (Organisational)		
40.	KM-1201F	Foundation	Cyber security Training & Awareness	7

S No.	KM/ SM ID	Level	Title of Module	No. of days
41.	KM-1201A	Advanced	Cyber security Training & Awareness	5
	KA-13	Knowledge Area: ICS Cyber Security (Technical)		
42.	KM-1301F	Foundation	ICS Cyber Security	10
43.	KM-1302F	Foundation	ICS Cyber Risk Assessment	10
44.	KM-1302A	Advanced	ICS Cyber Risk Assessment	14
45.	KM-1303A	Advanced	ICS Cyber security Design & Implementation	14
46.	KM-1303M	Master	ICS Cyber security Design & Implementation	21
47.	KM-1304A	Advanced	ICS Cyber security Operations & Maintenance	14
48.	KM-1304M	Master	ICS Cyber security Operations & Maintenance	21
Skill Modules				
	SA-01	Skill Area: Programming & Scripting (Technical)		
49.	SM-0101F	Foundation	Programming & Scripting Skills	5
	SA-02	Skill Area: Managing and securing systems, networks, applications (Technical)		
50.	SM-0201F	Foundation	Managing & Securing Skills	5
51.	SM-0201A	Advanced	Managing & Securing Skills	7
	SA-03	Managing and securing information and data (Technical/ Analytical)		
52.	SM-0301F	Foundation	Managing & Securing Skills	5
53.	SM-0301A	Advanced	Managing & Securing Skills	7
	SA-04	Skill Area: Software development lifecycle (Technical)		
54.	SM-0401F	Foundation	Software Development & Testing Skills	5
55.	SM-0401A	Advanced	Software Development & Testing Skills	7
	SA-05	Skill Area: Cyber Defence (Technical)		
56.	SM-0501F	Foundation	Cyber Defence Skills	5
57.	SM-0501A	Advanced	Cyber Defence Skills	7
	SA-06	Skill Area: Others (Technical)		
58.	SM-0601F	Foundation	Technical Skills	5
59.	SM-0602F	Foundation	Written Communication Skills	5
60.	SM-0603A	Advanced	Techno-administrative Skills	7

Note:

a. 1 Man-day equals to 8 hours and the no. of days are indicative in nature.
b. TBs can select and declare any domain from Annex 1A and/or any module from Annex 1B to demonstrate capability while applying for Scope of accreditation

Reference for Curriculum Development for a Training Course

Reproduced from Annex 1A in Section 3 from Certification Scheme for IT/ ICS Cyber Security Professionals (CyberPros)

KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
Knowledge Modules		
KA-01	***Knowledge Area: Network Infrastructure & Network Security (Technical)***	
KM-0101F	Foundation Module: Network Infrastructure and Administration	▪ Knowledge of concepts, terminology, and operations of a wide range of communications media (computer and telephone networks, satellite, fiber, wireless). ▪ Knowledge of communication methods, principles, and concepts that support the network infrastructure. ▪ Knowledge on the principles, concept, bandwidth and range of existing networks (e.g., PBX, LANs, WANs, WIFI, SCADA). ▪ Knowledge of Voice over IP (VoIP). ▪ Knowledge of the capabilities of different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts). ▪ Knowledge of computer networking concepts and protocols. ▪ Knowledge of traffic flows across the network (e.g. TCP, IP, OSI Model). ▪ Knowledge of network equipment capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware. ▪ Knowledge of network services and protocols interactions that provide network communications. ▪ Knowledge of network administration. ▪ Knowledge of scripting in the network domain. ▪ Knowledge of network hardware devices and functions. ▪ Knowledge of networking and Internet communications fundamentals (i.e. devices, device configuration, hardware, software, applications, ports/protocols, addressing, network architecture and infrastructure, routing, operating systems, etc.). ▪ Knowledge of the use of sub-netting tools.
KM-0101A	Advanced Module: Network Infrastructure and Administration	▪ Knowledge of network architecture concepts and its application including topology, protocols, and components.

KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		▪ Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware. ▪ Knowledge of local area and wide area networking principles and concepts including bandwidth management. ▪ Knowledge of network services and protocols interactions that provide network communications.
KM-0102F	Foundation Module: Network Security	▪ Knowledge of network access/ network access control mechanisms. ▪ Knowledge of network security methodologies. ▪ Knowledge of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection). ▪ Knowledge of network security implementations (e.g., host-based IDS, IPS, access control lists), including their function and placement in a network. ▪ Knowledge of scripting in the network domain. ▪ Knowledge of network access/ network access control mechanisms. ▪ Knowledge of network traffic analysis methods. ▪ Knowledge of packet-level analysis. ▪ Knowledge of network security methodologies such as testing, selection of test tools and preparation of network security test reports. ▪ Knowledge of Virtual Private Network (VPN) security. ▪ Knowledge on identification of various vulnerabilities including critical/potential in the NW devices by using various NW traffic analysis and security methods.
KM-0102A	Advanced Module: Network Security	▪ Knowledge of network security planning and management, identifying network security risk and potential control areas, technical vulnerability management, identification and authentication. ▪ Knowledge of network audit logging and monitoring, intrusion detection and prevention. ▪ Knowledge of protection against malicious code, cryptographic based services. ▪ Knowledge of network technical security architecture, design principles and design sign off. ▪ Knowledge of implementation aspects of network security such as criteria for network component, product / vendor selection. ▪ Knowledge of network management including logging, monitoring and incident response, documentation etc. ▪ Knowledge of securing communications between networks using security gates etc. ▪ Knowledge of enhanced collaboration services, network segmentation and understanding of catalogue of threads.

KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
KA-02	***Knowledge Area: Systems (HW, VM, OS) Security (Technical)***	
KM-0201F	Foundation Module: System Infrastructure and Administration	▪ Knowledge of physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage). ▪ Knowledge of virtualisation, operating systems, containers. ▪ Knowledge of system/server diagnostic tools and fault identification techniques. ▪ Knowledge of Windows Powershell, and Linux command-line tools ▪ Knowledge of virtualization technologies and virtual machine development and maintenance. ▪ Knowledge of installation, configuration, integration, and optimization of system components. ▪ Knowledge of server administration and systems engineering theories, concepts, and methods. ▪ Knowledge of server and client operating systems. ▪ Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems. ▪ Knowledge of operating system structures and internals (e.g., process management, directory structure, installed applications). ▪ Knowledge of configuration management techniques. ▪ Knowledge of operating system command-line tools. ▪ Knowledge of server diagnostic tools and fault identification techniques. ▪ Knowledge of performance tuning tools and techniques. ▪ Knowledge of the characteristics of physical and virtual data storage media. ▪ Knowledge of scripting in the systems domain. ▪ Knowledge of physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage). ▪ Knowledge of electrical engineering as applied to computer architecture (e.g., circuit boards, processors, chips, and computer hardware). ▪ Knowledge of Windows Powershell, Linux command-line tools. ▪ Knowledge of the type and frequency of routine hardware maintenance.
KM-0201A	Advanced Module: Systems Infrastructure and Administration	▪ Knowledge of cloud services platforms and models, technologies and administration. ▪ Knowledge of IIoT System Administration and Architecture.

KM-0202F	Foundation Module: System Security and Security Administration	▪ Knowledge of basic system, network, and OS hardening techniques. ▪ Knowledge of systems security testing and infrastructure audit against bill of material and deployment. ▪ Knowledge of information technology (IT) security principles and methods.

KM/ SM ID	**Knowledge / Skill Module Title**	**Curriculum (for use in assessment procedures for the expertise level)**
KM-0202A	Advanced Module: System Security and Security Administration	▪ Knowledge of Review Techniques (Documentation Review, Log Review, Ruleset Review, System Configuration Review, Network Sniffing, File Integrity Checking). ▪ Knowledge of Target Identification and Analysis Techniques (Network Discovery, Network Port and Service Identification, Vulnerability Scanning. ▪ Knowledge of Wireless Scanning (Passive Wireless Scanning, Active Wireless Scanning, Wireless Device Location Tracking, Bluetooth Scanning). ▪ Knowledge of Target Vulnerability Validation Techniques (Password Cracking). ▪ Knowledge of Penetration Testing (Penetration Testing Phases, Penetration Testing Logistics, Social Engineering).
KA-03	***Knowledge Area: Software and Platform Operations Security (Technical)***	

KM-0301F	Foundation Module: Software and Platform Operations	▪ Knowledge of identity and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML). ▪ Knowledge of system software and organizational design standards, policies, and authorized approaches relating to system design. ▪ Knowledge of middleware (e.g., enterprise service bus and message queuing). ▪ Knowledge of database systems and data administration. ▪ Knowledge of enterprise messaging systems and associated software. ▪ Knowledge of applicable business processes and operations of customer organizations. ▪ Knowledge of the capabilities and functionality associated with content creation technologies (e.g., wikis, social networking, content management systems, blogs). ▪ Knowledge of the capabilities and functionality associated with various technologies for organizing and managing information (e.g., databases, bookmarking engines). ▪ Knowledge of the capabilities and functionality of various collaborative technologies (e.g., groupware, SharePoint). ▪ Knowledge of web services (e.g., service-oriented architecture, Simple Object Access Protocol, and web service description language). ▪ Knowledge of various schemas, viz XML, JSON. ▪ Knowledge of scripting in the software domain.
KM-0301A	Advanced Module: Software and Platform Operations	▪ Knowledge of controlling costs and budgets regarding IT systems.

KM/ SM ID	**Knowledge / Skill Module Title**	**Curriculum (for use in assessment procedures for the expertise level)**
		▪ Knowledge of managing contracts with vendors (e.g., development platforms, telecommunication companies, password managers) and software licenses. ▪ Knowledge of developing IT policies and practices. ▪ Knowledge of implementing DevSecOps for microservices-based applications with service mesh.

KM-0302F	Foundation Module: Software and Platform Operations Security	▪ Knowledge of host access control mechanisms (e.g., access control list, RBAC, ABAC). ▪ Knowledge of cyber threats and vulnerabilities. ▪ Knowledge of specific operational impacts of cyber security lapses. ▪ Knowledge of authentication, authorization, and access control methods. ▪ Knowledge of the 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). ▪ Knowledge of current and emerging data encryption (e.g., Column and Tablespace Encryption, file and disk encryption) and security features in databases (e.g. built-in cryptographic key management features). ▪ Knowledge of current and emerging data remediation security features in databases.
KM-0302A	Advanced Module: Software and Platform Operations Security	▪ Knowledge of host access control mechanisms (e.g., access control list, RBAC, ABAC). ▪ Knowledge of authentication, authorization, and access control methods.
KA-04	***Knowledge Area: Secure Systems Engineering (Technical)***	
KM-0401F	Foundation Module: Secure Systems Engineering	▪ Knowledge of process engineering concepts. ▪ Knowledge of Zero Trust Architecture (ZTA). ▪ Knowledge of data classification standards and methodologies based on sensitivity and other risk factors. ▪ Knowledge of organizational process improvement concepts and process maturity models (e.g., Capability Maturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions). ▪ Knowledge of security architecture concepts and enterprise architecture reference models. ▪ Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).

KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
KM-0401A	Advanced Module: Secure Systems Engineering	▪ Knowledge of Information Technology Infrastructure Library [ITIL]. ▪ Knowledge of SSE (ISO 21827) Capability Maturity Model. ▪ Developing Cyber-Resilient Systems. ▪ Knowledge of microservices based application systems architecture, covering API gateways and service mesh.
KA-05	***Knowledge Area: Secure Software Design & Development (Technical)***	
KM-0501F	Foundation Module: Secure Software Design & Development	▪ Knowledge of capabilities and requirements analysis. ▪ Knowledge of software development models (e.g., Waterfall Model, Agile Model). ▪ Knowledge of Information Technology (IT) architectural concepts and frameworks. ▪ Knowledge of interpreted and compiled computer languages. ▪ Knowledge of secure coding techniques. ▪ Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools. ▪ Knowledge of microprocessors from a software development perspective. ▪ Knowledge of complex data structures. ▪ Knowledge of computer algorithms. ▪ Knowledge of computer programming principles. ▪ Knowledge of parallel and distributed computing concepts. ▪ Knowledge of programming language structures and logic. ▪ Knowledge of low-level computer languages (e.g., assembly languages). ▪ Knowledge of database management systems, query languages, table relationships, and views. ▪ Knowledge of query languages such as SQL (structured query language). ▪ Knowledge of data management and data standardization policies. ▪ Knowledge of data mining and data warehousing principles. ▪ Knowledge of human-computer interaction principles. ▪ Knowledge of software debugging principles. ▪ Knowledge of software design tools, methods, and techniques. ▪ Knowledge of concepts related to websites (e.g., web servers/pages, hosting, DNS, registration, web languages such as HTML).
KM-0501A	Advanced Module: Secure Software Design & Development	▪ Knowledge of cyber security and privacy principles and methods that apply to software development. ▪ Knowledge of encryption algorithms.

KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		▪ Knowledge of cryptography and cryptographic key management concepts. ▪ Knowledge of Application Security Risks (e.g., Open Web Application Security Project Top 10 list), penetration testing principles, tools, and techniques.
KM-0502F	Foundation Module: Software Security Testing	▪ Knowledge of systems testing and evaluation methods, tools, and processes. ▪ Knowledge of vast OWASP secure coding practices, web security testing.
KM-0502A	Advanced Module: Software Security Testing	▪ Knowledge of Software Security Test Plan (Strategy, Scope, Test Objective etc.) OWASP top 10 (mobile) vulnerabilities. ▪ Knowledge of interactive application security testing combines with analysis techniques and selection of tools. ▪ Knowledge of test management, test result validation & analysis and testing lifecycle.
KA-06	***Knowledge Area: Enterprise Governance, Risk and Compliance (Organisational)***	
KM-0601F	Foundation Module: Enterprise IT Governance, Risk and Compliance	▪ Knowledge of ISO 27001 (ISMS) family, ISO 27014 (ISMS) (governance). ▪ Knowledge of risk management frameworks (ISO 27005), requirements, its scoring, assessment methodologies, risk management and mitigation strategies, evaluation and validation. ▪ Knowledge of relevant laws, legal authorities, restrictions, and regulations pertaining to cyber defence activities. ▪ Knowledge of legal rules of evidence and court procedure. ▪ Knowledge of organizational security policies, security authorisation and assessment processes. ▪ Knowledge of information technology (IT) risk management policies, requirements, and procedures. ▪ Knowledge of laws, policies, procedures, or governance relevant to cyber security for critical infrastructures.
KM-0601A	Advanced Module: Enterprise Governance, Risk and Compliance	▪ Knowledge of strategies, standards, organisation's needs, intent, principles, approaches and legislation to establish the cyber security policies and processes to ensure effective management of cyber security risks in pursuit of its defined objectives. ▪ Knowledge of NIST CSF, CIS v8, IEC 62443-2-1 and other organisational frameworks and standards. ▪ Knowledge of cyber security and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data (relevant to confidentiality, integrity, availability, authentication and non-repudiation).

KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		▪ Knowledge of laws, regulations, policies, and ethics as they relate to cyber security and privacy. Knowledge of legal governance related to admissibility (e.g. Rules of Evidence). ▪ Knowledge of the organization's core business/mission processes. ▪ Knowledge of organization's risk tolerance and/or risk management approach. ▪ Knowledge of legal rules of evidence and court procedure. ▪ Knowledge of laws, policies, procedures, or governance relevant to cyber security for critical infrastructures. ▪ Knowledge of special considerations for factors like safety, potential physical impacts etc., in the risk assessment.
KM-0601M	Master Module: Enterprise Governance, Risk and Compliance	▪ Knowledge of emerging technologies, their synthesis and changing landscape of vulnerabilities and fast changing business and regulatory requirements to formulate new policies and translate them into various processes and to address the potential risks. ▪ Knowledge of NIST SP800-53 r5 controls. ▪ Knowledge of risk management frameworks NIST 800-37, requirements and its scoring, assessment methodologies, risk management and mitigation strategies, evaluation and validation, governance and trust models. ▪ Knowledge of ICT readiness and cyber insurance (ISO/IEC 27102) ▪ Knowledge of ISO 27001 (ISMS) family, ISO 27014 (ISMS) (governance), ISO / IEC 27019, IS 16335
KA-07	***Knowledge Area: Enterprise Supply Chain (Organisational)***	
KM-0701F	Foundation Module: Enterprise Supply Chain	▪ Knowledge of import/export control regulations and responsible agencies for the purposes of reducing supply chain risk. ▪ Knowledge of Supply Chain Risk management standards, processes, and practices. ▪ Knowledge of Information Technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures. ▪ Knowledge of information technology (IT) acquisition/procurement requirements. ▪ Knowledge of how to evaluate the trustworthiness of the supplier and/or product (trusted supply chain). ▪ Knowledge of the acquisition/procurement life cycle process.
KM-0701A	Advanced Module: Enterprise Supply Chain	▪ Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161) ▪ Knowledge of supply chain risk management standards, processes, and practices.

KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		▪ Knowledge of how to evaluate the trustworthiness of the supplier and/or product. ▪ Knowledge of the acquisition/procurement life cycle process. ▪ Knowledge of the supply chain ecosystem, organisation to expand the definition of the vendor, sub-contractor, service provider etc., to include an end-to-end security and an increase in the visibility of their security operation. ▪ Knowledge of mitigating maliciously tainted and counterfeit products. ▪ Knowledge of writing contracts/ RFPs, and procurement specifications to include aspects related to supply chain and extent of visibility.
KA-08	***Knowledge Area: Enterprise IT and Information Security (Technical)***	
KM-0801F	Foundation Module: Enterprise IT Strategy & Design	▪ Knowledge of enterprise, IT team supporting the business objective and operations with optimal technology solutions. ▪ Knowledge of IT baselining, financial IT analysis (covering application, infrastructure, management and user level computing). ▪ Knowledge of technology assessment and benchmarking. ▪ Knowledge of identifying IT opportunities. ▪ Knowledge of IT design principles covering alignment of IT and business strategy, target state design and target IT architecture. ▪ Knowledge of IT governance covering (IT vendor management, IT processes, IT supply and demand management, budgeting and cost allocation, service model and SLA).
KM-0801A	Advanced Module: Enterprise IT Strategy & Design	▪ Knowledge of the organization's core business/mission processes, enterprise information technology (IT) goals and objectives, nature and function of the enterprise information structure, IT architecture, information security architecture (systems, networks, applications, data, users, IT-GRC), sources, characteristics, and uses of the organization’s data assets, reporting structures and processes. ▪ Knowledge of the organisation's systems and networks (LAN, WAN) construction and topology, measures or indicators of system performance and availability, resiliency and redundancy. ▪ Knowledge of service management concepts (e.g., Information Technology Infrastructure Library [ITIL]), business continuity and disaster recovery, continuity of operations plans, crisis management protocols, processes and techniques, identification and reporting processes. ▪ Knowledge of use cases related to collaboration and content synchronization across platforms (e.g., Mobile, PC, Cloud).

KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
KM-0802F	Foundation Module: Enterprise Info Security Strategy & Design	▪ Knowledge of proactive, effective, actively supported and evolving information security strategy and design. ▪ Knowledge of planning for securing assets with changing vulnerability landscape and technology. ▪ Knowledge of preventing cyber-attacks and incidents and preparing organisations to respond to those incidents. ▪ Knowledge of Cyber Threat landscape in the organisation context and its assessment of cyber security maturity. ▪ Knowledge of preparing/documenting cyber security strategy to achieve its goals. ▪ Knowledge of design and architecting information in cyber security covering business context, conceptual layer, logical layer, implementation and reviewing the solutions with experts.
KM-0802A	Advanced Module: Enterprise Info Security Strategy & Design	▪ Knowledge of digital rights management, organization's information classification program and procedures for information compromise, privacy impact assessments. ▪ Knowledge of information security program management (policies, procedures, and regulations) and project management principles and techniques. ▪ Knowledge of vulnerability, risk and threat assessment, emerging security issues, common attack vectors on various layers, different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks), cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored), attack methods, current and emerging threats/threat vectors, cyber defence. ▪ Knowledge of types of digital forensics data and how to recognize them, deployable forensics, processes for seizing and preserving digital evidence, processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody, collection management processes, capabilities and limitations, front-end collection systems including traffic collection, filtering and selection. ▪ Knowledge of platforms and systems for an IT-enabled ISMS for asset management, patch and vulnerability management, backup management, log and event management, internal and external audits, VAPT and red-blue-purple teaming. ▪ Knowledge of information sharing from forums and sources using Threat Intelligence gathering techniques.
KM-0803F	Foundation Module: Enterprise IT and Info Security Operations	▪ Knowledge of SIEM system, mechanism of aggregation and correlation of data from security fields. ▪ Knowledge of events and response with log monitoring, analysing incidents responses (Auditing & Logging and Threat Hunting).

KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		▪ Knowledge of operational security administration such as identity and access management, key management, firewall administration and cloud SoC.
KM-0803A	Advanced Module: Enterprise IT and Info Security Operations	▪ Knowledge of enterprise incident response program, roles, and responsibilities. ▪ Knowledge of types of digital forensics data and how to recognize them, deployable forensics, processes for seizing and preserving digital evidence, processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody, collection management processes, capabilities and limitations, front-end collection systems including traffic collection, filtering, and selection. ▪ Knowledge of platforms and systems for an IT-enabled ISMS for asset management, patch and vulnerability management, backup management, log and event management, internal and external audits, VAPT and red-blue-purple teaming. ▪ Knowledge of tools and environments for automation of processes.
KM-0804F	Foundation Module: Enterprise Cyber Vulnerability, Threat & Risk Management	▪ Knowledge of risk management process, assessment of risk considering threat and vulnerabilities, likelihood of occurrence and consequences/impact. ▪ Knowledge of contact for risk-based decisions, risk assumptions, risk constraints, risk tolerance and vulnerabilities and pre-disposing conditions. ▪ Knowledge of response process to risk once determined and monitoring risk overtime.
KM-0804A	Advanced Module: Enterprise Cyber Vulnerability, Threat & Risk Management	▪ Knowledge of critical information infrastructure technologies, industry-standard security models like NIST CSF, procurement requirements, functionality, quality and security requirements, and how these will apply to specific items of supply (i.e., elements and processes), software quality assurance process, bolt-on security mechanisms, methodologies for system hardening. ▪ Knowledge of IT administration, N-tiered topologies (e.g. including server and client operating systems), system, network, and operating system hardening techniques, secure software deployment methodologies, tools, and practices, network security architecture concepts including topology, protocols, components, and principles (e.g., application of defence-in-depth), security implications of software configurations, continuous monitoring, continuous diagnostics and mitigation activities.
KA-09	***Knowledge Area: Enterprise Cyber Defence (Technical)***	
KM-0901F	Foundation Module: Enterprise Cyber Defence	▪ Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list) ▪ Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.

KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		▪ Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations. ▪ Knowledge of defence-in-depth principles and network security architecture. ▪ Knowledge of application vulnerabilities. ▪ Knowledge of cyber defence and vulnerability assessment tools and their capabilities. ▪ Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins). ▪ Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions. ▪ Knowledge of scripting and network tools (e.g., ping, traceroute, nslookup) ▪ Knowledge of incident categories, incident responses and timelines for responses. ▪ Knowledge of incident response and handling methodologies. ▪ Knowledge of system and application, security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code). ▪ Knowledge of web mail collection, searching/analyzing techniques, tools and cookies, file type abuse by adversaries for anomalous behavior, security event correlation tools, and malware analysis tools. ▪ Knowledge of web filtering technologies. ▪ Knowledge of system design tools, methods and techniques, Windows/Unix ports and services, network mapping and recreating network topologies, network analysis tools and packet-level analysis using appropriate tools (e.g., Wireshark, TCP dump).
KM-0901A	Advanced Module: Enterprise Cyber Defence	▪ Knowledge of information security systems engineering principles (NIST SP 800-160). ▪ Knowledge of current industry methods for evaluating, implementing and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities. ▪ Knowledge of new and emerging information technology (IT) and cyber security technologies. ▪ Knowledge of policy-based and risk-adaptive access controls. ▪ Knowledge of secure configuration management techniques. (e.g., Security Technical Implementation Guides (STIGs), cyber security best practices on cisecurity.org). ▪ Knowledge of MITRE ATT&CK and D3FEND frameworks, adversarial tactics, techniques, procedures, cyber-attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks). ▪ Knowledge of hacking methodologies.

KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		▪ Knowledge of social dynamics of computer attackers in a global context. ▪ Knowledge of anti-forensics tactics, techniques and procedures. ▪ Knowledge of malware analysis concepts and methodologies, signature implementation impact for viruses, malware, and attacks. ▪ Knowledge of incident reporting and dissemination procedures, procedures used for documenting and querying reported incidents, problems and events. ▪ Knowledge used to identify software communications vulnerabilities. ▪ Knowledge of industry indicators useful for identifying technology trends, and industry technologies' potential cyber security vulnerabilities. ▪ Knowledge of penetration testing principles, tools and techniques. ▪ Knowledge of root cause analysis techniques. ▪ Knowledge of key cyber threat actors and their equities, key factors of the operational environment and threat, methods and techniques used to detect various exploitation activities, exploitation techniques (e.g., gaining backdoor access, collecting/exfiltrating data, conducting vulnerability analysis of other systems in the network). ▪ Knowledge of obfuscation techniques (e.g., TOR/ Onion/ anonymizers, VPN/ VPS, encryption). ▪ Knowledge of Deception Technology and Deceptive Defences for high value assets.
KM-0901M	Master Module: Enterprise Cyber Defence	▪ Knowledge of policy-based and risk-adaptive access controls. ▪ Knowledge of secure configuration management techniques. (e.g., Security Technical ▪ Implementation Guides (STIGs), cyber security best practices on cisecurity.org). ▪ Knowledge of MITRE ATT&CK and D3FEND frameworks, adversarial tactics, techniques, procedures, cyber-attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks). ▪ Knowledge of incident reporting and dissemination procedures, procedures used for documenting and querying reported incidents, problems and events. ▪ Knowledge of industry indicators useful for identifying technology trends, and industry technologies' potential cyber security vulnerabilities. ▪ Knowledge of penetration testing principles, tools and techniques. ▪ Knowledge of root cause analysis techniques. ▪ Knowledge of key cyber threat actors and their equities, key factors of the operational environment and threat, methods and techniques used to detect various exploitation activities, exploitation

KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		techniques (e.g., gaining backdoor access, collecting/exfiltrating data, conducting vulnerability analysis of other systems in the network). ▪ Knowledge of obfuscation techniques (e.g., TOR/ Onion/ anonymizers, VPN/ VPS, encryption).
KA-10	***Knowledge Area: Data Science, Data Analytics, Machine Learning (Technical)***	
KM-1001F	Foundation Module: Data Science, Data Analytics, AI/ML	▪ Knowledge of statistics and operational analysis. ▪ Knowledge of data science tools to explore data (Python, R). ▪ Knowledge of machine learning theory and principles. ▪ Knowledge of data mining techniques.
KM-1001A	Advanced Module: Data Science, Data Analytics, AI/ML	▪ Knowledge of Data Management for Machine Learning ▪ Knowledge of Data Warehousing ▪ Knowledge of Graphs – Algorithms and Mining ▪ Knowledge of Probabilistic Graphical Models ▪ Knowledge of Ethics for Data Science ▪ Knowledge of Optimization Techniques for Analytics ▪ Knowledge of Data Management for Machine Learning ▪ Knowledge of Natural Language Processing ▪ Knowledge of Design of Experiments for Data Science ▪ Knowledge of Information Retrieval ▪ Knowledge of Data Visualization and Interpretation ▪ Knowledge of Stream Processing and Analytics ▪ Knowledge of Artificial and Computational Intelligence ▪ Knowledge of Machine Learning and Applied Machine Learning
KA-11	***Knowledge Area: Cyber Forensics (Technical)***	
KM-1101F	Foundation Module: Cyber Forensics & Investigation	▪ Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, digital scanners, electronic organizers, hard drives, memory cards, modems, network components, networked appliances, networked home control devices, printers, removable storage devices, telephones, copiers, facsimile machines, etc.).

KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		▪ Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]), file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip), types and collection of persistent data. ▪ Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files. ▪ Knowledge of concepts and practices of processing digital forensic data. ▪ Knowledge of forensics lab design configuration and support applications (e.g., VMWare, Wireshark). ▪ Knowledge of debugging procedures and tools.
KM-1101A	Advanced Module: Cyber Forensics & Investigation	▪ Knowledge of hardware reverse engineering techniques. Knowledge of software reverse engineering techniques. ▪ Knowledge of digital forensic framework covering ISO 27037, ISO 27035, ISO 27050 and ISO 27041, NIST IR – 8438.
KM-1101M	Master Module: Cyber Forensics & Investigation	▪ Knowledge of context for collecting digital evidence, principles of digital evidence, requirements for digital evidence handling and digital evidence handling processes. ▪ Knowledge of key components of identification, collection, acquisition and preservation of digital evidence, chain of custody precautions at the site of incident, roles and responsibilities, competency, use reasonable care, documentation, prioritizing collection and acquisition, and preservation of potential digital evidence. ▪ Knowledge of assuring suitability and adequacy of incident investigative methods. ▪ Knowledge of method development and assurance, General principles, General development and deployment model. ▪ Knowledge of assurance stages, requirements capture and analysis, process design, verification, implementation, validation, confirmation, deployment, review and maintenance. ▪ Knowledge of assurance models viz. In-house assurance, external assurance and mixed assurance. ▪ Knowledge of production of evidence for assurance, external assurance, mixed assurance and its production of evidence for assurance. ▪ Knowledge of pre-validation preparation, producing evidence of validation, maintenance of validation, validation of examinations and validation of investigations. ▪ Knowledge of electronic discovery foundation, principles, electronically stored information and electronic discovery process.

KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
KA-12	***Knowledge Area: Cyber Security Training & Awareness (Organisational)***	
KM-1201F	Foundation Module: Cyber security Training & Awareness	▪ Knowledge of the organisation's work roles and associated tasks, competency (knowledge and skills) requirements. ▪ Knowledge of learning assessment techniques (evaluation plans, tests, quizzes). ▪ Knowledge of computer-based training and e-learning services. ▪ Knowledge of organizational training policies. ▪ Knowledge of learning levels (i.e., Bloom's Taxonomy of learning). ▪ Knowledge of Learning Management Systems and their use in managing learnings. ▪ Knowledge of learning styles (e.g., assimilator, auditory, kinesthetic). ▪ Knowledge of modes of learning (e.g., rote learning, observation). ▪ Knowledge of organizational training systems. ▪ Knowledge of media communication and dissemination techniques. ▪ Knowledge of organizational human resource policies, processes, and procedures. ▪ Knowledge of physical and physiological behaviors that may indicate suspicious or abnormal activity. ▪ Knowledge of cyber competitions as a way of developing skills by providing hands-on experience in simulated, real-world situations.
KM-1201A	Advanced Module: Cyber security Training & Awareness	▪ Knowledge of principles of curriculum design based on an identified lead, and effective implementation of control. ▪ Knowledge of process for selection, grading, sequencing, staging and recycling of learning assets as a part of organisation's' capability. ▪ Knowledge of process for content/subject matter generation, delivery method and capturing learning experience. ▪ Knowledge of evaluation of the effectiveness of the delivery of subject matter/content.
KA-13	***Knowledge Area: ICS Cyber Security (Technical)***	
KM-1301F	Foundation Module: ICS Cyber Security	▪ Knowledge of ICS cyber security policy & program ▪ Knowledge of basics of ICS cyber risk analysis, its methodologies, categorising risk and building risk matrix ▪ Knowledge of industrial networking and network security ▪ Knowledge of ICS cyber risk mitigation and management techniques

KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		▪ Knowledge of ICS cyber security architecture to validate or verify the ICS cyber security ▪ Knowledge of ICS operations and components (SCADA, TCS, PLC etc.). ▪ Knowledge of concepts of ICS security including functionality, foundation requirements, defence of depth, security zones, conduits, channels and security levels, asset models, reference architecture. ▪ Knowledge of improving and maintaining the cyber security posture of the ICS system. ▪ Knowledge of methods to identify ICS assets and categorise them based on risk criticality ▪ Knowledge of interconnectivity and communication paths of assets in the ICS environment ▪ Knowledge of processes of ICS systems in the organisation, cyber threat libraries and stages of cyberattacks ▪ Knowledge of monitoring, reviewing and executing operational requirements to ensure the integrity of ICS network infrastructure ▪ Knowledge of security requirements of the organisation and security environment ▪ Knowledge of Virtual Private Network (VPN)- types, functions and operation, limitations, bandwidth and dynamics. ▪ Knowledge of configuration of routers and switches and ICS security system components ▪ Knowledge of hardware and software security products, features and capabilities ▪ Knowledge of network protocols and operating systems with common specifications and designs for secure ICS systems ▪ Knowledge of security perimeters, functions, protocols, standards and data encryption along with security threats and vulnerabilities facing ICS systems ▪ Knowledge of levels of security assurance and functional requirements ▪ Knowledge of elements, objectives and purpose of security controls in ICS environment ▪ Knowledge of types of models for OT security {such as Incorporation of Purdue Model for ICS Security (PERA)} ▪ Knowledge of vulnerability and patch management configuration tools and techniques ▪ Knowledge of analysis and verification process, tools and techniques for testing effectiveness of patches ▪ Knowledge of internal guidelines for managing vulnerability and patch deployment, validation and user- access ▪ Knowledge of types of system conflicts created when implementing external vendor patches and resources ▪ Knowledge of purposes of ICS systems and their dependencies on network

KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		▪ Knowledge of ICS network performance indicators and methods to assess them ▪ Knowledge of detection, identification, isolation and limitation techniques of network faults and failures in the ICS environment ▪ Knowledge of potential causes and impacts of network faults or downtime ▪ Knowledge of resolution techniques for a range of different network issues in the ICS environment ▪ Knowledge of critical information to be communicated to the organisation regarding network updates ICS network visualisation and modelling ▪ Knowledge of Impact of network performance on ICS operations ▪ Knowledge of best practices in network administration and maintenance in the ICS environment ▪ Knowledge of priorities, audience and dependencies with regards to communicating network updates in the ICS environment ▪ Knowledge of relevant programming languages for applications ▪ Knowledge of indicators of network performance
KM-1302F	Foundation Module: ICS Cyber Risk Assessment	▪ Knowledge of techniques to perform cyber risk assessment in the ICS environment ▪ Knowledge of methods to identify ICS assets and categorise them based on risk criticality ▪ Knowledge of Risk analysis methodology ▪ Knowledge of methods to categorise risk and build risk matrix ▪ Knowledge of methods to document risk analysis results ▪ Knowledge of interconnectivity and communication paths of assets in the ICS environment ▪ Knowledge of processes of ICS systems in the organisation ▪ Knowledge of cyber threat libraries and stages of cyberattacks ▪ Knowledge of elements of risk assessment and risks scenarios
KM-1302A	Advanced Module: ICS Cyber Risk Assessment	▪ Knowledge of cyber risk assessment techniques for the ICS environment ▪ Knowledge of security risks, threats and vulnerabilities in the organisation's ICS environment ▪ Knowledge of operational, safety and business risks and implications from cyber security loopholes ▪ Knowledge of possible treatments of ICS cyber risks ▪ Knowledge of key requirements and objectives of various ICS cyber risk assessments ▪ Knowledge of pros and cons of various risk mitigation treatment approaches

KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
KM-1303A	Advanced Module: ICS Cyber security Design & Implementation	▪ Knowledge of monitoring, reviewing and executing operational requirements to ensure the integrity of ICS network infrastructure ▪ Knowledge of security requirements of the organisation ▪ Knowledge of Virtual Private Network (VPN)- types, functions and operation, limitations, bandwidth and dynamics. ▪ Knowledge of security environment ▪ Knowledge of configuration of routers and switches ▪ Knowledge of hardware and software security products, features and capabilities ▪ Knowledge of network protocols and operating systems ▪ Knowledge of security perimeters, functions, protocols, standards and data encryption ▪ Knowledge of Security threats and vulnerabilities facing ICS systems ▪ Knowledge of Levels of security assurance and functional requirements ▪ Knowledge of ICS security system components ▪ Knowledge of Elements and workings of security controls ▪ Knowledge of Objectives and purpose of security controls ▪ Knowledge of Common specifications and designs for secure OT systems ▪ Knowledge of Types of models for ICS security (such as Incorporation of Purdue Model for ICS Security (PERA)) ▪ Knowledge of Methods to access ICS systems
KM-1303M	Master Module: ICS Cyber security Design & Implementation	▪ Knowledge of Industry best practices in ICS security architectures and systems design ▪ Knowledge of emerging trends and potential impacts on enterprise architecture and security controls ▪ Knowledge of Key criteria for determining required level of security controls ▪ Knowledge of New and emerging ICS security system design methodologies, tools and techniques ▪ Knowledge of Interdependencies and impact of changes on ICS systems
KM-1304A	Advanced Module: ICS Cyber security Operations & Maintenance	▪ Knowledge of vulnerability and patch management configuration tools and techniques ▪ Knowledge of analysis and verification process, tools and techniques for testing effectiveness of patch ▪ Knowledge of internal guidelines for managing vulnerability and patch deployment, validation and user- access ▪ Knowledge of types of system conflicts created when implementing external vendor patches and resources ▪ Knowledge of purposes of ICS systems and their dependencies on network

KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		▪ Knowledge of ICS network performance indicators and methods to assess them ▪ Knowledge of detection, identification, isolation and limitation techniques of network faults and failures in the ICS environment ▪ Knowledge of potential causes and impacts of network faults or downtime ▪ Knowledge of resolution techniques for a range of different network issues in the ICS environment ▪ Knowledge of critical information to be communicated to the organisation regarding network updates ▪ Knowledge of ICS network visualisation and modelling ▪ Knowledge of impact of network performance on ICS operations ▪ Knowledge of best practices in network administration and maintenance in the ICS environment ▪ Knowledge of priorities, audience and dependencies with regards to communicating network updates in the ICS environment ▪ Knowledge of relevant programming languages for applications ▪ Knowledge of indicators of network performance
KM-1304M	Master Module: ICS Cyber security Operations & Maintenance	▪ Knowledge of range of patch management configuration techniques ▪ Knowledge of internal stakeholder's requirements and guidelines for patching of ICS systems or embedded devices ▪ Knowledge of threats posed by relevant stakeholders provided with access and privilege to ICS systems or embedded devices ▪ Knowledge of types of interactions and possible conflict during patch deployment by internal and external stakeholders ▪ Knowledge of tools and techniques for safe deployment of patches in ICS systems or embedded devices host architectures (Appliances, mobile devices, laptops, firmware's) and interdependencies with ICS systems for patch updates ▪ Knowledge of vulnerability and patch management techniques and strategies and their implications on ICS system operations and legacy systems ▪ Knowledge of industry best practices, frameworks and developments in vulnerability and patch management ▪ Knowledge of tradeoffs 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

KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		▪ Knowledge of resources and capability requirements to support software- defined infrastructure in the ICS environment ▪ Knowledge of network virtualisation management and monitoring tools and methods ▪ Knowledge of scope of multi-tier networking in ICS environment ▪ Knowledge of range of network rules and programming codes ▪ Knowledge of semantics of different networks and network types in the ICS environment
Skill Modules		
SA-01	***Skill Area: Programming & Scripting (Technical)***	
SM-0101F	Foundation Module: Programming & Scripting Skills	▪ Skill in Python, Javascript languages, Shell programming/ scripting ▪ Skill in Kali Linux operating system and tools. ▪ Skill in writing code in Java, C, C++. ▪ Skill in data science and machine learning tools (Python, R)
SA-02	***Skill Area: Managing and securing systems, networks, applications (Technical)***	
SM-0201F	Foundation Module: Managing & Securing Skills	▪ Skill in diagnosing connectivity problems. ▪ Skill in discerning the protection needs (i.e., security controls) of information systems and networks. ▪ Skill in applying host/network access controls (e.g., access control list). ▪ Skill in establishing a routing schema. ▪ Skill in analyzing network traffic capacity and performance characteristics. ▪ Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance relative to the goals of the system. ▪ Skill in identifying possible causes of system performance degradation or availability and initiating actions needed to mitigate this degradation. ▪ Skill in installing, configuring and troubleshooting LAN and WAN components such as routers, hubs, and switches. ▪ Skill in maintaining databases. (i.e., backup, restore, delete data, transaction log files, etc.). ▪ Skill in maintaining directory services. (e.g., Microsoft Active Directory, LDAP, etc.).

KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		▪ Skill in preserving evidence integrity according to standard operating procedures or national standards. ▪ Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix Xen Desktop/Server, Amazon Elastic Compute Cloud, etc.). ▪ Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware). ▪ Skill in securing network communications. ▪ Skill in configuring and utilizing network protection components (e.g., Firewalls, VPNs, network intrusion detection systems). ▪ Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities in applications (e.g. S/MIME email, SSL traffic).
SM-0201A	Advanced Module: Managing & Securing Skills	▪ Skill in designing the integration of hardware and software solutions. ▪ Skill in developing, testing and implementing network infrastructure contingency and recovery plans. ▪ Skill in implementing, maintaining and improving established network security practices. ▪ Skill in determining how a security system should work (including its resilience and dependability capabilities). ▪ Skill in developing and applying security system access controls. ▪ Skill in optimizing database performance. ▪ Skill in systems integration testing. ▪ Skill in developing and deploying signatures. ▪ Skill in system, network and OS hardening techniques. (e.g., remove unnecessary services, password policies, network segmentation, enable logging, least privilege, etc.).
SA-03	***Skill Area: Managing and securing information and data (Technical/ Analytical)***	
SM-0301F	Foundation Module: Managing & Securing Skills	▪ Skill in using data dictionaries. ▪ Skill in using knowledge management and technical documentation technologies. ▪ Skill in conducting information searches. ▪ Skill in using data analysis, data mapping and trend analysis tools.
SM-0301A	Advanced Module: Managing & Securing Skills	▪ Skill in conducting capabilities and requirements analysis. ▪ Skill in conducting knowledge mapping (e.g., map of knowledge repositories). ▪ Skill in creating and deploying data dictionaries.

KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		▪ Skill in creating and deploying knowledge management and technical documentation technologies. ▪ Skill in using basic descriptive statistics and techniques (e.g., normality, model distribution, scatter plots). ▪ Skill in conducting queries and developing algorithms to analyze data structures. ▪ Skill in creating and utilizing mathematical or statistical models. ▪ Skill in designing a data analysis structure (i.e., the types of data a test must generate and how to analyse that data). ▪ Skill in developing data models. ▪ Skill in data mining techniques (e.g., searching file systems) and analysis.
SA-04	***Skill Area: Software development lifecycle (Technical)***	
SM-0401F	Foundation Module: Software Development & Testing Skills	▪ Skill in writing test plans. ▪ Skill in conducting test events.
SM-0401A	Advanced Module: Software Development & Testing Skills	▪ Skill in configuring and optimizing software. ▪ Skill in conducting software debugging. ▪ Skill in developing operations-based testing scenarios.
SA-05	***Skill Area: Cyber Defence (Technical)***	
SM-0501F	Foundation Module: Cyber Defence Skills	▪ Skill in detecting host and network-based intrusions via intrusion detection technologies (e.g., Snort). ▪ Skill in generating queries and reports. ▪ Skill in performing packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump). ▪ Skill in using network management tools to analyze network traffic patterns (e.g., simple network management protocol). ▪ Skill in identifying, modifying and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files). ▪ Skill in using binary analysis tools (e.g., Hexedit, command code xxd, hexdump). ▪ Skill in one-way hash functions (e.g., Secure Hash Algorithm [SHA], Message Digest Algorithm [MD5]). ▪ Skill in identifying common encoding techniques (e.g., XOR, ASCII, Unicode, Base64, Uuencode, URL encode).

KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		▪ Skill in verifying the integrity of all files. (e.g., checksums, Exclusive OR, secure hashes, check constraints, etc.) ▪ Skill in reading and interpreting signatures (e.g., snort). ▪ Skill in applying security controls. ▪ Skill in using security event correlation tools. ▪ Skill in performing root cause analysis.
SM-0501A	Advanced Module: Cyber Defence Skills	▪ Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems. ▪ Skill of identifying, capturing, containing and reporting malware. ▪ Skill in using social engineering techniques. (e.g., phishing, baiting, tailgating, etc.). ▪ Skill in using penetration testing tools and techniques. ▪ Skill in using protocol analyzers. ▪ Skill in analyzing memory dumps to extract information. ▪ Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK). ▪ Skill in conducting audits or reviews of technical systems. ▪ Skill in reviewing logs to identify evidence of past intrusions. ▪ Skill in assessing security controls based on cyber security principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cyber security Framework, etc.). ▪ Skill in auditing firewalls, perimeters, routers and intrusion detection systems.
SA-06	***Skill Area: Others (Technical)***	
SM-0601F	Foundation Module: Technical Skills	▪ Skill in conducting system/server planning, management, and maintenance. ▪ Skill in correcting physical and technical problems that impact system/server performance. ▪ Skill in troubleshooting failed system components (i.e., servers) ▪ Skill in monitoring and optimizing system/server performance. ▪ Skill in recovering failed systems/servers. (e.g., recovery software, failover clusters, replication, etc.). ▪ Skill in operating system administration. (e.g., account maintenance, data backups, system performance, install and configuring new hardware/software). ▪ Skill in setting up physical or logical sub-networks that separate an internal local area network (LAN) from other untrusted networks. ▪ Skill in configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers, as appropriate)
SM-0602F	Foundation Module: Written Communication Skills	▪ Skill in technical writing.

KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		▪ Skill in using various open-source data collection tools. ▪ Skill in utilizing virtual collaborative workspaces and/or tools.
SM-0602A	Advanced Module: Written Communication Skills	▪ Skill in documenting and communicating complex technical and programmatic information. ▪ Skill in writing, reviewing and editing cyber-related Intelligence/assessment products from multiple sources. ▪ Skill in building inclusivity and documenting/formulating creative thinking. ▪ Skill in communicating the legal perspective connecting standards and business environment.
SM-0603A	Advanced Module: Techno-administrative Skills	▪ Skill in oral and written communication meant for the Board and Executive levels. ▪ Skill in strategic and trans-disciplinary thinking, such as IT-OT convergence, people-process-technology integration. ▪ Skill in customer and users' orientation.

SECTION 5

RULES FOR USE OF SCHEME MARK

1. Introduction

1.1 The accreditation Scheme for TBs are designed and developed as per international best practices.

1.2 The 'Scheme Mark' denotes the Mark that is assigned to the accredited TBs.

1.3 The Mark is allowed to be used for promotion by accredited TBs, who are allowed to display the mark in off-product(s) as per the prescribed rules mentioned in the subsequent paras of this document.

1.4 Further, it is the collective responsibility of the NCIIPC and QCI and its constituent accreditation boards to keep an oversight on the use of Mark.

2. Purpose

The QCI and its constituent accredited organisations can benefit 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 organisations displaying the Mark 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.

3. Objective

3.1 The objective of this document is to establish rules for use of the Scheme Mark.

3.2 This document sets out the conditions that must be followed by accredited TBs that are permitted to use the logo or symbols. They are however, only authorised to issue participation certificates for the course enrolled by the candidate without the use of Scheme logo.

3.3 This document establishes the process to be adopted by the Scheme Manager for the grant of use of Scheme Mark to accredited TBs.

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 as Entities

5.1.1 The Mark holders that have been approved under the Scheme, are eligible to use Scheme

Mark. They are required to submit an application authorising them for Use of Scheme Mark
(refer to Annex A). As per the contract between the Scheme Manager (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.

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

5.2 **Oversight Responsibility**

5.2.1 The QCI secretariat is responsible to establish, implement, and amend this procedure. The Mark Holder are responsible to comply with the procedure, specifically undertaking surveillance or re- certification assessment.

5.2.2 The Mark Holder should have a strong market surveillance system to ensure that compliance is met at all times.

5.2.3 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.

5.3 **Rules for Use of Scheme Mark**

5.3.1 The Mark holder needs to comply with applicable criteria in totality.

5.3.2 The Scheme Mark is allowed to be used only by accredited Training Bodies.

5.3.3 The mark may also be used by the accredited TBs for their promotion. However, they are not allowed to use the same while issuing training certificate to their clients.

5.3.4 In some cases, if a Mark Holder has acquired Marks from different Scheme, he/she is required to seek explicit approval from QCI to affix multiple marks together.

5.3.5 A Mark Holder, which has been a subject to important changes or overhauls, aiming to modify its original mandate after it has secured approval, must apply de novo.

5.3.6 The Scheme Mark may be used as any photographic reduction or enlargement. The colour Scheme of the Marks shall be the same as described below. A different combination of the colour Scheme shall not be used.

5.3.7 During the photographic reduction and enlargement, sufficient care to be exercised to ensure that there is deviation in the aspect ratio and colour degradation/change.

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

5.3.9 The Mark holder, upon suspension or withdrawal of its attestation, shall discontinue use of all advertising matter that contains any reference to its attestation status.

5.3.10 In case the Scheme Mark is observed to be used by a Mark holder in contravention to the 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”.

5.3.11 Depending upon the degree of violation, suitable action(s) may range from advice for corrective actions, to withdrawal of certification, especially in situations of repeated violations. In case the Mark holder does not take suitable action to address the wrong usage of the Scheme Mark, the QCI may suspend/withdraw its accreditation.

5.3.12 If a Mark holder's accreditation is suspended; its attestation cancelled, withdrawn or discontinued, it is the Mark holder's responsibility 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. QCI or the Scheme Manager that has approved the Mark holders needs to ensure compliance as stated above.

5.3.13 The Mark holders shall sign a legally enforceable agreement with the Scheme Manager, QCI whereby it is allowed to use the Scheme Mark, after agreeing to all the relevant conditions as described in this document.

5.3.14 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.

5.3.15 Misuse scenarios:

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

d. 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 training program, written permission needs to be sought from the respective organisation.

e. 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.

6. Conditions for use of Scheme Mark by Mark Holder Organisations (TBs)

Following conditions shall apply for use of Scheme Mark:

6.1 The Scheme Mark may be used in publicity material, pamphlet, letterheads, other similar stationary, media for exchange of any communication, for promoting the awareness of the Scheme, the Scheme Mark, etc.

6.2 While using the above documents, care shall be taken to ensure that the Mark is used only with respect to the Mark holder and it shall 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 company are also certified/attested.

6.3 The Mark holder shall not make any misleading claims with respect to the Scheme Mark.

6.4 It shall not use the Scheme Mark in such a manner as to bring the Scheme Owner (NCIIPC) QCI (Scheme Manager), into disrepute.

7. Conditions for Use of the Scheme Mark by TBs

7.1 The Scheme Mark will be displayed only on the competency profile certificate issued to them by an accredited TBs. The TBs will not use or display the Scheme Mark anywhere else. This mark will not be used by any client of TBs.

7.2 The TBs shall submit an undertaking placed at Annex B of this Section once certified, committing to the requirement of the Scheme through their accredited TBs.

7.3 Once the Mark holder is certified by the QCI or QCI accredited TBs, it shall require the clients / trainers to fill up in duplicate the contract form, template for which is enclosed in Annex A of this Section.

7.4 The accredited TBs shall forward the filled contract form received from the accredited TBs 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 as a minimum the following information:

7.4.1 Name and address of the Mark holder;
7.4.2 Legal entity Status (with evidence);
7.4.3 Names of the top management/ownership details;
7.4.4 Details of the certification granted – number, validity, etc.;
7.4.5 Scope of certification granted to the Mark holder;
7.4.6 Any other significant detail(s) considered as relevant.

7.5 The TBs are required to submit an undertaking to the respective accredited TBs for abiding by the Rules for Use of Certification Mark.

7.6 Upon receiving the signed contract form from QCI, the attestation body shall issue the certificate, inform the Mark holder regarding permission for using the Scheme Mark, and also forward the signed contract form to them.

7.7 The contract between QCI and the Mark holder shall be valid as long as the later holds valid accreditation under the Scheme or unless is otherwise advised to do so.

8. Design of the Mark

8.1 Attestation of accredited TBs

8.2 The Scheme Mark below, is only allowed to be used by the accredited TBs 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 TB**	
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 TBs)

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 certification 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, the Mark holder agrees to go through the appeal procedure under the Scheme and accepts its decision as final.

2.4. The 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. The Mark holder shall nominate the chief executive or an authorized signatory for the agreement as the point of contact with QCI.

2.7. **The Mark holder hereby accepts and agrees with the above terms as documented in this agreement.**

1. Signature :

Name of Mark holder: _____

(the chief executive of the organization 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 : _____