



NCIIPC – QCI Initiative

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

Issue No. 1 | Feb 2024

**Personnel Certification Scheme for
IT/ICS Cyber Security Professionals**



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 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 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 is a part of CAF that pertains to Personnel Certification Scheme for IT/ICS Cyber Security Professionals. Certification Bodies for Persons, hereafter have been referred as PrCBs in this document.



ACKNOWLEDGEMENT

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

At the outset, we would specifically like to express our gratitude to Shri Navin Kumar Singh, DG, NCIIPC for giving us the opportunity to partner on the initiative of securing the cyber security ecosystem. We further extend our gratitude to Shri Lokesh Garg (DDG), NCIIPC and Col. K. Pradeep Bhat (Retd.) (Consultant), NCIIPC for their contribution in 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. 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) and members 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 Krishnamurthy Srinivasan, conformity assessment expert.

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

Dr. Manish Pande
Director and Head
PADD, QCI



Contributors

1. Steering Committee

S No.	Name	Organization
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	Organization
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	Persistent System Ltd.
6	Sh. Anand Shankar	Power Grid Corporation of India
7	Sh. Anand Deep	National Accreditation Board for Certification Bodies
8	Sh. Anurag Rastogi	National Accreditation Board for Education and
9	Sh.Ashutosh	Indian Computer Emergency Response Team
10	Prof. Faruk Kazi	Veermata Jijabai Technological Institute
11	Sh.Praveen Kumar	Noida Power Corporation Limited
12	Ms. Reena Garg	Bureau of Indian Standards
13	Prof. Sandeep Shukla	IIT Kanpur
14	Ms. Seema Mittal	National Critical Information Infrastructure Protection
15	Sh.Shaleen	BSES Rajdhani Ltd.
16	Sh. Sivakumar V	Central Power Research Institute
17	Sh. Sushil Kumar	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	Organization
Chair		
1	Dr. Rajesh N. Pillai	Defence Research and Development Organization
Members		
2	Sh. Ajay Bagati	Bharat Heavy Electricals Ltd.
3	Sh. Anand Deep Gupta	National Accreditation Board for Certification Bodies
4	Sh. Anurag Rastogi	National Accreditation Board for Education and
5	Sh. Atul Gupta	Standardisation Testing and Quality Certification
6	Sh. A. K. Patel	NTPC Limited
7	Col. Debashish Bose	National Security Council Secretariat
8	Sh. Harry Dhaul	Independent Power Producers Association of India
9	Dr. Manju Mam	National Power Training Institute
10	Sh. Manoj Belgaonkar	SIEMENS Limited.
11	Sh. Reji Pillai	India Smart Grid Forum
12	Sh. Samir Matondkar	Larsen & Toubro Limited
13	Sh. Sandeep Puri	NHPC Limited
14	Ms. Seema Shukla	TIC Council
15	Sh. Sundeep Kumar	Bureau of Indian Standards



SECTION 1

INTRODUCTION



1. Background

- 1.1. Critical Sector Entities (CSEs) require IT/ICS Cyber Security Professionals with varied competencies to design, implement, operate and manage cyber security with respect to their businesses, industrial processes and underlying information infrastructures, so as to bring cyber resilience in their respective organizations.
- 1.2. The CSEs are increasingly dependent on cyber security professionals to handle cyber security threats and risks, related to their complex Information Technology (IT) and Operational Technology (OT) systems. However, there is a dearth of certified cyber security professionals with proven knowledge, skills and capabilities to handle the domain of cyber security w.r.t. Industrial Control Systems (ICS), convergence of IT and ICS, and its inter-dependencies within and across the sectors.
- 1.3. The certification scheme for cyber security professionals is designed with the objective of creating a pool of certified professionals, where knowledge and skills will be assessed for further attestation by independent bodies.
- 1.4. The Scheme defines the set of competency-profiles that are designed for the attestation of knowledge, skills and expertise levels of cyber security professionals with regards to different domains. This in turn will help organizations to map their domains to different activities and tasks required in every job role. The competence of cyber security professionals include aspects that establish their ability to tackle situations commensurate to the level of certification acquired by them. Cyber security professionals can acquire their knowledge and skills by their own individual efforts or by seeking training from training bodies.
- 1.5. The Scheme defines a certification process to assess the competence and expertise levels of cyber security professionals through third-party attestation carried out by Certification Bodies for Persons hereinafter referred to as PrCBs.

2 Objective

- 2.1. The principal objective of Personnel Certification Scheme for cyber security professionals, hereinafter referred to in this document as the 'Scheme', is to provide a framework that equitably attests and certifies the competence of cyber security professionals. The competency criteria and expertise levels for cyber security professionals can be used by:
 - 2.1.1. IT/ICS system owners, for creating a certified pool of cyber security professionals in different domains. The pool may be created either through hiring, outsourcing or training their workforce. The competency profiles and expertise levels defined in the Scheme may be used as a guideline by CSEs for defining cyber security job roles in different domains. It may be used for hiring, identification of knowledge/skills/expertise levels of their workforce, internal transfers and/or career advancement.
 - 2.1.2. Cyber security professionals and cyber security aspirants to establish their competency through an independent body for employment and career enhancement.



The individuals, who seek a meaningful career in IT/ICS cyber security sector may be able to upgrade their competencies and expertise levels in their respective domains in order to be aligned with the current scenario.

- 2.1.3. Training Bodies (TBs) for designing training courses to develop knowledge, skills and expertise levels of individuals in different domains. Also, TBs may be able to offer specialised courses to organizations for the development of cyber security in workplace.
- 2.1.4. Consultancy Organizations (COs) to have certified cyber security professionals to demonstrate their organizational competencies.

3 Scope

- 3.1. This document aims to define and describe the elements of certification of cyber security professionals that include competence criteria, certification process, requirements of PrCBs and rules for the Scheme Mark.
- 3.2. It may be noted that though this Scheme is developed primarily for CSEs, it does not preclude organizations in other sectors from adopting the framework to improve their cyber security resilience.

4 Structure of the document

This document is divided into seven sections, as under:

Section 1: Introduction

Section 2: Governing Structure

Section 3: Certification Criteria (Competence Profiles for cyber security professionals)

Section 4: Certification Process

Section 5: Requirements for Certification Bodies for Persons (PrCBs)

Section 6: Provisional Approval System

Section 7: 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 its family of standards and IEC 62443. In case of any differences in terminology, the definitions in the Information Technology Act, 2000 [As Amended by Information Technology (Amendment) Act 2008] shall prevail, wherever applicable.

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



- 5.2. **Accreditation Body** - authoritative body that performs accreditation. The authority of an accreditation body can be derived from government, public authorities, contracts, market acceptance or Scheme owners.
- 5.3. **Applicant for Personnel Certification** - person who applies for the certification process.
- 5.4. **Approval** - permission for a product / process to be marketed or used for stated purposes or under stated conditions. Approval can be based on fulfilment of specified requirements or completion of specified procedures.
- 5.5. **Asset** - anything that has value to an individual, an organization or a government.
- 5.6. **Asset Owner** - individual or company responsible for one or more assets.
- 5.7. **Assessment** - process that evaluates the fulfilment of the Scheme requirements by a person.
- 5.8. **Attest** - process that confirms the conformance of the entity and individual certified, inspected, accredited, or approved.
- 5.9. **Attestation** - issue of a statement, based on a decision following review that is in fulfilment of specified requirements has been demonstrated. The resulting statement, referred to in this Standard as a “statement of conformity”, conveys the assurance that the specified requirements have been fulfilled. Such an assurance does not, of itself, afford contractual or other legal guarantees. First-party and third-party attestation activities are distinguished by the terms. For second-party attestation, no special term is available.
- 5.10. **Candidate for Personnel Certification** - applicant who has fulfilled specified prerequisites and has been admitted to the certification process.
- 5.11. **Certificate** - document issued by a certification body under the provisions of this Standard, indicating that the named person has fulfilled the certification requirements.
- 5.12. **Certification** - third-party attestation related to products, processes, systems or persons. Certification of a management system is also called registration. Certification is applicable to all objects of conformity assessment except for conformity assessment bodies themselves, to which accreditation is applicable.
- 5.13. **Certification Requirements** - specified set of requirements, including requirements of the Scheme to be fulfilled in order to establish or maintain certification.
- 5.14. **Certification Scheme** - competence and other requirements related to specific occupational or skilled categories of persons.
- 5.15. **Certified person** - a person who holds a certificate.
- 5.16. **Competence** - ability to apply knowledge and skills to achieve intended results



- 5.17. **Complaint** - expression of dissatisfaction, other than appeal, by any person or organization to a conformity assessment body or accreditation body, relating to the activities of that body, where a response is expected.
- 5.18. **Computer Resource** - computer, communication device, computer system, computer network, data, computer database or software [Information Technology Act, 2000 {as amended by Information Technology (Amendment) Act 2008}].
- Note: The system is also used to describe the ICS elements. Further the word ICS also includes OT/IACS elements. At places where required, the terms OT and IACS are explicitly defined.
- 5.19. **Conformity Assessment** - demonstration of the fulfilment of specified requirements. Conformity assessment includes activities defined in this document and is not limit to testing, inspection, validation, verification, certification or accreditation.
- 5.20. **Conformity Assessment Body** - body that performs conformity assessment activities, excluding accreditation. The CAF includes following conformity assessment bodies:
- 5.20.1 Certification Body (CB)
 - 5.20.2 Inspection Body (IB)
 - 5.20.3 Certification Body for Persons (PrCB)
- 5.21. **Conformity Assessment Framework** - structure of processes and specifications, related to conformity assessment system, designed to support the accomplishment of a specific task. There are various conformity assessment schemes that can be used to determine whether specified requirements are fulfilled, they include but are not limited to inspection, evaluation, audit of management system etc. In a framework, these conformity assessment schemes / system share common vocabulary, principles and family of standards which ensure interoperability of various schemes.
- 5.22. **Conformity Assessment System** - set of rules and procedures for the management of similar or related conformity assessment schemes. A conformity assessment system can be operated at an international, regional, national, sub-national, or industry sector level.
- 5.23. **Conformity Assessment Scheme** - set of rules and procedures that describes the objects of conformity assessment identifies the specified requirements and provides the methodology for performing conformity assessment. A scheme can be managed within a conformity assessment system. A scheme can be operated at an international, regional, national, sub-national, or industry sector level. A scheme can cover all or part of the conformity assessment functions.
- 5.24. **Critical Information Infrastructure (CII)** - computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.



- 5.25. **Critical Sector** - a sector that has been designated as critical to the nation by appropriate authority.
- 5.26. **Critical Sector Entity (CSE)** - entities of critical sectors, whose assets, systems, and networks are so vital that their incapacitation or destruction would have a debilitating impact on national security, economy, public health or public safety, or any combination.
- 5.27. **Cyber Crisis Management Plan** - 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.
- 5.28. **Cyber Security Domains** - distinct technical/ organizational capabilities of processes, people and technology that a CSE must have to meet its cyber security objectives successfully.
- 5.29. **Cyber Security Functions** - technical and management activities that organizations need to carry out to be cyber resilient. Organizations implement the cyber security functions through institutionalised practices and processes that are carried out by a trained workforce, enabled by technology and tools. The process, people and technology combined together will enable the organizations to accomplish their mission, fulfil their legal and regulatory requirements, maintain their day-to-day functions, and protect their assets and individuals.
- Cyber security functions defined in the Scheme are Govern and Administer (GA), Acquire and Provision (AP), Operate and Maintain (OM), Analyse & Investigate (AI), Train and Enable (TE), Identify (ID), Protect (PR), Detect (DE), Respond (RP), Recover (RC). Description of each of these functions are given in Annex D of Section 3 in this document.
- 5.30. **Cyber Security Management System (CSMS)** - system designed and implemented by a CSE in order to establish and maintain cyber security resilience in an organization.
- 5.31. **Cyber Security** - protecting information, equipments, devices, computer and computer resources, communication devices and the information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction [Information Technology Act, 2000 {As Amended by Information technology (Amendment) Act 2008}]
- 5.32. **Cyber Security Professional** - individual seeking a meaningful career in IT/ICS cyber security and aspires to demonstrate competence in one or more cyber security domains and acquire certifications.
- 5.33. **Cyberspace** - information and operation infrastructure within and across organizations which are interconnected using public and private networks. They are functional in a federated manner for enable the delivery of critical functions, business and industrial services, operations and capabilities.



The interdependent network of information technology infrastructures which includes the Internet, telecommunications networks, computer systems, embedded processors and controllers in critical sectors / industries of the nation.

The complex environment resulting from the interaction of people, softwares and the Internet services are facilitated by the means of integrated technological devices and networks.

- 5.34. **Distributed Control System** - type of control system where the elements are dispersed but operated in a coupled manner. Distributed control systems may have shorter coupling time constants than those typically found in ICS systems. Distributed control systems are commonly associated with continuous processes such as electric power generation, oil and gas refining, chemical, pharmaceutical and paper manufacture, as well as discrete processes such as automobile and other goods manufacturing, packaging and warehousing.
- 5.35. **Examination** - mechanism which is part of the assessment in order to measure a candidate's competency through multiple mediums such as written, oral practical and observational, as defined in the Scheme.
- 5.36. **Examiner** - competent person for conducting and scoring an examination, where it requires professional judgements.
- 5.37. **Framework** - structure of processes and specifications designed to support the accomplishment of a specific task.
- 5.38. **Impartiality** - objectivity with regard to the outcome of a conformity assessment activity. Objectivity can be understood as freedom from bias or freedom from conflict of interest.
- 5.39. **Impartiality for Personnel Certification** - presence of objectivity, fairness and equal opportunity for success provided to each candidate in the certification process
- 5.40. **Invigilator** - person authorized by the certification body who administers or supervises an examination but does not evaluate the competence of the candidate
- 5.41. **Independence** - freedom of a person or organization from the control or authority of another person or organization. Example: A conformity assessment body can be independent from the person who is the object of conformity assessment or from the organization providing the object of conformity assessment
- 5.42. **Industrial Automation and Control System (IACS)** - collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process.
- 5.43. **Industrial Automation and Control System (ICS/IACS)** - general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures.



An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy) and can affect or influence the safe, secure and reliable operation of an industrial process/Operation.

- 5.44. **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 (ISO 27000:2018).

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (NIST SP 800-53 Rev 5).

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

- 5.46. **Mark Holder** - entities that are authorized to use the Scheme Mark. These include Conformity Assessment Bodies (CAB), namely Certification Bodies (CB) and Inspection Bodies (IB), Certification Bodies of Personnel (PrCB) and their client base, and Specialized Professional Bodies (SPB), namely Training Bodies (TB) and Consultancy Organizations (COs), excluding their client base.

- 5.47. **Mark Owner** - The person or organization responsible for developing, issuing and managing of the Scheme Mark.

- 5.48. **Object of Conformity Assessment** - entity to which specified requirements apply.

Example: product, process, service, system, installation, project, data, design, material, claim, person, body or organization, or any combination thereof. The term “body” is used in this framework to refer to conformity assessment bodies and accreditation bodies. The term “organization” is used in its general meaning and may include bodies according to the context.

- 5.49. **Off-Product** - generic term for publicity material, pamphlets, and letterheads, other similar stationery, media for exchange of any communication.

- 5.50. **Operational Technology** - programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/ devices detect or cause a direct change through the monitoring and/ or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms (NIST SP 800-37 Rev 2).

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

- 5.52. **Principles of conformity assessment** - conformity assessment is a series of three functions that satisfy a need or demand for demonstration that specified requirements are fulfilled. These functions are selection, determination, review and attestation.



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

- 5.53. **Protected System** - any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure [Information Technology Act, 2000 {as amended by Information Technology (Amendment) Act 2008}].
- 5.54. **Qualification** - demonstrated education, training and work experience, where applicable.
- 5.55. **Review** - verification of the suitability, adequacy and effectiveness of selection and determination activities, and the results of these activities, with regard to fulfilment of specified requirements by an object of conformity assessment
- 5.56. **Scheme Mark** - a protected mark owned by QCI (on behalf of NCIIIPC), 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”.
- 5.57. **Scope of Attestation** - range or characteristics of objects of conformity assessment covered by attestation.
- 5.58. **Supervisory Control and Data Acquisition System (SCADA system)** - type of loosely coupled distributed monitoring and control system commonly associated with electric power transmission and distribution systems, oil and gas pipelines, and water and sewage systems. These definitions are specific to IT / OT environment for ICS systems.
- 5.59. **Stakeholder** - person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity.
- 5.60. **Surveillance** - systematic iteration of conformity assessment activities as a basis for maintaining the validity of the statement of conformity.
- 5.61. **Suspension** - temporary invalidation of the statement of conformity for all or part of the specified scope of attestation.
- 5.62. **Validity** - evidence that the assessment measures what it is intended to measure, as defined by the Certification Scheme.
- 5.63. **Vulnerability** - weakness of an asset or control that can be exploited by a threat.
- 5.64. **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
BIS	Bureau of Indian Standards
CAB	Conformity Assessment Body
CAF	Conformity Assessment Framework
CB	Certification Body
CC	Certification Committee
CERT-In	Indian Computer Emergency Response Team
CII	Critical Information Infrastructure
CMMI	Capability Maturity Model Integration
CO	Consultancy Organization
CSA	Cyber Security Agency
CSE	Critical Sector Entity
CSMS	Cyber Security Management System for IT/ ICS
DCS	Distributed Control System
GRC	Governance, Risk, and Compliance
IACS	Industrial Automation and Control System
IAF	International Accreditation Forum
IB	Inspection Body
ICS	Industrial Control System
IEC	International Electrotechnical Commission
IIoT	Industrial Internet of Things
ISMS	Information Security Management System
IS	Indian Standards
ISO	International Organization for Standardisation
IT	Information Technology
ITAA	Information Technology Association of America
KA	Knowledge Area
KM	Knowledge Module
MSC	Multi-stakeholder committee
NABCB	National Accreditation Board for Certification Bodies
NCIIPC	National Critical Information Infrastructure Protection Centre
NIST	National Institute of Standards and Technology
NSAB	National Security Advisory Board
NSCS	National Security Council Secretariat
NTRO	National Technical Research Organization
OA	Office Assessment



Abbreviation	Acronym
OT	Operational Technology
PLC	Programmable Logic Controller
PrCB	Certification Body for Persons
QCI	Quality Council of India
RTI	Right to Information
SC	Steering Committee
SCADA	Supervisory Control and Data Acquisition
SM	Skill Module
SO	Scheme Owner
SPB	Specialised Professional Body
SSD	Secure Software Development
TB	Training Body
TC	Technical Committee
TSA	Technology & System Security Architecture
WA	Witness Assessment

SECTION 2

GOVERNING STRUCTURE



1. Objective

The objective of this section is to define the governing structure of the Scheme and the roles and responsibilities of various 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 provide guidance 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 relevant day to day and routine operations are handled smoothly. Following activities/ decisions are delegated to the Scheme Manager:
 - a. Ensure that information about the Scheme is made publicly available and to 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 operating procedures of the Scheme, particularly 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 from the Scheme Manager 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.
 - e. Participate in all meetings of Committees – Steering, Technical and Certification, as needed for the development and management of the Scheme, as and when organized by the Scheme Manager.

2.2 Roles and Responsibilities of the Scheme Manager

- 2.2.1 Responsible for all activities related to the upkeep of scheme documents. Information regarding the schemes will be continuously updated on its website.
- 2.2.2 Responsible for establishing, implementing and maintaining scheme requirements.



- 2.2.3 Ensure that sufficient evidence is maintained to justify that the conformity assessment activity and the criteria selected for the approval of the PrCBs.
- 2.2.4 Ensure that the scheme documents, including the criteria and process to assess conformity are publicly available.
- 2.2.5 Whenever the Scheme Manager provides any clarification about the Scheme to any interested party, it shall ensure that the information is also made available to all the bodies within the Scheme.
- 2.2.6 Have a legally enforceable agreement with PrCBs to ensure that the PrCBs and the cyber security professionals use the Scheme as published, without any additions or reductions, and are in compliance with the rules for applying the symbol/ statement/ mark, as applicable.
- 2.2.7 As the provider of provisional approval, mandate the approved PrCBs to provide reasonable access and cooperation as necessary to enable the QCI assessment team, which includes assessors, technical experts, observers and regulators to assess its 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 PrCBs 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 its own or external, which defines 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 PrCBs' clients, wherever necessary, and by other parties interested in the Scheme.
- 2.2.11 Include all the necessary components like describing responsibilities 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 impacts the operationalisation of the Schemes.

3. Governing Structure

- 3.1 The governing structure of the Scheme comprises 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 Scheme Manager) on behalf of NCIIPC (being the SO).

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

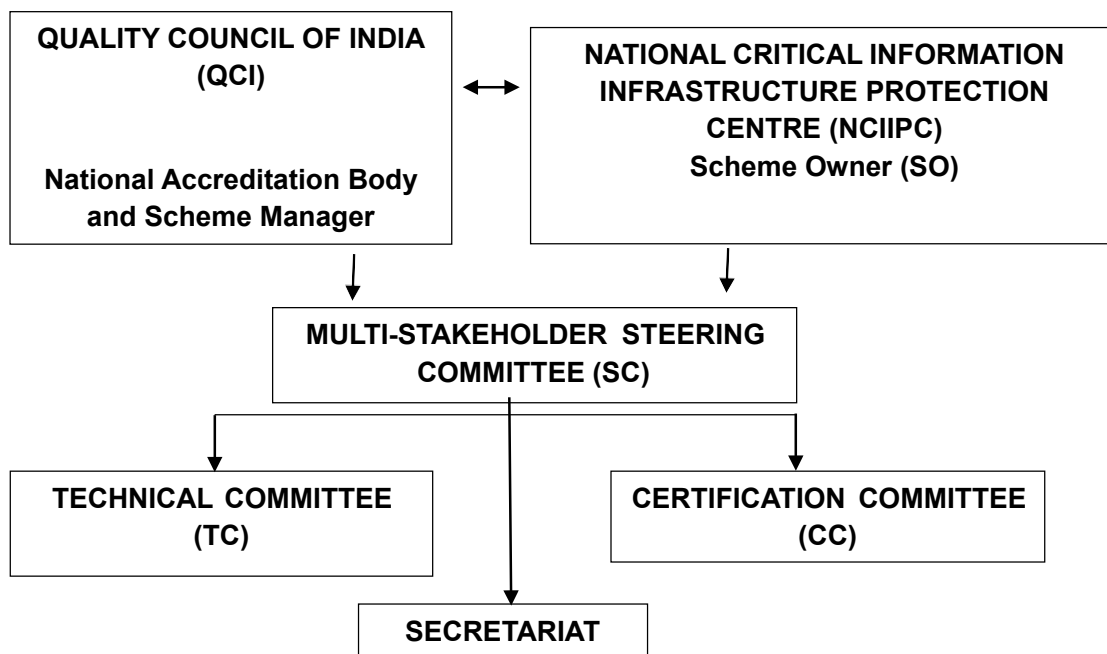


Figure 2.1: Governing Structure

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 organizations, training bodies, testing laboratories, user associations, academic/ research bodies, manufacturers of products, providers of services and representatives of organizations working in related areas, etc..
- 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 an organizational representative.
- 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 for 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 organizations as members with a definitive term, the Secretariat may call one or more organizations/entities as special invitees.
- 3.3.8 A minimum of one-third members shall constitute the quorum for each committee meeting.
- 3.3.9 Minutes of the meeting are to be issued by the Secretary of the committee with consent of the respective Chairs of the Committees.
- 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 collate the documents of the respective Committee for their review, inputs and consent so that it is approved by the respective Chair of the Committees.
- 3.3.13 The Chair of TC and CC may present the results of the deliberations of their respective committees to SC for information. SC may advise/ guide only on policy-related matters.

4. Multi-stakeholder Steering Committee (SC)

4.1 Membership

The SC shall comprise of the following:

- 4.1.1 Chairperson – Seasoned professional considered to be well respected by Government and Industry alike, can be in individual capacity.
- 4.1.2 Nominees from the concerned Ministries – Representative from the Ministries responsible for the critical sectors, namely Banking, Financial Services & Insurance, Telecom, Government, Power & Energy, Transport, Strategic Enterprises and Healthcare, representative from the regulatory bodies responsible for the critical sectors, such as Central Electricity Authority (CEA), Reserve Bank of India (RBI) etc.
- 4.1.3 Government Agencies – Representative from government agencies, namely NCIIPC, National Security Advisory Board (NSAB), and National Security Council Secretariat (NSCS).
- 4.1.4 Chairperson SC may co-opt more members in consultation with Scheme Owner and Manager.
- 4.1.5 Secretariat – Quality Council of India

4.2 Terms of Reference

The SC is responsible for the following:

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



- 4.2.2 Receiving recommendations of the TC/ CC and further deliberating on it.
- 4.2.3 Constituting committees as needed.
- 4.2.4 The SC may note approvals of the Chair TC and/ or CC and, if required, give general directions for any course correction.
- 4.2.5 A minimum of one-third members shall constitute the quorum of the committee meeting.
- 4.2.6 Minutes of meetings of the Committees will be issued by the committee's Secretary with consent of the respective Chair of the Committees.

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 stakeholders:

- 5.1.1 Chairperson – a person of eminence, may be in the capacity of an individual.
- 5.1.2 Ministries and regulatory bodies with superintending 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/ Consultancy Organizations working in Cyber security.
- 5.1.7 Chairperson TC may co-opt more members in consultation with Scheme Owner (SO) and Manager. Further representatives of similar organizations 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 (TC) is responsible for the following:

- 5.2.1 Defining the certification/ technical criteria for the Scheme and resolving related issues.
- 5.2.2 Defining the competence profiles for cyber security professionals, viz essential knowledge and skills for different expertise levels in different cyber security domains.
- 5.2.3 Providing an overall direction and guidance based on the knowledge, skills and expertise level required for each of the cyber security domain.



- 5.2.4 Providing appropriate direction and guidance on technical assessment methodologies for cyber security competence profiles.
- 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 content of the examination/ assessment process employed by the Scheme Manager, and any of the accredited PrCBs.
- 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 may be held more frequently until the stabilisation of the Scheme.

6. Certification Committee (CC)

6.1 Membership

- 6.1.1 Chairperson – A person of eminence, may be in the capacity of an individual.
- 6.1.2 Government Organizations.
- 6.1.3 Critical Sector Entities.
- 6.1.4 Industry associations.
- 6.1.5 Academic Institutions/ Training Bodies.
- 6.1.6 Chairperson CC may co-opt more members in consultation with Scheme Owner (SO) and Manager. As per requirement, representatives of similar organizations may be called by rotation and mutual agreement by Chairperson CC, Scheme Owner and Manager.
- 6.1.7 Secretariat – Quality Council of India.

6.2 Terms of Reference

The Certification Committee is responsible for the following:

- 6.2.1 Developing, maintaining and revising the Scheme, as appropriate.
- 6.2.2 Developing, maintaining and revising the documents such as certification process and requirements for PrCBs for PrCBs to apply for accreditation, as appropriate.
- 6.2.3 Developing, maintaining, and revising as appropriate the document i.e. provisional approval system for PrCBs to apply for accreditation.
- 6.2.4 Developing, maintaining and revising the process for permitting approved entities for the use of Certification mark, as appropriate and if any.
- 6.2.5 Deliberations on any other issue relating to Certification of Persons.

6.3 Meetings

The CC shall meet at least once every year. Initially the meetings may be held more frequently until the stabilization of the Scheme.



7. Roles of Organizations

- 7.1 NCIIPC is the Owner of the Scheme and shall maintain superintendence on the overall efficacy of the operationalisation of the Scheme by QCI.
- 7.2 Quality Council of India is the Scheme Manager and will manage and operationalise the Scheme on behalf of NCIIPC. It shall establish the MSC and be responsible for the overall management of the Scheme. QCI shall provide as the Secretariat for the Scheme
- 7.3 National Accreditation Board for Certification Bodies (NABCB), a constituent Board of the QCI, shall be responsible for accrediting PrCBs who are desirous of participation in the Scheme. NABCB shall, through a legally enforceable agreement with the accredited PrCB, ensure that the PrCB shall offer NABCB and its representatives, including assessors, experts, observers, and regulators appointed in the assessment teams, such reasonable access and cooperation, as necessary, to enable NABCB assessment team to monitor conformity with the Agreement and the relevant standard(s). The accredited PrCB shall also provide access to NABCB assessors, experts and observers, to its premises for conducting assessment activities. The access to NCIIPC personnel or any personnel nominated by them will hold similar position to that of NABCB. The Scheme allows accreditation by another Accreditation Board (an IAF member) having the scope for accreditation in the domain of Cyber Security.

8. Complaints

- 8.1 A complaint is an expression of dissatisfaction, other than an appeal, by any person or organization to a PrCB or AB, relating to the activities of that body, where a response is expected.
- 8.2 The system has provisions for accepting complaints from the stakeholders against any component of the Scheme. The PrCBs and ABs are required to have a standardised complaint system in place, as applicable. Stakeholders are encouraged to utilise the available mechanisms for complaint registration.
- 8.3 Complaint(s) received by the NCIIPC shall be directly referred to QCI, which shall further monitor and take appropriate actions against whom the complaint is registered.
- 8.4 Any complaint received by QCI shall be similarly handled.
A statement on complaints (as received) along with their status shall be reported to the MSC in each meeting.

9. Appeals

- 9.1 An appeal is a request by a cyber security professional or PrCB, to the PrCB or AB for reconsideration of a decision made by that body.
- 9.2 Provisions for addressing appeals from the applicant/ certified persons/ accredited PrCBs under the Scheme shall be utilized invariably.



- 9.3 In case anyone is aggrieved by the decisions of TC/CC with regards 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 underlying principle is that the appeal is handled independently, of the personnel involved in the decision, and shall be maintained.
- 9.6 The statement of appeals, received by the NCIIPC shall be forwarded to QCI and shall process the same or may place it before the MSC in the meetings.

10. Review of the Scheme

The scheme shall be reviewed for its relevance to the existing milieu at least once every year lasting for a period of three years from the date of launch, and subsequently once every five years, or earlier if required. Upon reviewing, the consideration shall include past performance(s) data in relation with the approved PrCBs and certified cyber security professionals, the status of complaints/ appeals/ RTIs/ and other relevant information.

SECTION 3

COMPETENCY PROFILES

(Criteria for Certification of IT/ICS Cyber Security Professionals)



1 Background

- 1.1 In the past few years, there has been an exponential growth in the use of IT and ICS for automating businesses and industrial processes, critical functions and operations, governance and electronic service delivery around the world, especially in India. The informational security requirements are very complex and is a constant struggle for organizations to meet their workforce requirements to design, implement, operate, manage, protect and defend the complexity and interconnectivity of information technology, industrial control systems and networks. This has resulted in a huge demand on the human resource supply chain to create and sustain large pools of professionally competent IT and ICS cyber security personnel with certified knowledge, skills, and expertise.
- 1.2 CSEs and other organizations are dependent on cyber security specialists, whether they are own employees or from external parties like System Integrators, OEMs and consultancy providers. These specialists are required to handle threats and risks to their IT and ICS systems and networks, applications and data.
- 1.3 Cyber security professionals working with or providing services to CSEs are increasingly required to handle the convergence and integration of IT and ICS disciplines, each with its own objectives, bodies of knowledge, organizational cultures, and attitudes towards cyber security. Sectors that use ICS have specific processes and operational procedures mandated from health, safety, and environmental perspectives. Therefore, plugging identified gaps in information security quickly and seamlessly into these systems and networks, requires a high degree of expertise in both IT and ICS. The CSEs also operate in an interconnected digital ecosystem that requires an understanding of the interdependencies within and across the sectors.
- 1.4 Cyber security is specialty domain in its own right, even though it is deeply embedded and integrated into the IT and ICS domains of all technology-enabled organizations and entities. However, the mechanisms for identifying and recognizing different competencies and expertise levels related to cyber security are somewhat disjointed and somewhat localised within the organizations themselves. Globally, many countries have addressed the standardization of cyber security competency profiles and associated capabilities.
- 1.5 The Certification Scheme for cyber security professionals is designed and developed to address the cyber security competency requirements of professionals in the Indian environment. Since the work roles and tasks in the Indian context are not yet standardized and remains local to each organization, the approach taken in the certification scheme is to define competency profiles for different cyber security domains that are based on a combination of knowledge, skills and expertise levels in distinct specialisation areas. Cyber security professionals are then certified for the competency profile as per ISO/IEC 17024:2012 framework that engages the certification of Persons.
- 1.6 A cyber security professional certified under the scheme can demonstrate his competency mentioned in the certificate provided by a PrCB after completing the due



process of certifying the knowledge, skills and expertise of the certified personnel in the respective cyber security domain. Guidance to cyber security professionals for certification is described in Annex C of this section.

- 1.7 An organization can classify its information security/ cyber security functions under different cyber security domains defined in the Scheme and use the associated competency profiles to ensure that the competencies of the workforce are aligned to the work roles and responsibilities of the different cyber security domains. This process is described in Annex D of this section.
- 1.8 The Scheme will keep in pace with the latest cyber security knowledge, skills and expertise requirements by issuing updated versions periodically.

2 Purpose

The purpose of this section is to:

- 2.1 Provide information and direction to cyber security professionals to acquire knowledge and develop skills in different specialisation areas, if they want to be assessed, measured, and certified by PrCBs.
- 2.2 Provide a standardised mechanism for PrCBs to assess and certify cyber security professionals for different cyber security competencies of the Scheme.
- 2.3 Provide a framework and guidance to CSEs, consultancy organizations and training bodies to hire, engage and impart training to cyber security professionals for different cyber security domains.

3 Objective

The objective of this section is to:

- 3.1 Define the **levels of expertise** (work capability and responsibility) that organizations require from their workforce in the distinct **cyber security domains** and the **levels of expertise** (knowledge and skills) that cyber security professionals achieve in distinct **specialisation areas**.

Note: A typical statement to describe an organization's workforce requirement – A cyber security professional should have the required knowledge and skills in... specialisation area(s) so as to be capable of / responsible for ... work in a cyber security domain of the organization.

- 3.2 Define the framework for PrCBs to assess and certify the cyber security professionals (Refer to Section 6 of this document).

4 Intended Stakeholders

The following are the intended beneficiaries for this document:

- 4.1 Certification Bodies for persons (PrCBs)
- 4.2 Accreditation Body.



- 4.3 Regulatory and National nodal agencies: NCIIIPC, CERT-In, CEA etc.
- 4.4 Authorised Training bodies and Consulting Organizations, national bodies that are responsible for cybersecurity.
- 4.5 Academic Institutions, Individual Cybersecurity Professionals, and other Interested stakeholders- Personnel and Entities involved in various phases of the life cycle of systems in Critical Sector.

5 Normative references

The reference documents were indispensable for the application of this document. For dated references, only the cited edition are applicable. For undated references, the latest edition of the reference document (including any amendments) are applicable. For the purpose of reference, this Scheme shall refer to Indian Standards (IS) wherever the same has been adopted/published by the Bureau of Indian Standards (BIS).

- 5.1.1 Conformity assessment - General requirements for bodies operating certification of persons, ISO/IEC 17024: 2012.
- 5.1.2 Conformity assessment - Vocabulary related to competence of persons used for certification of persons, ISO/IEC TS 17027: 2014.

6 Design and Development of the Scheme

- 6.1 The certification scheme is developed through the following steps:

- 6.1.1 Define the knowledge and skills that cyber security professionals have to acquire in the distinct specialisation areas (Refer to Table 3.1 and Annex 1A in Section 3 of this document).
- 6.1.2 Define the cyber security domains of CSEs and the associated cyber security functions (Refer to Table 3.2 of this section).
- 6.1.3 Define the levels of expertise that organizations require from their workforce and the levels of expertise that cyber security professionals achieve in specialisation areas (Refer to Annex E of this section).
- 6.1.4 Define the competency profiles for certification defined under the Scheme and associate them with an organization's cyber security domains and functions and specialisation areas (Refer to Tables 3.3 and 3.4 and Annex 1B of this section).
- 6.1.5 Define the curriculum for knowledge and skill modules for different expertise levels (mentioned in Annex 1A of this section) to enable the PrCBs to develop procedures (mentioned in Section 6) to test the cyber security professionals in different specialisation areas for issue of competency profile certificate.
- 6.1.6 Standardise the assessment and measurement requirements to be followed by the PrCBs (refer to Annex B of this section), while using the developed procedures to assess and measure the knowledge, skills and expertise levels of cyber security professionals (mentioned in Section 6 of this document).

6.2 Knowledge and Skills

- 6.2.1 A **specialisation area** (listed in Table 3.1) is a distinct specialisation in knowledge areas or skillsets specialisation that can be attained through learning, academic and professional training and work experience.

Table 3.1: Knowledge and Skill Specialisation Areas

S. No	KM/ SM Id	Knowledge and Skills Specialisation Areas
		Knowledge Area
1	KA01	Network Infrastructure & Network Security (Technical)
2	KA02	Systems (HW, VM, Firmware, OS) Security (Technical)
3	KA03	Software and Platform Operations Security (Technical)
4	KA04	Secure Systems Engineering (Technical)
5	KA05	Secure Software Design & Development (Technical)
6	KA06	Enterprise Governance, Risk and Compliance (Organizational)
7	KA07	Enterprise Supply Chain (Organizational)
8	KA08	Enterprise IT and Information Security (Technical)
9	KA09	Enterprise Cyber Defence (Technical)
10	KA10	Data Science, Data Analytics, Machine Learning (Technical)
11	KA11	Cyber Forensics (Technical)
12	KA12	Cyber Security Training & Awareness (Organizational)
13	KA13	ICS Cyber Security (Technical)
		Skillsets
1	SA01	Programming & Scripting (Technical)
2	SA02	Managing and securing systems, networks, applications (Technical)
3	SA03	Managing and securing information and data (Technical/ Analytical)
4	SA04	Software development lifecycle (Technical)
5	SA05	Cyber Defence (Technical)
6	SA06	Others (Technical)

- 6.2.2 Every Specialisation Area, whether Knowledge Area (KA) or Skillset (SA), has a set of Knowledge Modules (KM) or Skill Modules (SM) grouped under it, with one or more expertise levels. The characteristics of modules are described in 6.2.3 and 6.2.4.
- 6.2.3 Knowledge Modules (KM) describe what a cyber security professional should know and attain at a particular expertise level. The required depth of knowledge within a KM is defined by the expertise level tag (F/A/M) assigned to it.
- 6.2.4 Skill Modules (SM) describe what a cyber security professional of particular expertise level should be able to do (observable actions) under particular circumstances. The skills described in skill modules can range from simple (one or few steps) to complex (multiple steps) skills. The required grade of skills within a SM is defined by the expertise level tag (F/A/M) assigned to it.

6.3 Cyber Security Domains and Functions

- 6.3.1 A cyber security domain is a distinct technical/ organizational capability of processes, people and technology that a CSE must have to meet its cyber security objectives successfully.



- 6.3.2 Each cyber security domain typically has a job hierarchy associated with it that is designed to handle different levels of work and responsibilities. The Scheme categorises the work and responsibilities of each cyber security domain into three levels, namely, Foundation (F), Advanced (A) and Master (M).
- 6.3.3 Each cyber security domain is associated with one or more cyber security functions of the CSE (described in Annex D of this section).
- 6.3.4 The Scheme lists 19 cyber security domains that cover all the major capability requirements of a CSE, with one domain also relevant for Training Bodies. These are listed in Table 3.2 below.

Table 3.2: Cyber Security Domains and associated Cyber Security Functions

S. No.	Cyber security Domain Type	Cyber security domain	Associated Cyber security Function
1	Organizational	Governance, Risk and Compliance	Govern & Administer (GA)
2	Technical	Technology & System Security Architecture	Acquire & Provision (AP)
3	Technical	Secure Software Development	Acquire & Provision (AP)
4	Technical	Application Security Testing	Acquire & Provision (AP)
5	Technical	Security Product Testing	Acquire & Provision (AP)
6	Technical	Network Security Administration	Operate & Maintain (OM)
7	Technical	System Security Administration	Operate & Maintain (OM)
8	Technical	Applications & Data Security Administration	Operate & Maintain (OM)
9	Technical	Security Support Services	Operate & Maintain (OM)
10	Technical	Security Performance Management	Operate & Maintain (OM)
11	Technical	ICS Cyber Security	Operate & Maintain (OM)
12	Technical	ICS Cyber Risk Assessor	Analyse & Investigate (AI)
13	Technical	ICS Cybersecurity design, & Implementation	Acquire & Provision (AP)
14	Technical	ICS Cybersecurity Operations & Maintenance	Operate & Maintain (OM)
15	Technical	Cyber Defence	Analyse & Investigate (AI) [Identify (ID), Protect (PR)]
16	Technical	Cyber Vulnerability, Threat & Risk Management	Analyse & Investigate (AI) [Identify (ID), Protect (PR)]
17	Technical	Security Operations	Analyse & Investigate (AI) [Detect (DE), Respond (RP)]
18	Technical	Cyber Forensics & Investigation	Analyse & Investigate (AI) [Identify (ID), Protect (PR), Recover (RC)]
19	Organizational	Cyber Training & Awareness	Train & Enable (TE)



6.4 Expertise Levels

The levels of **work expertise** that organizations require from their workforce in distinct cyber security domains and the levels of **knowledge and skill expertise** that cyber security professionals can achieve in distinct specialisation areas are defined below.

6.4.1 Foundation Level (F)

This level is for all cyber security professionals interested in obtaining Foundation level competency certification in a cyber security domain (listed in Para 6.3.4) or specialisation area (listed in Para 6.2.1).

Cyber security professionals certified for this level have the required competence to be capable of / responsible for carrying out Foundation level work, activities and tasks in the associated cyber security domain or specialisation area of an organization.

6.4.2 Advanced Level (A)

This level is for experienced cyber security professionals who hold a Foundation level competency certification and have the requisite industry experience in a cyber security domain listed in Para 6.3.4.

Cyber security professionals certified for this level have the required competence to be capable of / responsible for carrying out Advanced level work, activities and tasks in the associated cyber security domain of an organization.

6.4.3 Master Level (M)

This level is expert cyber security professionals who hold an Advanced level competency certification and have the requisite industry experience in a cyber security domain listed in Para 6.3.4.

Cyber security professionals certified for this level have the required competence to be capable of / responsible for carrying out Master level work, activities and tasks in the associated cyber security domain of an organization. Annex C, Table 3A of this section gives sample mapping between cyber security domain certifications and the associated work expertise of cyber security professionals to carry out tasks within an organization. Annex D, Figures A4.2 and A4.3 give sample mapping of organization job roles to cyber security domains, functions and expertise levels.

6.5 Competency Profiles

6.5.1 A competency profile for certification of cyber security Professional is defined as a set of knowledge and skill modules that are relevant to a cyber security domain or a specialisation area, combined with a measurable level of expertise attained for that knowledge and skills.

6.5.2 A single Knowledge or Skill module may be applied to one or more competency profiles.



6.5.3 Cyber Security Domain Competency Certification: Each cyber security domain has one or more competency profiles associated with it that address the requirement of different levels of expertise for that domain. The competency profile certification codes allocated under the Scheme for different levels of expertise in relevant cyber security domains are listed in Table 3.3 below.

Table 3.3: Cyber Security Domain Certification Codes and Titles under the Scheme

S. No.	Certification Code / Id	Certification Title (Cyber Security Domain & Expertise Level)
1	GRC-F	Governance, Risk and Compliance (Foundation)
2	GRC-A	Governance, Risk and Compliance (Advanced)
3	GRC-M	Governance, Risk and Compliance (Master)
4	TSA-F	Technology & System Security Architecture (Foundation)
5	TSA-A	Technology & System Security Architecture (Advanced)
6	TSA-M	Technology & System Security Architecture (Master)
7	SSD-F	Secure Software Development (Foundation)
8	SSD-A	Secure Software Development (Advanced)
9	AST-F	Application Security Testing (Foundation)
10	AST-A	Application Security Testing (Advanced)
11	PST-F	Product Security Testing (Foundation)
12	PST-A	Product Security Testing (Advanced)
13	NSA-F	Network Security Administration (Foundation)
14	NSA-A	Network Security Administration (Advanced)
15	SSA-F	System Security Administration (Foundation)
16	SSA-A	System Security Administration (Advanced)
17	ADS-F	Applications & Data Security Administration (Foundation)
18	ADS-A	Applications & Data Security Administration (Advanced)
19	SSS-F	Security Support Services (Foundation)
20	SSS-A	Security Support Services (Advanced)
21	SPM-F	Security Performance Management (Foundation)
22	SPM-A	Security Performance Management (Advanced)
23	ICS-F	ICS Cyber Security (Foundation)
24	ICR-F	ICS Cyber Risk Assessment (Foundation)
25	ICR-A	ICS Cyber Risk Assessment (Advanced)
26	ICD-A	ICS Cyber Security Design & Implementation (Advanced)
27	ICD-M	ICS Cyber Security Design & Implementation (Master)
28	ICM-A	ICS Cyber Security Operations & Maintenance (Advanced)
29	ICM-M	ICS Cyber Security Operations & Maintenance (Master)
30	CYD-F	Cyber Defence (Foundation)
31	CYD-A	Cyber Defence (Advanced)
32	CYD-M	Cyber Defence (Master)
33	CRM-F	Cyber Vulnerability, Threat & Risk Management (Foundation)
34	CRM-A	Cyber Vulnerability, Threat & Risk Management (Advanced)

S. No.	Certification Code / Id	Certification Title (Cyber Security Domain & Expertise Level)
35	SCO-F	Security Operations (Foundation)
36	SCO-A	Security Operations (Advanced)
37	CYF-F	Cyber Forensics & Investigation (Foundation)
38	CYF-A	Cyber Forensics & Investigation (Advanced)
39	CYF-M	Cyber Forensics & Investigation (Master)
40	CTA-F	Cyber Training & Awareness (Foundation)
41	CTA-A	Cyber Training & Awareness (Advanced)

6.5.4 The cyber security domain competency certificates will have the following structure:

- Certification Code/ Id:** Unique Competency Profile Id in the format 3-letter cyber security domain code followed by 1-letter expertise level code.
- Certification Title:** Competency Profile Title, that describes the cyber security domain in which competency has been demonstrated.

6.5.5 Cyber security domain competency certifications for Foundation and Advanced levels are defined for all the cyber security domains listed in Table 3.2. Following cyber security domain competency certifications are defined for Master level:

- Governance, Risk and Compliance
- Technology & System Security Architecture
- ICS Cyber Security Design & Implementation
- ICS Cyber Security Operations & Maintenance
- Cyber Defence
- Cyber Forensics and Investigation

6.5.6 **Specialisation Area Competency Certification:** PrCBs are permitted to offer Foundation Level Specialisation Area Competency certification in one or more of the specialisation areas listed in Table 3.1 of this section. The competency profile certification codes allocated under the Scheme for the same are listed in Table 3.4 below.

Table 3.4: Specialisation Area Certification Codes and Titles under the Scheme

S. No	Certification Code / Id	Certification Title (Specialisation Area & Expertise Level)
1	KA01-F	Network Infrastructure & Network Security (Foundation)
2	KA02-F	Systems Security (Foundation)
3	KA03-F	Software and Platform Operations Security (Foundation)
4	KA04-F	Secure Systems Engineering (Foundation)
5	KA05-F	Secure Software Design & Development (Foundation)
6	KA06-F	Enterprise Governance, Risk and Compliance (Foundation)



S. No	Certification Code / Id	Certification Title (Specialisation Area & Expertise Level)
7	KA07-F	Enterprise Supply Chain (Foundation)
8	KA08-F	Enterprise IT and Information Security (Foundation)
9	KA09-F	Enterprise Cyber Defence (Foundation)
10	KA10-F	Data Science, Data Analytics, Machine Learning (Foundation)
11	KA11-F	Cyber Forensics (Foundation)
12	KA12-F	Cyber Security Training & Awareness (Foundation)
13	KA13-F	ICS Cyber Security (Foundation)
14	SA01-F	Programming & Scripting (Foundation)
15	SA02-F	Managing and securing systems, networks, applications (Foundation)
16	SA03-F	Managing and securing information and data (Foundation)
17	SA04-F	Software development lifecycle (Foundation)
18	SA05-F	Cyber Defence (Foundation)
19	SA06-F	Others (Foundation)

6.5.7 The specialisation area competency certificates will have the following structure:

- a. **Certification Code/ Id:** Unique Specialisation Area Id in the format KAx or SAx followed by 1-letter expertise level code (F only).
- b. **Certification Title:** Specialisation Area Title, that describes the specialisation area in which competency has been demonstrated.

6.5.8 The specialisation area competency certifications are designed to achieve the following objectives:

- a. For general use by students, professionals and employees to establish their own competence in different specialisation areas, through certification by accredited, independent, third-party certification bodies.
- b. For general use by CSEs, COs and TBs to establish the competence of their workforce in different specialisation areas, through certification by accredited, independent, third-party certification bodies.
- c. For specific use by cyber security professionals to obtain foundation level competency certification in specialisation areas, so that they are further eligible to receive advanced and master level competency certifications, as described in Annex 1B of this section. The PrCBs can verify that the cyber security professionals have the required certification for the Required (R) modules, prior to giving them the advanced and master level certifications.

6.5.9 The competency testing of foundation level specialisation area competency will be done using the Foundation level curriculum defined for the specialisation area. While carrying out the specialisation area competency certifications, PrCBs will follow all the governance and processes defined under this Scheme.



- 6.5.10 The curriculum for assessing the cyber security professionals for their knowledge, skills and expertise level in distinct specialisation areas is given in Annex 1A, Table 1A of this section. The mapping of knowledge and skills to competency profiles for certification is given in Annex 1B, Tables 1B and 1C of this section.
- 6.5.11 Attestation/ certification for the competency profiles is based solely on the assessment of knowledge and skills by the PrCBs. However, to enable the stakeholders to use the scheme effectively, separate supplementary guidance is provided in Annexures C, D and E of this section on using the competency profiles for hiring, career progression and training.
- 6.5.12 Employers may use the Annexures to design and issue organization-defined certificates to their employees with regard to their having the knowledge and skill sets in different knowledge and skill areas defined in this Scheme.

7 PrCB's Actions

- 7.1 The assessment process requires that cyber security professionals demonstrate their knowledge and skill at the requisite expertise level, to be eligible for certification for that competency profile code.
- 7.2 The knowledge and skill modules defined in Annex 1A in this section are not mutually exclusive. On the contrary, their association is flexible for achieving a specific objective of assessing the applicant's competence. The matrix design is done in a manner that it includes a comprehensive range of knowledge areas. The skill areas are kept minimal by leveraging the principle of commonality to minimise the complexity of the certification process.
- 7.3 The matrix design is modular that can be configured by selecting appropriate modules to cater to the requirement of any new levels/ scope arising for personnel certification.
- 7.4 In certain modules of Annex 1A of this section, the topics in the defined curriculum are kept common by design. The rationale is to allow the certification bodies to prepare the testing procedure by applying their professional experience for the common topics by calibrating a mix of easy (low intensity) medium (moderate intensity) and hard (high intensity). The depth of the tests shall be commensurate with the level of certification (foundation, advanced, master). The same is detailed in the certification process of the professional.
- 7.5 Some of the Knowledge Modules (KM) may be common (repetitive) across different expertise levels (F/A/M). However, the certification process will be based on different dimensions such as knowledge level/ application/ skill relevant for the level (F/A/M).
- 7.6 The prerequisites and methodology for the certification of cyber security professionals are given in Annex B of this section. The differentiating factors for different levels are documented in the column 'Methodology of Initial Assessment' in this Annexure.
- 7.7 Format for issuance of competency certification:



“Certified <Certification Title> Professional” - ‘<Expertise Level> Level’ under the certification scheme for IT and ICS cyber Security Professionals”.

The Certification Code/Id will be displayed on the certificate.

8 Relationship with other frameworks

- 8.1 The following frameworks are in place to accomplish cyber security best practices and conformity assessments.
 - 8.1.1 ISO/IEC 17024:2012 - Conformity assessment — General requirements for bodies operating certification of persons.
 - 8.1.2 Workforce framework for Cyber security (NIST: NICE framework).
 - 8.1.3 Operational Technology Cyber security Competency Framework, Singapore.

The exercise of comparison and mapping in the conformity assessments are termed as reciprocity or benchmarking. This involves understanding not only the content but also conformity assessment procedure to map various initiatives and evolves in the operation phase so that comparison in intent and content levels can be done when sufficient data is collected. The coverage and comparison of competencies has been made on a preliminary basis as part of this document in Annex C of this section.

9 Way Forward

- 9.1 Criteria for certifications is a living document and will continue to be updated and improved as and when stakeholders provide feedback on implementation. In addition, QCI will continue coordinating with the private sector and government agencies at all levels for suggestion to improve the same. As the framework is put into more excellent practice, additional lessons learned will be integrated into future versions. This will ensure the criteria meet the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats, risks, and associated emerging solutions.
- 9.2 QCI will keep a watch for development/up-gradation of equivalent international frameworks and map various cyber security programs offered by various organizations. QCI will work with NCIIPC, CSIRT-Power and respective allied ministries, to develop a mechanism to ensure that these developments are being taken care of and currency of this document is maintained.



Annexure 1A

Knowledge and Skill Modules (grouped by Specialisation Areas) and the Curriculum Scope for each Expertise Level

Knowledge Modules (KM) and Skill Modules (SM) listed below have unique ids, the first two numerals representing the Knowledge/ Skill Area (01 to 13), the next two numerals representing the Knowledge/ Skill module within the Area (01 to 99) and F/A/M tag representing the Expertise level.

Table 1A: Knowledge and Skill Modules Master List - grouped by Specialisation Areas

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	<ul style="list-style-type: none"> ▪ Knowledge of concepts, terminology, and operations of a wide range of communications media (computer and telephone networks, satellite, fibre, 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 administratio



KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ Knowledge of network architecture concepts and its application including topology, protocols, and components. ▪ 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	<ul style="list-style-type: none"> ▪ 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/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
KM-0102A	Advanced Module: Network Security	<ul style="list-style-type: none"> 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.
KA-02	Knowledge Area: Systems (HW, VM, OS) Security (Technical)	
KM-0201F	Foundation Module: System Infrastructure and Administration	<ul style="list-style-type: none"> 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.



KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ 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-0202A	Advanced Module: System Security and Security Administration	<ul style="list-style-type: none"> ▪ 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/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
KM-0301F	Foundation Module: Software and Platform Operations	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ Knowledge of controlling costs and budgets regarding IT systems. ▪ 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	<ul style="list-style-type: none"> ▪ 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



KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		<p>PII compliance, data loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing).</p> <ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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-0401A	Advanced Module: Secure Systems Engineering	<ul style="list-style-type: none"> 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.



KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
KA-05	Knowledge Area: Secure Software Design & Development (Technical)	
KM-0501F	Foundation Module: Secure Software Design & Development	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ Knowledge of cyber security and privacy principles and methods that apply to software development. ▪ Knowledge of encryption algorithms. ▪ Knowledge of cryptography and cryptographic key management concepts.



KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 (Organizational)	
KM-0601F	Foundation Module: Enterprise IT Governance, Risk and Compliance	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Knowledge of strategies, standards, organization's needs, intent, principles, approaches and legislation to establish the cybersecurity policies to ensure effective management of cybersecurity risks in pursuit of its defined objectives. Knowledge of NIST CSF, CIS v8, IEC 62443-2-1 and other organizational frameworks and standards.



KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		<ul style="list-style-type: none"> ▪ 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). ▪ 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	<ul style="list-style-type: none"> ▪ 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 (Organizational)	
KM-0701F	Foundation Module: Enterprise Supply Chain	<ul style="list-style-type: none"> ▪ 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.



KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161) Knowledge of supply chain risk management standards, processes, and practices. 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, organization 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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-



KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		<p>GRC), sources, characteristics, and uses of the organization's data assets, reporting structures and processes.</p> <ul style="list-style-type: none"> ▪ Knowledge of the organization'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-0802F	Foundation Module: Enterprise Info Security Strategy & Design	<ul style="list-style-type: none"> ▪ 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 organizations to respond to those incidents. ▪ Knowledge of Cyber Threat landscape in the organization 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	<ul style="list-style-type: none"> ▪ 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



KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		<p>management processes, capabilities and limitations, front-end collection systems including traffic collection, filtering and selection.</p> <ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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). 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Knowledge of critical information infrastructure technologies, industry-standard security models like NIST CSF, procurement requirements, functionality, quality and security requirements, and how



KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		<p>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.</p> <ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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. 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.



KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		<ul style="list-style-type: none"> ▪ 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, TCPdump).
KM-0901A	Advanced Module: Enterprise Cyber Defence	<ul style="list-style-type: none"> ▪ 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. ▪ 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



KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		<p>techniques (e.g., gaining backdoor access, collecting/exfiltrating data, conducting vulnerability analysis of other systems in the network).</p> <ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ 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 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	<ul style="list-style-type: none"> ▪ 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/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
KM-1001A	Advanced Module: Data Science, Data Analytics, AI/ML	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ 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.). ▪ 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/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
KM-1101A	Advanced Module: Cyber Forensics & Investigation	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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.
KA-12	Knowledge Area: Cyber Security Training & Awareness (Organizational)	
KM-1201F	Foundation Module: Cyber security Training & Awareness	<ul style="list-style-type: none"> Knowledge of the organization'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.



KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		<ul style="list-style-type: none"> ▪ 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, kinaesthetic). ▪ 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 behaviours 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	<ul style="list-style-type: none"> ▪ 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 organization'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	<ul style="list-style-type: none"> ▪ Knowledge of ICS cybersecurity 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 ▪ Knowledge of ICS cybersecurity architecture to validate or verify the ICS cybersecurity ▪ 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.



KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		<ul style="list-style-type: none"> ▪ 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 organization, 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 organization 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 ▪ 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



KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		<ul style="list-style-type: none"> ▪ 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 organization 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	<ul style="list-style-type: none"> ▪ 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 organization ▪ 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	<ul style="list-style-type: none"> ▪ Knowledge of cyber risk assessment techniques for the ICS environment ▪ Knowledge of security risks, threats and vulnerabilities in the organization'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 Cybersecurity Design & Implementation	<ul style="list-style-type: none"> ▪ Knowledge of monitoring, reviewing and executing operational requirements to ensure the integrity of ICS network infrastructure ▪ Knowledge of security requirements of the organization ▪ 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 Cybersecurity Design & Implementation	<ul style="list-style-type: none"> ▪ 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 Cybersecurity Operations & Maintenance	<ul style="list-style-type: none"> ▪ Knowledge of vulnerability and patch management configuration tools and techniques ▪ Knowledge of analysis and verification process, tools and techniques for testing effectiveness of patch



KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		<ul style="list-style-type: none"> ▪ 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 ▪ 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 organization 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 Cybersecurity Operations & Maintenance	<ul style="list-style-type: none"> ▪ Knowledge of range of patch management configuration techniques ▪ Knowledge of internal stakeholders 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, firmwares) and interdependencies with ICS systems for patch updates



KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		<ul style="list-style-type: none"> ▪ 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 ▪ 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	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ 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.



KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		<ul style="list-style-type: none"> ▪ Skill in analysing 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.). ▪ 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	<ul style="list-style-type: none"> ▪ 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.



KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		<ul style="list-style-type: none"> Skill in system, network and OS hardening techniques. (e.g., remove unnecessary services, password policies, network segmentation, enable logging, least privilege, etc.).
SA-03	<i>Skill Area: Managing and securing information and data (Technical/ Analytical)</i>	
SM-0301F	Foundation Module: Managing & Securing Skills	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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. 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 analyse 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	<i>Skill Area: Software development lifecycle (Technical)</i>	
SM-0401F	Foundation Module: Software Development & Testing Skills	<ul style="list-style-type: none"> Skill in writing test plans. Skill in conducting test events.
SM-0401A	Advanced Module: Software Development & Testing Skills	<ul style="list-style-type: none"> Skill in configuring and optimizing software. Skill in conducting software debugging. Skill in developing operations-based testing scenarios.



KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
SA-05	Skill Area: Cyber Defence (Technical)	
SM-0501F	Foundation Module: Cyber Defence Skills	<ul style="list-style-type: none"> ▪ 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). ▪ 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	<ul style="list-style-type: none"> ▪ 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.



KM/ SM ID	Knowledge / Skill Module Title	Curriculum (for use in assessment procedures for the expertise level)
		<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ Skill in technical writing. ▪ 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	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ 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.



The document is focused on development of competency profile for IT/ICS cyber security professional. Therefore, basic knowledge of cyber security principles is applicable to all domains including the following:

- a. Knowledge of cyber security and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation)
- b. Knowledge of cyber threats and vulnerabilities
- c. Knowledge of network security architecture concepts including topology, protocols, components and principles (e.g., application of defence-in-depth)
- d. Knowledge of risk management processes (e.g., methods for assessing and mitigating risk)
- e. Knowledge of laws, regulations, policies and ethics as they relate to cyber security and privacy



Annexure 1B

Certification of Competency Profiles - Mapping Knowledge and Skill Modules

1. **The mapping of KM and SM to competency profiles for certification is described below:**
 - 1.1 The mapping of KM and SM required for different cyber security domains (Table 1B) and specialisation areas (Table 1C) below has been done by domain, industry and organization experts. It is derived from the understanding of what competence (knowledge, skills, expertise) the cyber security professionals are required to have, to be capable of / responsible for carrying out Foundation/ Advanced/ Master level work and tasks in the associated cyber security domains and specialisation areas of an organization.
 - 1.2 PrCBs will regularly conduct assessment procedures (written and practical examinations, etc.) to enable the applicant cyber security professionals to obtain various Foundation/ Advanced/ Master level Cyber Security Domain / Specialisation Area competency certifications, covering the corresponding KMs and SMs.
 - 1.3 In Table 1B below, each Certification Code/ Id has a set of KM and SM modules, marked as 'R' (Required).
 - 1.4 Typically, an applicant cyber security professional seeking Advanced or Master certification in a cyber security domain would have already been assessed earlier for some of the 'R' modules, when he/ she obtained Foundation or Advanced certification in either the same or another cyber security domain (Table 1B) or in a specialisation area (Table 1C). In such cases, re-assessment of competence in the already certified "R" modules is unnecessary and duplication of assessment.
 - 1.5 It is also necessary that the competence assessment of applicant cyber security professionals is comprehensive at each level and there is no possibility of any bypass in the assessment process. Hence, while applying for advanced and master level certification, the applicant cyber security professional must demonstrate that he/ she has been assessed for competency in all the 'R' modules required for the certification. The applicant cyber security professional is required to submit any/ all of the following documents to the PrCB for validation:
 - a) Valid Cyber Security Domain Competency certifications (listed in Table 1B) acquired and held by the cyber security professional.
 - b) Valid Specialisation Area Competency certifications (listed in Table 1C) acquired and held by the cyber security professional.
 - 1.6 The PrCBs will validate that all the 'R' KM and SM modules for a cyber security domain competency certification are attested/ assessed:
 - a) In case an applicant cyber security professional's certifications do not cover any 'R' KM and SM modules, inform him/ her to obtain certifications for the same.



- b) If the applicant cyber security professional's certifications together cover all the required 'R' KM and SM modules, process the case further for award of Cyber Security Domain competency certification to the applicant cyber security professional.

2. Guidance Notes

2.1 The procedure described above is further explained through an example using Tables 1B and 1C.

2.2 The NSA-A competency profile (S No. 14) requires a cyber security professional to have attested competency in the required ('R') modules KM-0101F, KM-0102F, SM-0201F, KM-0201F, KM-0202F, KM-0101A, KM-0102A, SM-0201A.

2.3 An applicant cyber security professional seeking NSA-A competency profile certificate uses a combination of the following methods to demonstrate competence in all the 'R' KM and SM modules of NSA-A competency profile, using certificates acquired and held by him/ her from any PrCB:

- 2.3.1 Submit valid NSA-F certification to demonstrate successful competency assessment in KM-0101F, KM-0102F, SM-0201F modules.
- 2.3.2 Submit valid SSA-F certification to demonstrate successful competency assessment in KM-0201F, KM-0202F, SM-0201F modules.
- 2.3.3 Submit valid KA01-F, KA02-F and SA02-F certifications to demonstrate successful competency assessment in (KM-0101F+KM-0102F), (KM-0201F+KM-0202F) and SM-0201F modules respectively.
- 2.3.4 Acquire and submit valid certification from any PrCB that demonstrates successful competency assessment for KM-0101A, KM-0102A, SM-0201A modules.

Note: PrCBs are required to regularly offer assessment procedures (written/ practical examinations) to cover the certification requirements of different KM and SM modules.



Table 1B: Mapping Knowledge and Skill modules to Cyber Security Domain Competency Certification

KM/ SM ID	GRC-F	GRC-A	GRC-M	TSA-F	TSA-A	TSA-M	SSD-F	SSD-A	AST-F	AST-A	PST-F	PST-A	NSA-F	NSA-A	SSA-F	SSA-A	ADS-F	ADS-A	SSS-F	SSS-A	SPM-F	SPM-A	ICS-F	ICR-F	ICR-A	ICD-A	ICD-M	ICM-A	ICM-M	CYD-F	CYD-A	CYD-M	CRM-F	CRM-A	SCO-F	SCO-A	CYF-F	CYF-A	CYF-M	CTA-F	CTA-A			
Table 3-2 Serial No	1	1	1	2	2	2	3	3	4	4	5	5	6	6	7	7	8	8	9	9	10	10	11	11	11	11	11	11	11	12	12	12	13	13	14	14	15	15	15	16	16			
Table 3-3 Serial No	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41			
KA-01																																												
KM-0101F													R	R		R				R		R																						
KM-0101A														R																														
KM-0102F													R	R		R				R		R																						
KM-0102A														R																														
KA-02																																												
KM-0201F											R	R		R	R	R			R	R		R															R	R						
KM-0201A												R				R				R																			R					
KM-0202F											R	R		R	R	R			R	R		R																						
KM-0202A												R				R				R																								
KA-03																																												
KM-0301F																	R	R																										
KM-0301A																		R																										
KM-0302F																	R	R																										
KM-0302A																		R																										
KA-04																																												
KM-0401F				R	R	R																																						
KM-0401A					R	R																																						
KA-05																																												

KM/ SM ID	GRC-F	GRC-A	GRC-M	TSA-F	TSA-A	TSA-M	SSD-F	SSD-A	AST-F	AST-A	PST-F	PST-A	NSA-F	NSA-A	SSA-F	SSA-A	ADS-F	ADS-A	SSS-F	SSS-A	SPM-F	SPM-A	ICS-F	ICR-F	ICR-A	ICD-A	ICD-M	ICM-A	ICM-M	CYD-F	CYD-A	CYD-M	CRM-F	CRM-A	SCO-F	SCO-A	CYF-F	CYF-A	CYF-M	CTA-F	CTA-A	
Table 3-2 Serial No	1	1	1	2	2	2	3	3	4	4	5	5	6	6	7	7	8	8	9	9	10	10	11	11	11	11	11	11	11	11	12	12	12	13	13	14	14	15	15	15	16	16
Table 3-3 Serial No	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	
KM-0501F							R	R																																		
KM-0501A								R																																		
KM-0502F									R	R																																
KM-0502A										R																																
KA-06																																										
KM-0601F	R	R	R																																							
KM-0601A		R	R																																							
KM-0601M			R																																							
KA-07																																										
KM-0701F		R	R																																							
KM-0701A			R																																							
KA-08																																										
KM-0801F				R	R	R																																				
KM-0801A					R	R																																				
KM-0802F				R	R	R																																				
KM-0802A					R	R																																				
KM-0803F				R	R	R													R	R																R	R					
KM-0803A					R	R														R																R						
KM-0804F																															R	R	R	R	R							
KM-0804A																																R	R		R							
KA-09																																										
KM-0901F																															R	R	R									
KM-0901A																																R	R									



KM/ SM ID	GRC-F	GRC-A	GRC-M	TSA-F	TSA-A	TSA-M	SSD-F	SSD-A	AST-F	AST-A	PST-F	PST-A	NSA-F	NSA-A	SSA-F	SSA-A	ADS-F	ADS-A	SSS-F	SSS-A	SPM-F	SPM-A	ICS-F	ICR-F	ICR-A	ICD-A	ICD-M	ICM-A	ICM-M	CYD-F	CYD-A	CYD-M	CRM-F	CRM-A	SCO-F	SCO-A	CYF-F	CYF-A	CYF-M	CTA-F	CTA-A		
Table 3-2 Serial No	1	1	1	2	2	2	3	3	4	4	5	5	6	6	7	7	8	8	9	9	10	10	11	11	11	11	11	11	11	11	12	12	12	13	13	14	14	15	15	15	16	16	
Table 3-3 Serial No	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41		
KM-0901M																																R											
KA-10																																											
KM-1001F																					R	R																					
KM-1001A																						R																					
KA-11																																											
KM-1101F																																							R	R	R		
KM-1101A																																							R	R	R		
KM-1101M																																								R			
KA-12																																											
KM-1201F																																										R	R
KM-1201A																																										R	R
KA-13																																											
KM-1301F																							R																				
KM-1302F																								R	R																		
KM-1302A																									R																		
KM-1303A																										R	R																
KM-1303M																											R																
KM-1304A																												R	R														
KM-1304M																													R														
SA-01																																											
SM-0101F				R	R	R							R	R	R	R	R	R	R	R	R	R								R	R	R			R	R	R	R	R				



KM/ SM ID	GRC-F	GRC-A	GRC-M	TSA-F	TSA-A	TSA-M	SSD-F	SSD-A	AST-F	AST-A	PST-F	PST-A	NSA-F	NSA-A	SSA-F	SSA-A	ADS-F	ADS-A	SSS-F	SSS-A	SPM-F	SPM-A	ICS-F	ICR-F	ICR-A	ICD-A	ICD-M	ICM-A	ICM-M	CYD-F	CYD-A	CYD-M	CRM-F	CRM-A	SCO-F	SCO-A	CYF-F	CYF-A	CYF-M	CTA-F	CTA-A			
Table 3-2 Serial No	1	1	1	2	2	2	3	3	4	4	5	5	6	6	7	7	8	8	9	9	10	10	11	11	11	11	11	11	11	12	12	12	13	13	14	14	15	15	15	16	16			
Table 3-3 Serial No	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41			
SA-02																																												
SM-0201F													R	R	R	R																												
SM-0201A														R		R																												
SA-03																																												
SM-0301F				R	R	R											R	R																										
SM-0301A					R	R												R																										
SA-04																																												
SM-0401F							R	R	R	R	R	R																																R
SM-0401A								R		R		R																																
SA-05																																												
SM-0501F																															R	R	R						R	R	R			
SM-0501A																																R	R							R	R			
SA-06																																												
SM-0601F														R	R	R	R																											
SM-0602F	R	R	R	R	R	R																										R	R	R	R							R	R	
SM-0602A		R	R		R	R																											R		R								R	
SM-0603A		R	R			R																											R		R									

Organizations may however want their workforce to have certification in additional KM and SM modules that they think are relevant for the work and responsibilities assigned to the cyber security professional.



Table 1C: Mapping Knowledge and Skill modules to Foundation Level Specialisation Area Competency Certification

S. No	Certification Code / Id	Certification Title (Specialisation Area & Expertise Level)	Knowledge and Skill Modules covered by the certification
1	KA01-F	Network Infrastructure & Network Security (Foundation)	KM0101F, KM0102F
2	KA02-F	Systems Security (Foundation)	KM0201F, KM0202F
3	KA03-F	Software and Platform Operations Security (Foundation)	KM0301F, KM0302F
4	KA04-F	Secure Systems Engineering (Foundation)	KM0401F
5	KA05-F	Secure Software Design & Development (Foundation)	KM0501F, KM0502F
6	KA06-F	Enterprise Governance, Risk and Compliance (Foundation)	KM0601F
7	KA07-F	Enterprise Supply Chain (Foundation)	KM0701F
8	KA08-F	Enterprise IT and Information Security (Foundation)	KM0801F, KM0802F, KM0803F, KM0804F
9	KA09-F	Enterprise Cyber Defence (Foundation)	KM0901F
10	KA10-F	Data Science, Data Analytics, Machine Learning (Foundation)	KM1001F
11	KA11-F	Cyber Forensics (Foundation)	KM1101F
12	KA12-F	Cyber security Training & Awareness (Foundation)	KM1201F
13	KA13-F	ICS Cyber Security (Foundation)	KM1301F
14	SA01-F	Programming & Scripting (Foundation)	SM0101F
15	SA02-F	Managing and securing systems, networks, applications (Foundation)	SM0201F
16	SA03-F	Managing and securing information and data (Foundation)	SM0301F
17	SA04-F	Software development lifecycle (Foundation)	SM0401F
18	SA05-F	Cyber Defence (Foundation)	SM0501F
19	SA06-F	Others (Foundation)	SM0601F, SM0602F

Table 1C covers the certification only for Foundation Level specialisation areas, to ensure that the certification process is not too unwieldy.



Annexure B

Pre-requisites and Methodology for Certification of Cyber Security Professionals

The prerequisites and methodology for certification of cyber security professionals is given in Table 2A below.

Table 2A: Pre-requisites cum Methodology for Certification of Cyber Security Professionals

Expertise Level (Level of certification)	Pre Requisite Minimum expertise level attained in the associated cyber security domains	Methodology of Initial Assessment	Methodology of Surveillance	Methodology of Recertification
FOUNDATION	No requirement	1. Written Exam (Physical / Proctored online). 2. Practical testing of skills.	Twice in a certification cycle (between 12 to 36 months) through verification of peer reviews and/or continuous professional development logs and/or self-declaration from certified cyber security professionals and/or customer feedback	After every 3 years
ADVANCED	2 years of work experience in the relevant field with demonstration of completed 2 Project.	1. Review of credentials/ Resume/ experience logs. 2. Written Exam (Physical / Proctored online). 3. Practical / Simulation.		Satisfactory performance during previous certification cycle
MASTER	3 years of work experience in the relevant field with demonstration of completed 3 Projects of complex in nature.	1. Review of credentials/ Resume/ experience logs/ publications. 2. Presentation (Face to Face/ Virtual). 3. Practical / Simulation. 4. Interaction with panel (at least 3 members).		Completion of at least 50 hours trainings in three years as per scope. Assessment methods same as initial assessment.



Annexure C

Guidance for Cyber Security Professionals on Selection of Competency Profiles for Certification

This Annexure provides general guidance to cyber security professionals on choosing competency profile(s) for certification that are appropriate for the knowledge and skills they wish to acquire in the cyber security career. Table 3A gives a generic mapping between the certification codes/ id and the capability expected of the cyber security professional to carry out work, activities and tasks of the associated cyber security domain and functions. This guidance is to be used by cyber security professionals and organizations to chart their certification road maps.

Table 3A: Mapping Certification Code/ Id to work, activities and tasks expected to be carried out by the Certificate Holder

S. No.	Certification Code / Id	Certification Title (Cyber security Domain & Expertise Level)	Cyber security Functions	Work, activities and tasks expected to be carried out by the Certificate Holder
1	GRC-F	Governance, Risk and Compliance (Foundation)	GA	Conduct risk assessment to help identify cyber security risks and determine appropriate controls to ensure that IT and ICS systems perform within acceptable limits of risks. Monitor, track and manage risk mitigations and exceptions to ensure compliance with cyber security standards and policies.
2	GRC-A	Governance, Risk and Compliance (Advanced)	GA	Drive cyber security policies, standards and guidelines aligned to the organization's risk management framework, legislation and regulation. Responsible for establishing and approving ISMS policies, standards and guidelines to effectively manage cyber security risks, integrate and align the cyber risk management framework in the organization's context.
3	GRC-M	Governance, Risk and Compliance (Master)	GA	Strategize, design GRC framework and ISMS for organizations and drive projects and investments for cyber security of the organization.
4	TSA-F	Technology & System Security Architecture (Foundation)	AP	Provide engineering support in the field for security and security management of in-production/ in-use IT and ICS systems of both on-premises and cloud infrastructure of organizations.
5	TSA-A	Technology & System Security Architecture (Advanced)	AP	Conceptualise, design, engineer, integrate and implement the security and security management aspects in IT and ICS systems of both on-premises and cloud infrastructure of organizations.



S. No.	Certification Code / Id	Certification Title (Cyber security Domain & Expertise Level)	Cyber security Functions	Work, activities and tasks expected to be carried out by the Certificate Holder
6	TSA-M	Technology & System Security Architecture (Master)	AP	<p>Strategize, conceptualise, design, engineer, integrate the security and security management aspects of large, complex IT and ICS systems of both on-premises and cloud infrastructure of organizations.</p> <p>Identify IT and ICS cyber security needs of the organization and translate them into security designs and principles. Recommend and lead the adoption of new technological advances and best practices in IT and ICS systems to mitigate security risks.</p>
7	SSD-F	Secure Software Development (Foundation)	AP	Provide security engineering support for development of secure software (DevSecOps, secure CI/CD and AI/ML pipelines).
8	SSD-A	Secure Software Development (Advanced)	AP	Design, oversee and manage secure software design and engineering, including secure software supply chain management.
9	AST-F	Application Security Testing (Foundation)	AP	Security testing of software platforms and applications prior to use in production environment and prior to upgrades.
10	AST-A	Application Security Testing (Advanced)	AP	Oversee and manage the security testing of software platforms and applications.
11	PST-F	Product Security Testing (Foundation)	AP	Security testing of hardware, devices and appliances prior to use in production environment and prior to upgrades.
12	PST-A	Product Security Testing (Advanced)	AP	Oversee and manage the security testing of hardware, devices and appliances.
13	NSA-F	Network Security Administration (Foundation)	OM	<p>Configure, operate, and administer the day to day security aspects of telecom, IT and ICS networks of organizations.</p> <p>Network devices, appliances and platforms include switches, routers, firewalls, IDS/ IPS, NAC, VPN, log collectors & aggregators, encryption in-transit (IPSEC, SSL), DNS, DHCP, proxy servers, bastion hosts.</p>



S. No.	Certification Code / Id	Certification Title (Cyber security Domain & Expertise Level)	Cyber security Functions	Work, activities and tasks expected to be carried out by the Certificate Holder
				Work to be done using enterprise platforms for patch management, configuration management (CMDB), ticketing and incident management, NMS (network management), reporting.
14	NSA-A	Network Security Administration (Advanced)	OM	Plan, design, engineer, analyse, oversee the security and security management aspects of telecom, IT and ICS networks of organizations.
15	SSA-F	System Security Administration (Foundation)	OM	<p>Configure, operate, administer the day to day security aspects of systems of both on-premises and cloud infrastructure of organizations.</p> <p>Systems include HW, VM, OS, virtual switches and routers (on cloud), encryption at-rest (PKI, certificate management), domain services, security appliances like SIEM.</p> <p>Work to be done using enterprise platforms for patch management, configuration management (CMDB), ticketing and incident management, EMS (systems management), reporting.</p>
16	SSA-A	System Security Administration (Advanced)	OM	Plan, design, engineer, analyse, oversee the security and security management aspects of systems of both on-premises and cloud infrastructure of organizations.
17	ADS-F	Applications & Data Security Administration (Foundation)	OM	<p>Configure, operate, administer the day to day security aspects of both on-premises and cloud software platforms (including SaaS) of organizations.</p> <p>Software platforms include web servers, application servers, database servers, business application platforms, email, content management and sharing platforms.</p> <p>Work to be done using enterprise platforms for identity, role-based access management, LDAP, zero-trust infrastructure, IT and ICS asset management, EMS (application management), ITSM and ISMS platforms for patch management, configuration management</p>



S. No.	Certification Code / Id	Certification Title (Cyber security Domain & Expertise Level)	Cyber security Functions	Work, activities and tasks expected to be carried out by the Certificate Holder
				(CMDB), ticketing and incident management, compliance management, reporting.
18	ADS-A	Applications & Data Security Administration (Advanced)	OM	Plan, design, engineer, analyse, oversee the security and security management aspects of software platforms of both on-premises and cloud infrastructure (including SaaS) of organizations.
19	SSS-F	Security Support Services (Foundation)	OM	Operate and support the day to day security issues of end user systems and devices.
20	SSS-A	Security Support Services (Advanced)	OM	Plan, design, engineer, analyse, and oversee the security and security management aspects of end user systems and devices.
21	SPM-F	Security Performance Management (Foundation)	OM	Collect, collate, normalise, analyse cyber security related data for assessing performance of cyber security functions
22	SPM-A	Security Performance Management (Advanced)	OM	Plan, design, engineer, oversee the cyber security performance analysis to derive insights and identify areas of improvement.
23	ICS-F	ICS Cyber Security for Power Sector (Foundation)	OM	Operate, administer the day to day security aspects of ICS environment of organizations.
24	ICR-F	ICS Cyber Risk Assessment for Power Sector (Foundation)	AI	Develop and implement cyber risk assessment and mitigation strategies across the systems' life-cycle, taking into consideration the organization's OT environment and external threats.
25	ICR-A	ICS Cyber Risk Assessment for Power Sector (Advanced)	AI	Assess and direct enhancements to OT cyber risk assessment techniques, and develop strategies to address and mitigate OT cyber risks.
26	ICD-A	ICS Cyber Security Design & Implementation for Power Sector (Advanced)	AP	Embed security principles into the design and specification of security architectures and controls for OT systems to meet defined OT cybersecurity needs
27	ICD-M	ICS Cyber Security Design & Implementation for Power Sector (Master)	AP	Embed security principles into the design of security architectures and establish organizational guidelines for the



S. No.	Certification Code / Id	Certification Title (Cyber security Domain & Expertise Level)	Cyber security Functions	Work, activities and tasks expected to be carried out by the Certificate Holder
				design of OT security controls driving the enhancement of organization-wide OT security systems
29	ICM-A	ICS Cyber Security Operations & Maintenance for Power Sector (Advanced)	OM	Administrate network and monitor to provide for optimum levels of network performance and minimisation of downtime. Deploy vulnerability mitigations and patches in phases to minimise operation disruption during testing, deployment and validation to mitigate vulnerabilities in OT systems.
29	ICM-M	ICS Cyber Security Operations & Maintenance for Power Sector (Master)	OM	Administrate network and monitor to provide for optimum levels of network performance and minimisation of downtime. Management of detection, isolation, recovery and limitation of the impact of failures on the network as well as provision of support to system users through ongoing maintenance information sharing and training. Deploy vulnerability mitigations and patches in phases to minimise operation disruption during testing, deployment and validation to mitigate vulnerabilities in OT systems.
30	CYD-F	Cyber Defence (Foundation)	AI	Operate, carry out the day to day cyber defence functions like rogue asset discovery, vulnerability tracking, cyber threat intelligence (CTI) analysis.
31	CYD-A	Cyber Defence (Advanced)	AI	Plan, design, engineer, analyse, and oversee the security and security management aspects of cyber defence. May include cyber security management of outsourced and third-party service providers like MSPs and MSSPs.
32	CYD-M	Cyber Defence (Master)	AI	Develop frameworks, strategies and processes for protection, threat and cyber incident detection, response, recovery in the IT environment.
33	CRM-F	Cyber Vulnerability, Threat & Risk Management (Foundation)	AI	Carry out the day to day vulnerability and risk assessment, threat hunting activities, technical audits.



S. No.	Certification Code / Id	Certification Title (Cyber security Domain & Expertise Level)	Cyber security Functions	Work, activities and tasks expected to be carried out by the Certificate Holder
				Proactively scan logs, network traffic, SIEMs and other channels for suspicious behaviours and indicators of compromise. Identify IT and ICS assets prone to cyber threats and attacks, monitor for potential threats actors/ groups/ individuals attempting cyber-attacks.
34	CRM-A	Cyber Vulnerability, Threat & Risk Management (Advanced)	AI	Plan, design, engineer, oversee, manage the vulnerability and risk assessment, threat hunting activities, and technical audits. Derive deep insights for providing strategic direction and investments.
35	SCO-F	Security Operations (Foundation)	AI	Carry out the day to day security operations activities in the SOC, like surveillance and monitoring of IT and ICS systems and assets, support the identification of threats and vulnerabilities, provide incident response and remediation support.
36	SCO-A	Security Operations (Advanced)	AI	Plan, design, engineer, oversee, manage the security operations in the SOC. Respond to cyber incidents coordinate with departments for containment and mitigation of incidents and recovery.
37	CYF-F	Cyber Forensics & Investigation (Foundation)	AI	Analyse and investigate cyber incidents to identify breaches, loopholes, process deviations, failures.
38	CYF-A	Cyber Forensics & Investigation (Advanced)	AI	Plan, direct, oversee, monitor and manage the cyber forensic analysis and investigation activities into the cause and impact of incidents, develop detailed reports on incident timeline, evidence, findings, conclusions and recommendations.
39	CYF-M	Cyber Forensics & Investigation (Master)	AI	Strategize, design, engineer, integrate cyber forensics and investigation processes into the security management of large, complex IT and ICS systems of both on-premises and cloud infrastructure of organizations.
40	CTA-F	Cyber Training & Awareness (Foundation)	TE	Manage the routine cyber security training and awareness programmes.
41	CTA-A	Cyber Training & Awareness (Advanced)	TE	Design cyber security curriculum for end users, IT and ICS specialists and managers.

Annexure D

Suggested usage of the Scheme by Organizations

- 1.1. Diagrammatic view of the Scheme from an organization's perspective is given in Figure A 4.1 below.

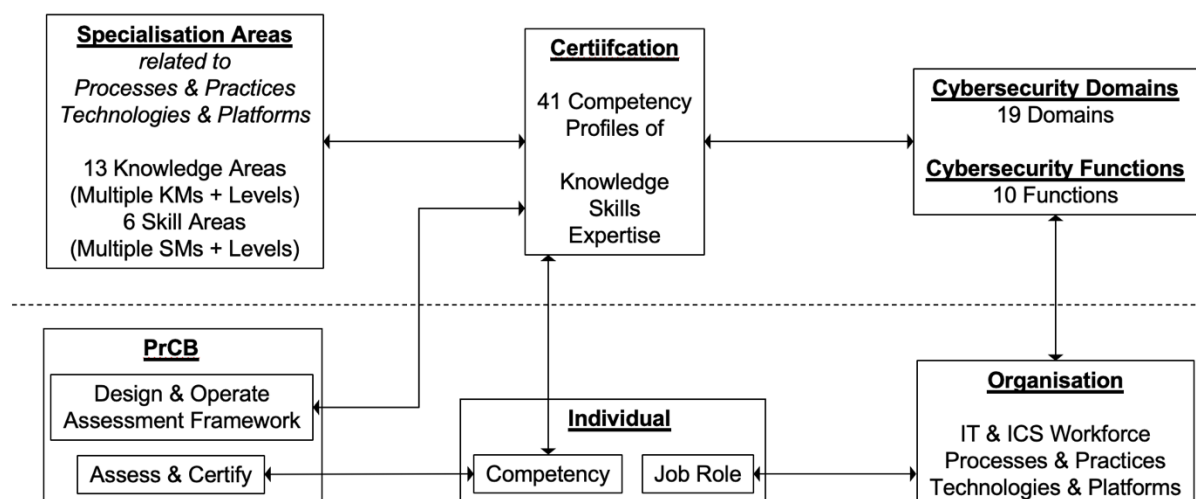


Figure A 4.1: Diagrammatic View of the Scheme from an organization's perspective

- 1.2. Cyber security functions comprise technical and management activities that Organizations need to carry out to be cyber resilient. Organizations can implement the cyber security functions through institutionalised practices and processes that are carried out by a trained workforce, enabled by technology and tools. The process, people and technology combination together will enable the Organizations to accomplish their mission, fulfil their legal and regulatory requirements, maintain their day-to-day functions, and protect their assets and individuals.
- 1.3. The cyber security functions and their objectives are described using ten action-verbs. The first five action-verbs, namely Identify, Protect, Detect, Respond and Recover, are termed as core cyber security functions. These comprise day to day and periodic operating processes and practices that are primarily carried out by the IT, OT and IS technical teams. The next five action-verbs, namely, Govern & Administer, Acquire & Provision, Operate & Maintain, Analyse & Investigate, Train & Enable, are termed as cyber security support functions. These comprise the larger management processes and practices that are collaboratively carried out by different units and departments of the organization. Together, these ten cyber security functions provide a common vocabulary for communication of cyber security activities and desired outcomes within the organizations, from the executive level to the implementation/operations level, and with external stakeholders.
- 1.3.1 Identify (ID) function addresses the need for Organizations to identify things of value that need to be secured and protected from harm.
- 1.3.2 Protect (PR) function addresses the need for Organizations to develop capabilities to ensure resilience in the delivery of mission and business critical services. Actions under



this function are directed towards safeguarding the regular daily functions of organizations, delivery of critical services, and minimising the possibility and impact of cyber-attacks and insider threats.

- 1.3.3 Detect (DE) function addresses the need for Organizations to develop capabilities in the day-to-day operations to observe and detect vulnerabilities, threats and risks associated with anomalous events, activities and user behaviours, policy violations and non-compliances, security control effectiveness, failure of cyber security processes etc. Monitoring each of these parameters can provide advance insights to mitigate a potential cyber security breach.
- 1.3.4 Respond (RP) function addresses the need for Organizations to develop capabilities in the day-to-day operations to act on detected cyber security breaches and cyber-attacks and respond to the same in order to contain/ mitigate their adverse impact.
- 1.3.5 Recover (RC) function addresses the need for Organizations to develop capabilities in the day-to-day operations to rapidly restore the business, IT and ICS functions and/ or services that were impaired due to cyber-attack.
- 1.3.6 Govern & Administer (GA) function addresses the need for Organizations to develop policies, practices, processes and oversight mechanisms for governance and administration of people, processes, and systems on a day-to-day and periodic basis.
- 1.3.7 Acquire & Provision (AP) function addresses the need for Organizations to develop policies, practices, processes and oversight mechanisms for acquisition and provisioning of trustworthy systems.
- 1.3.8 Operate & Maintain (OM) function addresses the need for Organizations to develop policies, practices, processes and oversight mechanisms for secure operations and maintenance of systems.
- 1.3.9 Analyse & Investigate (AI) function addresses the need for Organizations to continually design, develop, test, implement, analyse and improve the core and supporting cyber security functions, thereby improving the cyber resiliency of the organization.
- 1.3.10 Train & Enable (TE) function addresses the need for Organizations to train the IT Operations and IT Security workforce and other employees (users of IT services) in all the above-mentioned cyber security functions.
- 1.4 Aspects of usage of the Scheme by different organizations are described below.
 - 1.4.1 An organization can classify its information security/ cyber security functions under different cyber security domains defined in the Scheme and use the associated competency profiles to ensure that the competencies of the workforce are aligned to the work roles and responsibilities of the different cyber security domains.
 - 1.4.2 The Scheme provides a framework of knowledge and skills in various domains and across various categories, which can be used by the organizations while recruiting and promoting their cyber security workforce. The organizations may define the job roles for various cyber security functions in terms of the work, activities, tasks and responsibilities associated with the job roles. Organizations may use Annex 1A mentioned In Section 3 of this document to list out and describe the knowledge and skills requirements and

expertise level for each of their cyber security related job roles. This is usually established by the senior management.

- 1.4.3 The knowledge, skills and expertise levels required for each job role can then be translated into cyber security competency profile certifications that the workforce should possess/ acquire in order to be assigned the job role. Organizations may use Annex 1B mentioned in Section 3 of this document to map the knowledge, skills and expertise requirements of their job roles to the competency profiles offered under this Scheme.
- 1.4.4 The competency profile certifications under this Scheme are granted by independent third-party Certification of Persons Bodies (PrCB). Hence, organizations can be confident that their workforce possessing the competency profile certifications have the required knowledge, skills and expertise as appropriate to their certification.
- 1.4.5 Organizations may also use the competency profiles framework to design their training programs or hire training bodies to train their workforce in different cyber security domains listed in this Scheme, as part of their capability development programs. Organizations may use the knowledge and skills statements listed in Annex 1A of Section 3 for designing the training curriculum for different cyber security domains.
- 1.4.6 The mapping of competency profiles offered under this Scheme to an organization's job roles can also be useful in the organization's recruitment/ hiring program. Organizations can use the competency profile certifications provided by independent PrCBs as a basis for selection, rather than carrying out their own testing and evaluation of competencies.
- 1.4.7 The competency profile certifications can also be used by organizations to demonstrate the regulators and national agencies that cyber security personnel employed in critical IT & ICS domains have the required competence to carry out the respective job role responsibilities.
- 1.5 Cyber security domains and functions of an organization are given in Figure A4.2 below.

Cybersecurity Domains	Organisational		Technical [Cyber Security]		Technical [IT & ICS Security]				
	GA	TE	AI		AP				
			DE	RP	ID	PR	DE	RP	RC
Leadership	Governance		Cyber Resilience		Use of Technology & Systems				
Management	Risk & Compliance		Cyber Security		Technology & Systems Security				
Operations	GRC		Security Operations	Cyber Defence	Security Support	Applications & Data Security			
			Vulnerability, Risk, Threat Analysis	Cyber Forensics	IT / ICS Systems Security	Network Security			
Engineering	Cyber Training & Awareness		Security Performance	ICS Cyber Security	Technology & System Security Architecture	Secure Software Development			
					Product Security Testing	Application Security Testing			

Figure A4.2: Cyber security Domains

1.6 Generic Mapping of Typical Job Roles to Cyber security Functions and Expertise Levels

1.6.1 Figure A4.3 below gives a generic mapping of typical job roles in CSEs and other organizations with the cyber security functions and the organizational hierarchy.

1.6.2 The mapping is done across three dimensions:

- Dimension–1 - Cyber security Domains and Functions.
- Dimension–2 - Level of Organizational Hierarchy.
- Dimension–3 - Organizational job roles describing work, tasks and responsibilities.

Cybersecurity Domains	Organisational	Technical [Cyber Security]	Technical [IT & ICS Security]
Master Strategist Architect	3. IT GRC Strategist	35. Cyber Defence Architect 28. Cyber Defence Strategist	6. Technology & System Security Architect 25. ICS Cyber Security Architect
	2. Chief Information Security Officer (CISO)	5. Chief IT Officer (CIO), Chief Technology Officer (CTO)	
Advanced Manager Administrator Engineer Analyst Team Leader	2. Information Security Officer (ISO) 37. Cyber Training Curriculum Manager	Cyber Security Manager [Any Certification] 32. Security Operations Analyst 34. Cyber Forensics Analyst 30. Vulnerability, Risk, Threat Analyst 27. Cyber Defence Analyst 22. Security Performance Analyst	IT, ICS Security Manager [Any Certification] 20. Security Support Team Leader 18. Apps & Data Security Admin 12. Product Security Analyst 16. System Security Admin 10. Software QA Team Leader 14. Network Security Admin 5. Technology & System Security Team Leader 8. Software Security Team Leader 24. ICS Cybersecurity Analyst
Foundation Operator Engineer Specialist Developer Tester	1. IT GRC Specialist 36. Cyber Training & Awareness Specialist	31. Security Operations Specialist 29. Vulnerability, Risk, Threat Specialist 26. Cyber Defence Specialist 21. Security Performance Specialist	19. Security Support Operator 17. Apps & Data Security Engineer 11. Product Security Tester 15. System Security Engineer 9. Software QA Engineer 13. Network Security Engineer 4. Field Security Engineer 7. Software Security Engineer 23. ICS Cybersecurity Specialist

Figure A4.3: Mapping of Job Roles to Cyber security Functions and Expertise Levels



Annexure E

Table A5.1 Indicative Mapping of Certification Codes/ Ids to Organization Job Roles

Table A5.1 below describes a few of the typical cyber security related job roles (job titles), the work, activities and tasks (job description) required to be done as part of the job role, the knowledge and skills required for doing the work and indicative Scheme certifications that are applicable to the job role.

S. No	Organization Job Role (Job Title)	Work, activities and tasks required to be done as part of the Job Role (Job Description)	Knowledge & Skills Required	Certifications	Applicable to
1	IT-GRC Specialist	Conduct risk assessment to help identify cybersecurity risks and determine appropriate controls to ensure that IT and ICS systems perform within acceptable limits of risks. Monitor, track and manage risk mitigations and exceptions to ensure compliance with cybersecurity standards and policies.	KM-0601F SM-0602F	GRC-F	All entities
2	Information Security Officer (ISO) Chief Information Security Officer (CISO)	Drive cybersecurity policies, standards and guidelines aligned to the organization's risk management framework, legislation and regulation. Responsible for establishing and approving ISMS policies, standards and guidelines to effectively manage cybersecurity risks, integrate and align the cyber risk management framework in the organization's context.	KM-0601F, KM-0601A, KM-0701F SM-0602F, SM-0602A, SM-0603A	GRC-F, GRC-A	Small, medium and large entities, Consultancy Orgs, Training Bodies
3	IT GRC Strategist	Strategize, design IT GRC framework and ISMS for organizations and drive projects and investments for cybersecurity of the organization.	KM-0601F, KM-0601A, KM-0601M, KM-0701F, KM-0701A SM-0602F, SM-0602A, SM-0603A	GRC-F, GRC-A, GRC-M	Very large entities (conglomerates), Consultancy Orgs
4	Cyber Defence Specialist	Operate, carry out the day to day cyber defence functions like rogue asset discovery, vulnerability tracking, cyber threat intelligence (CTI) analysis.	KM-0804F, KM-0901F SM-0101F, SM-0501F	CYD-F	All entities, MSSPs



S. No	Organization Job Role (Job Title)	Work, activities and tasks required to be done as part of the Job Role (Job Description)	Knowledge & Skills Required	Certifications	Applicable to
5	Cyber Defence Analyst	Plan, design, engineer, analyse, and oversee the security and security management aspects of cyber defence. May include cybersecurity management of outsourced and third-party service providers like MSPs and MSSPs.	KM-0804F, KM-0804A, KM-0901F, KM-0901A, SM-0101F, SM-0501F, SM-0501A	CYD-F, CYD-A	Medium, large & very large entities, Consultancy Orgs, Training Bodies, MSPs, MSSPs
6	Cyber Defence Strategist	Develop frameworks, strategies and processes for protection, threat and cyber incident detection, response, recovery in the IT environment.	KM-0804F, KM-0804A, KM-0901F, KM-0901A, KM-0901M, SM-0101F, SM-0501F, SM-0501A, SM-0601F, SM-0601A, SM-0603A	CYD-F, CYD-A, CYD-M	Very large entities, Consultancy Orgs
7	Vulnerability, Threat, Risk Specialist	Carry out the day to day vulnerability and risk assessment, threat hunting activities, technical audits. Proactively scan logs, network traffic, SIEMs and other channels for suspicious behaviours and indicators of compromise. Identify IT and ICS assets prone to cyber threats and attacks, monitor for potential threats actors/ groups/ individuals attempting cyber-attacks.	KM-0804F SM-0101F	CRM-F	Medium, large & very large entities, MSSPs
8	Vulnerability, Threat, Risk Analyst	Plan, design, engineer, oversee, and manage the vulnerability and risk assessment, threat hunting activities, and technical audits. Derive deep insights for providing strategic direction and investments.	KM-0804F, KM-0804A, SM-0602F, SM-0602A, SM-0603A	CRM-F, CRM-A	Medium, large & very large entities, Consultancy Orgs, Training Bodies, MSSPs
9	Security Operations Specialist	Carry out the day to day security operations activities in the SOC, like surveillance and monitoring of IT and ICS systems and assets, support the identification of threats and vulnerabilities, provide incident response and remediation support.	KM-0201F, KM-0803F, SM-0101F	SCO-F	Medium, large & very large entities, MSSPs



S. No	Organization Job Role (Job Title)	Work, activities and tasks required to be done as part of the Job Role (Job Description)	Knowledge & Skills Required	Certifications	Applicable to
10	Security Operations Analyst	Plan, design, engineer, oversee, manage the security operations in the SOC. Respond to cyber incidents coordinate with departments for containment and mitigation of incidents and recovery.	KM-0201F, KM-0201A, KM-0803F, KM-0803A SM-0101F	SCO-F, SCO-A	Medium, large & very large entities, Consultancy Orgs, Training Bodies, MSSPs
11	Cyber Forensics Specialist	Analyse and investigate cyber incidents to identify breaches, loopholes, process deviations, failures.	KM-1101F SM-0101F, SM-0501F	CYF-F	Medium, large & very large entities, Consultancy Orgs, MSPs, MSSPs
12	Cyber Forensics Analyst	Plan, direct, oversee, monitor and manage the cyber forensic analysis and investigation activities into the cause and impact of incidents, develop detailed reports on incident timeline, evidence, findings, conclusions and recommendations.	KM-1101F, KM-1101A SM-0101F, SM-0501F, SM-0501A	CYF-F, CYF-A	Medium, large & very large entities, Consultancy Orgs, Training Bodies, MSPs, MSSPs
13	Cyber Defence Architect	Strategize, design, engineer, integrate cyber forensics and investigation processes into the security management of large, complex IT and ICS systems of both on-premises and cloud infrastructure of organizations.	KM-1101F, KM-1101A, KM-1101M SM-0101F, SM-0501F, SM-0501A	CYF-F, CYF-A, CYF-M	Very large entities, Consultancy Orgs
14	Cyber Training & Awareness Specialist	Manage the routine cybersecurity training and awareness programmes.	KM-1201F SM-0601F	CTA-F	All entities
15	Cyber Training & Curriculum Manager	Design cybersecurity curriculum for end users, IT and ICS specialists and managers.	KM-1201F, KM-1201A SM-0601F, SM-0601A	CTA-F, CTA-A	Large & very large entities, Consultancy Orgs, Training Bodies

SECTION 4

CERTIFICATION PROCESS



1. Introduction

The document aims to establish the process required to be followed by the certification body to assess the competence of cyber security professional as per the knowledge and skills defined in the section 'Requirement for Certification of Persons' of this Scheme. This document shall be used by the applicant, PrCB and the organization that wish to lend their professionals to the attestation by the PrCBs.

2. Objective

The objective of this document is to define the process of certification of cyber security professionals under the Scheme to promote uniformity in its implementation among the PrCBs, the cyber security professionals seeking certification across domain and categories, though provisionally approved PrCB from QCI or accredited PrCB from any AB that is an IAF member for the required scope.

3. Scope

This document explains the process of certification under the Scheme and the requirements that should be followed in order to obtain and maintain the certification.

- 3.1 The purpose of assessment under this Scheme, is to certify individual applicants as cyber security professionals for establishing their necessary competence to implement, monitor, maintain and manage across the domain, either as a self- employed or as an employee of organizations.
- 3.2 The necessary knowledge and skills statements have been identified against each competence criteria.
- 3.3 A competency profile for certification of cyber security professional is defined as a set of knowledge and skill modules that are relevant to a cyber security domain, combined with a measurable level of expertise attained for that knowledge and skills. A single Knowledge or Skill module may be applied to one or more competency profiles. Each cyber security domain has one or more competency profiles associated with it that addresses the requirements of different levels of expertise for that domain.
- 3.4 The competency profiles for certification under the Scheme have been defined in Section 3 of this document.
- 3.5 Certification of cyber security professionals under this Scheme shall be carried out by the PrCBs provisionally approved by QCI or accredited by any other IAF member AB for the Scheme, as per ISO/IEC 17024:2012. However, until such time the market develops, QCI, as Scheme Manager, may directly evaluate applicants on the basis of a defined competence criteria.
- 3.6 The validity of the certification of cyber security professionals shall be for a period of 3 years from the date of decision that will be duly recorded upon fulfilment of Scheme requirements. The re-certification needs to be applied 4 months in advance before the validity of the certificate.



4. Certification Process

4.1 Registration of Application

- 4.1.1 The approved PrCB shall respond to all enquiries received from prospective applicants for certification as cyber security professionals with complete information on the certification process, appropriate to certification scheme (including fee structure), a list of documents containing the requirements for certification, the applicants' obligations and rights and the duties of a certified person which includes a code of conduct declaration within 7 days of receipt of the query.
- 4.1.2 The applicant shall apply to the approved PrCB in the Application format prescribed by the PrCB.
- 4.1.3 The applicant shall declare whether he/she has been an applicant or a candidate, or a person certified under this Scheme by any other PrCB, and if yes, then shall provide details of status of application/certification, scope and period of certification as appropriate. The PrCB may verify the information provided by contacting the earlier PrCB.
- 4.1.4 The applicant shall, along with the application, declare any pending judicial proceedings relating to his/her conduct, and/or any pending proceedings by any regulatory body. Application from such an applicant shall not be entertained. The applicant shall also declare any instances of discomfort/disability caused during any of his/her previous applications in the past 2 years.
- 4.1.5 All applications for certification shall be reviewed by the PrCB for completeness and adequacy, and deficiencies observed, if any, shall be informed to the applicant within 7 days of receipt of the application. Records of review shall be maintained.
- 4.1.6 All applications, found complete, shall be registered within 7 days of receipt of application/additional information, in the order of receipt with a unique identification number, duly acknowledged and records maintained. Registration shall be done, if found complete.
- 4.1.7 Applicants found violating the terms and conditions of the scheme during the certification process, shall be rejected after a due notice of 15 days.
- 4.1.8 Applications from applicants who have misused the earlier certification or whose earlier certification was cancelled/application rejected because of violation of terms & conditions, shall not be registered within one year of cancellation of the certificate/rejection of applicant by any PrCB.
- 4.1.9 Requests for certification from ex-applicants shall be processed like a fresh applicant and the entire procedure for grant of certification be adhered to.
- 4.1.10 PrCB shall reject or close all applications under the following conditions:
 - a. If deficiencies observed in the application are not satisfactorily completed within 1 month.
 - b. If the applicant does not take the evaluation within 03 months of registration of application.



- c. Misuse of certification mark, if any.
- d. Evidence of malpractice.
- e. Voluntary withdrawal of application.

4.1.11 In the event of a closure/rejection of an application, the application fee submitted with the application may be refunded as per the policy of the certification body.

4.1.12 In case of any request submitted by an applicant for accommodating special needs like separate examination area, translator, reader etc., PrCB shall address the same without compromising the scheme requirements. Request for Special Accommodation(s) during the application stage must be received at least 45 days prior to the date of preferred examination.

4.1.13 Requests for special needs accommodation require documentation of a formally diagnosed and qualified disability by a qualified professional who has provided evaluation or treatment for the candidate in the format provided by the PrCB.

Note: Requests without proper documentation shall not be processed until all required documentation is received by PrCB and the 45-day advance notice window will begin as on the date of receipt of all documentations.

4.2 Competence Evaluation Process

4.2.1 The Scheme has developed assessment method for evaluating the competence of cyber security professionals which is elaborated in Table 4.1.

Table 4.4: Assessment Method for Cyber Security Professionals

Levels	Foundation	Advanced	Master
Educational Qualification	N/A	Graduate in computer science, computer engineering, telecommunication engineering, cyber security, information technology, software engineering, information systems etc.	Graduate in computer science, computer engineering, telecommunication engineering, cyber security, information technology, software engineering, information systems etc.
Total experience	N/A	2 years	3 years
Cyber security relevant domain specific experience	0	At least in 1 domains	
Cyber security relevant experience (in years)	0	1 year	2 years
Minimum Exam/Assessment duration (in minutes)	60	60	120 minutes (@60 minutes/assessment)



Levels	Foundation	Advanced	Master
Minimum No. of questions (each domain to carry equal weightage)	45	45	Case Study and Interview
Exam focus	Assess the knowledge, skills and ability to implement, deploy, operate and manage cyber security of IT & ICS in organizations, using platforms and tools	Assess the ability to understand and govern IT & ICS cyber security in organizations, identify and manage risks, monitor performance and compliance, and provide direction and leadership in cyber security	Assess the ability to provide mentorship in cyber security governance, cyber defence, cyber forensics, and design and integration of cyber security solutions across IT & ICS
Knowledge	50%	20%	N/A
Skill/Demonstration	50%	20%	20%
Case Study/Interview	N/A	60%	80%
Minimum marks required in each module	50%	50%	50%
Minimum aggregate %	70%	70%	70%

4.2.2 Written Examination

- The PrCB shall develop a question paper for the written examination to assess the knowledge of candidate. The question test papers shall be set by competent personnel as designated by the PrCB. The question paper for the examination shall be picked up from the bank not more than 3 days before the date of the examination.
- The certification body shall update the question bank to avoid any repeatability and shall adhere to the prescribed domain and corresponding category.
- The PrCB shall ensure that no question is repeated with the same content and language, and same sequence of answers in the multiple-choice questions.
- The evaluation shall be conducted in English language.

4.2.3 Skill/ Demonstration

- The PrCB shall have a procedures for the examiner to assess the skill sets possessed by the candidate commiserating to the applied scope. Practical/Simulation if done through virtual mode duly recorded, same shall be conducted with adequate provisions of safety and security to eliminate risks pertaining to unethical practices.
- Case Study/Interview: The PrCB shall prepare questions and guidelines for the Interview and a structured evaluation record to be maintained for the same. Interview can be done through virtual mode with adequate provisions of safety and security to eliminate risks pertaining to unethical practices. The interaction will be carried out with the objective to



assess the ability of the candidate to demonstrate practical application of knowledge in terms of critical thinking and analytical skills in the designed/scenario based case study as per the scope of certification.

- c. There shall be a minimum of 1 examiner who shall evaluate the candidates and provide a final score. In case marking is done through a software/app-controlled system, validation of the same shall be done once initially and at least once in 12 months thereafter.
- d. The PrCB shall ensure that the questions for written and oral evaluation, and the guidelines for demonstration/case studies are fair, valid and reliable across test centres, across time zones and across examiners.

- 4.2.4 The evaluation of the applicants shall be conducted within 3 months extendable to 6 months of registration of application, failing which the application fee shall be refunded by the PrCB.
- 4.2.5 The PrCB shall schedule the evaluations (written, demonstration and oral interview, simulation/demonstration, etc.) as and when the number of applicants totals to 5 as a minimum. The PrCB at its discretion may evaluate with a smaller number of candidates. The PrCB shall ensure that the certification process is completed within 15 days from the date of the actual evaluation.
- 4.2.6 The PrCB shall inform all applicants who meet the eligibility criteria, regarding the dates of evaluation, including those appearing for a re-evaluation, and the means of evaluation at least 15 days prior to the evaluation. The PrCB shall host as a publicly available information through its website, the dates for the written examination and the names of the candidates.
- 4.2.7 The PrCBs shall have requisite test bed or shall have formal agreement with a facility which possess a testbed, test run environment, test tool, techniques and process capable of testing all skills of applicants to the Scope which is sought by the PrCB at desired levels for which the PrCB would be issuing the certification. PrCB to ensure that all skills shall be necessarily evaluated based on hands on demonstration of skills in a reliable, repeatable and reproducible manner. The technical expert of the certification body shall be witnessing the efficacy of the test bed at the time of evaluation and approval of PrCB.
- 4.2.8 The approval shall be granted by QCI and by NABCB by engaging experts of the relevant domain areas of the Scope sought by the PrCB. QCI shall grant provisional approval and subsequently NABCB shall grant accreditation.
- 4.2.9 The written examination test papers shall be available at the evaluation site in exact numbers required if examination is conducted in off-line mode.
- 4.2.10 The written examination shall be conducted under the supervision of an invigilator.
- 4.2.11 The certification body shall identify and nominate invigilators for this purpose. The invigilator shall, at the end of every written examination, collect all the Question-and-Answer sheets from each candidate that takes the written examination, seal immediately and forward them to the PrCB's office within one working day of completion of the



evaluation. In case of on-line mode, password protected mechanism and other adequate information security controls shall be implemented to ensure integrity of process.

4.2.12 The names/identities of the applicants shall be communicated well in advance to the Evaluation team for identification of conflict of interest, if any. Any conflicts identified with respect to the applicants shall be suitably addressed by the PrCB.

- a. The certification body shall make publicly available, through its website, the dates for the written, demonstration and oral evaluation. If the candidate has any conflict of interest and voluntarily decides not to undergo the oral evaluation, the PrCB shall provide them the option for another evaluation or reimburse the relevant application fee.
- b. Any conflicts identified, with respect to the candidate, shall be suitably addressed by the certification body.
- c. The certification body shall inform the candidate regarding the name of evaluation centre where the demonstration is being planned in advance, for the identification of conflict of interest, if any. If the applicant candidate has any conflict of interest and voluntarily decides not to undertake the demonstration, the PrCB shall provide them the option for another demonstration or reimburse the relevant application fee.

4.2.13 Checking of Evaluation Papers and Demonstration/Simulation Report

- a. The evaluation of written test answer sheets shall be carried out by a competent examiner.
- b. **Written** – The Examiner shall check the written answer sheets and consolidate the results within 15 days of the evaluation.
- c. **Oral/ Interview/ panel interaction** – Each member of the team of examiners shall record their results for each of the questions on a structured evaluation sheet against each candidate interviewed. The individual evaluation result for each candidate shall be discussed by the team. The representative of the PrCB shall at the end of the oral evaluation (interview/presentation/interaction) collect all the evaluation results from each of the team members, collate the results and calculate the consensus score for each question asked, seal and thereafter shall submit the same to the PrCB's office within one working day of completion of the evaluation.
- d. Candidate shall score a minimum of 50% each in the written, demonstration, oral interview/interaction, or any other applicable assessment method of the evaluations for qualifying as cyber security professional and is required to score a minimum of 70% as aggregate.
- e. PrCB may dismiss a candidate from the exam for any of the following reasons:
 - i. If the candidate's admission to the exam is unauthorized;
 - ii. If the candidate creates a disturbance or gives/receives help;
 - iii. If the candidate attempts to remove exam materials or notes from the testing room;
 - iv. If the candidate attempts to take the exam for someone else;



- v. If the candidate has in his/her possession any such item excluded from the exam centre, as specified above.
- vi. If the candidate exhibits behaviour consistent with memorization or copying of exam items
- f. Any candidate who removes or attempts to remove exam materials including memorizing exam questions or is observed cheating in any manner while taking the exam, will be subject to disciplinary and/or legal action. Any unauthorized individual found in possession of exam materials will be subject to disciplinary procedures in addition to possible legal action.

4.3 Decision on Certification

- 4.3.1 The certification body shall take a decision on certification that will be duly recorded and exhibited in the certificate, by a competent person(s) independent of evaluation(s), based on the information gathered during the certification process, and shall ensure the following;
 - a. The evaluation result of the candidate is not below the minimum specified;
 - b. Availability of necessary documentation as proof of the means of evaluation chosen to assess the candidate; and
 - c. Any other requirements prescribed by the Certification Body.
- 4.3.2 There shall be no conditional grant of certification.

The decision of the certification body shall be communicated to the candidate and QCI. QCI and PrCB shall maintain an updated register of candidate, certified cyber Security professionals with scope of certification and their status of certification.
- 4.3.3 When applicants fail to meet the acceptance criteria for evaluation, the PrCB shall inform them. The applicants may take another evaluation with the same or another PrCB, but would have to declare their previous performance while reapplying to other PrCB only after expiry of 06 month of earlier evaluation.
- 4.3.4 On grant of certification, the Certification body shall issue a Certificate, uniquely identified to the cyber security professional, indicating the name of the Professional, application number, cell phone number, scope (including certification code and title) of certification, language of examination, effective date, date of expiry, and the name of the certification body as a minimum.
- 4.3.5 The effective date of certification shall not be before the date of decision to grant the certification to the cyber security professionals.
- 4.3.6 The certification shall be for a period of 3 years from the date of decision to grant the certification. The effective date shall not be before the date of decision to grant certification.



4.4 Surveillance

- 4.4.1 The certified cyber security professionals for level foundation and above, shall be periodically evaluated as per the competence profile during the period of the valid certification.
- 4.4.2 The surveillance (as per applicability defined in Competence Profile document) shall be done by means of peer reviews, and continuous professional development logs, self-declaration cyber security professionals in a live session covering demonstration of knowledge, skills and ability.
- 4.4.3 The professional shall be responsible for maintaining and upgrading their level of knowledge and skill by undergoing training and maintaining records of the same.
- 4.4.4 The professional shall undertake a minimum of 16 hours of formal training per year and a minimum of 50 hours for a period of 03 years within the scope of certification.

4.5 Suspension of Certification

- 4.5.1 The certification body shall issue instructions to a certified person for the suspension of certification, with a notice of minimum 15 days, when;
 - a. the surveillance outcome is not satisfactory
 - b. any serious complaint/feedback which is found to be valid
 - c. any violation of terms and conditions of certification scheme
- 4.5.2 On receipt of instructions for the suspension of certification, the certified cyber security professional shall, with immediate effect, remove any reference(s) to certification, in any of his communication and/or presentation.
- 4.5.3 The certified cyber security professional after suspension shall be advised to undertake a root cause analysis and thereafter, identify and initiate necessary corrective actions for resolving the same.
- 4.5.4 The certification body shall revoke the suspension only when corrective actions have been taken and verified by the certification body.
- 4.5.5 The suspension shall not exceed a period of six months, provided it is still within the validity period of the certificate. The certified cyber security professional's inability to resolve issue(s) relating to the suspension within this period, shall lead to withdrawal of certification.

4.6 Withdrawal of Certification

- 4.6.1 The certification body shall withdraw the certification when;
 - a. Certified cyber security professional contravenes the terms and conditions of certification and provisions of this certification scheme, like claiming or displaying scope of certification other than that granted, or any fraudulent behaviour is established, etc.



- b. The corrective action(s) taken are not ensuring compliance, or the proposed plan for corrective action(s) will take a considerable time beyond 3 months for implementation;
 - c. Certified cyber security professional contravenes the Scheme's Code of Conduct
- 4.6.2 The certification body shall cancel the certificate at the request of the certified cyber security professional, if the certified professional is no longer interested.
- 4.6.3 In the event of cancellation, the certification body shall advise the cyber security professional to return the Certificate issued by the certification body. . In case of soft copy of the certificate, the professional shall confirm in a declaration that he/she doesn't retain the soft copy anymore.
- 4.6.4 On receipt of instructions for withdrawal of certification, the certified cyber security professional shall, with immediate effect, remove any reference to certification in any of his communication or/and presentation.
- 4.7 Renewal / Recertification**
- 4.7.1 The certification body shall send the Renewal notice to the certified cyber security professional, at least 4 months prior to the expiry of certificate validity period, to the registered email id of the cyber security professional and/or to the registered address.
- 4.7.2 The certified cyber security professional shall apply for renewal in the prescribed format along with the fee, if any prescribed by the PrCB, at least 3 months prior to expiry of certification.
- 4.7.3 The certification body shall review the performance of the certified cyber security professional seeking recertification (renewal of the Certificate), with respect to compliance in competence criteria during the entire certification cycle, prior to a decision on the renewal of the certificate.
- 4.7.4 The performance of the certified cyber security professional shall be reviewed on the basis of:
- a. The surveillance evaluation report(s);
 - b. Corrective actions taken on any feedback given during surveillance;
 - c. Any suspension of certificate during the previous validity period;
 - d. Complaints received, if any
 - e. Feedback reports from institution employed in, if applicable, obtained by the PrCB;
 - f. Adverse information, if any;
 - g. Peer review records;
 - h. Documented information related to continuous professional development;
- 4.7.5 Recertification of the certified cyber security professional shall be based on their satisfactory performance during the previous certification period, and shall be done before expiry of the certification.
- 4.7.6 Each certified professional, during the 3 years recertification period, shall undertake minimum 50 hours of training, for professional development in the relevant field. This



development may be in terms of participation in courses or seminars and/or other acceptable means of professional development, and shall be documented as per the PrCB's satisfaction, prior to recertification

- 4.7.7 The certification body shall not recertify cyber security professional with conditions for compliance to be verified subsequently. There shall be no conditional certification of cyber security professional.
- 4.7.8 The PrCB shall not recertify any certified cyber security professional whose certification is under suspension.
- 4.7.9 If performance of the certified cyber security professional is not satisfactory, the certification body shall withhold the recertification of the cyber security professional while clearly stating the reasons, and give time for effecting corrective actions. The verification and decision on recertification shall be taken within 6 months of the expiry date.
- 4.7.10 The certification body shall verify corrective actions.
- 4.7.11 The recertification shall be effective from the date of the expiry of the previous certificate, and the intervening period shall be treated as a period of suspension. The certified cyber security professional shall not claim certification during this period.
- 4.7.12 In case the certified cyber security professional does not abide to the satisfactory actions within three months, the certificate shall stand expired from the date of expiry of previous validity.
- 4.7.13 If a certificate is not renewed, it shall expire at the end of validity period.

4.8 Change(s) to the Level of Certification

- 4.8.1 A change to a higher level of certification on application by a professional, shall be done after ascertaining the competence, through the prescribed means of evaluation for an initial certification.
- 4.8.2 An applicant who applies for upgrade of the cyber security professional certificate to higher level, must have a valid cyber security professional certificate, must document that the cyber security professional examination has been passed for both the written and oral part, and must provide documentation and must fulfil all eligibility requirements.
- 4.8.3 The applicant shall be issued a fresh certificate as in initial certification in lieu of the current certificate as and when the candidate applies and successfully completes the certification process.

4.9 The Certificate

- 4.9.1 The PrCB shall provide a certification document to the certified cyber security professional that clearly conveys, or permits identification of:
 - a. the name of the person who has been certified;
 - b. the dates of granting, or renewing certification;
 - c. the effective date of certification;
 - d. the expiry date or recertification due date consistent with the recertification cycle;



- e. a unique identification code certification title and code;
- f. language of examination;
- g. cell phone number;
- h. including issued number and/or revision, against which the person has been certified;
- i. the level of certification;
- j. the name and address of the certification body;
- k. other marks (e.g., certification mark, accreditation symbol) may be used provided they are not misleading or ambiguous;
- l. any other information required by the competence criteria used for certification;
- m. in the event of issuing any revised certification documents, a means to distinguish the revised documents from any prior obsolete documents.

4.9.2 The PrCB shall issue certificates to successful candidates in their legal name.

4.9.3 Candidates who legally change their name must notify the certification office in writing. Name change requests should be mailed to the certification office. Please note that a notarized copy of official or certified documentation supporting the request (e.g., a notarized copy of a marriage certificate) must be included with the request. Requests received without official documentation shall not be processed.

4.9.4 The effective date on a certification document shall not be before the date of the certification/recertification decision.

4.9.5 The formal certification documentation shall include the signature of the individual(s) of the PrCB assigned such responsibility. This could be either digital or physical depending on the resources available.

4.10 Duplicate or Replacement Certificates

4.10.1 Individual duplicate or replacement certificates can be issued by PrCB. Duplicates/replacements shall only be issued to original certificate holder. Any change of address must be requested in writing from the certificate holder.

4.10.2 The effective date on a certification document shall not be before the date of the certification/recertification decision. The formal certification documentation shall include the signature of the individual(s) of the PrCB assigned such responsibility.

4.10.3 The certified persons should be encouraged to use only the original certificates issued by the PrCB for all purposes. The certified persons may apply for additional original copies of the certificate and the PrCB shall provide additional copies for a fee.

4.11 Extensions Due to Extenuating Circumstances

4.11.1 In cases where certified personnel, due to extenuating circumstances, cannot obtain the renewal by the required renewal date, a request for an extension should be sent in writing to the PrCB. The PrCB can grant up to 120 days of extension for the renewal requirements when:



- a. The extension request is in writing and is based upon extenuating circumstances;
- b. The extension request includes a written plan as to how the individual will obtain the missing renewal requirements within the mandated 120 days extension period.

4.11.2 If the renewal requirements are met during the extension period, the date of next renewal will continue to be the original date of renewal. Extenuating circumstances would include conditions such as active government duty, extended illness, or limited availability of renewal requirements in a particular area.

5. Appeals

- 5.1 Requests for an appeal in the case of a denied renewal must be made to the PrCB not later than 30 days after the notification to the applicant of the denied renewal.
- 5.2 Appeals shall be reviewed by PrCB to determine if the appeal is a valid appeal. Should the appeal be found invalid, the PrCB shall notify the candidate of the reason(s) the appeal is not valid.
- 5.3 The PrCB shall also notify the candidate if additional information is needed, or if the appeal is being forwarded to the decision-making authority for review. However, the PrCB shall ensure that the decision making personnel on appeal handling process is different from those involved in the decision being appealed.
- 5.4 Within 90 days of the receipt of the written appeal, the PrCB shall communicate its decision to the appellant.

6. Revision to the Scheme

Whenever the certification scheme is revised, the PrCB shall inform the applicants, candidates and certified persons, in a clear manner, the process to be followed by them to comply with the provisions of the revised scheme.

7. Fee Structure

The PrCB shall abide by the commercials as applicable.



SECTION 5

REQUIREMENTS FOR CERTIFICATION BODIES FOR PERSONS (PrCBs)



1. **Scope**

This document describes the requirements for Certification Bodies operating the Certification Scheme for cyber security professionals (also referred to as 'the Scheme'), and also specifies cyber security professionals Scheme specific additional requirements.

2. **Objectives**

- 2.4 The objective of this section is to ensure that different PrCBs operate in a harmonized way by standardising the Requirements for PrCBs. This document along with Conformity Assessment Process for PrCBs will ensure that certified professionals from different PrCBs have equivalent level of knowledge and skill set.
- 2.5 The requirements described in this document are based on ISO/IEC 17024:2012 needs to be complied with by the PrCBs.
- 2.6 The PrCBs desirous of cyber security professional Certification under the Scheme, shall meet the criteria as prescribed in clauses 3 and 4 of this document.

3. **Administrative Requirements**

3.1 **Legal Entity**

- 3.1.1 The Certification Bodies which are part of government, or are government departments, shall be deemed to be legal entities on the basis of their governmental status. The status and structure of such bodies shall be formally documented, and the bodies shall comply with all the requirements of this document.
- 3.1.2 The accreditation shall be granted to a legal entity, who can be legally held responsible for its work, irrespective of whether the entire organization or a part of it, performs the certification functions.
- 3.1.3 The PrCB shall be responsible for and shall retain authority for its decisions relating to certification. This includes the granting, maintaining, renewing, extending, reducing, suspending and withdrawing of certification.

3.2 **Organizational Structure**

The PrCB shall define and document the duties, responsibilities and reporting structure of its personnel and any committee and its place within the organization. When the certification body is a defined part of a legal entity, documentation of the organizational structure shall include the line of authority and the relationship to other parts within the same legal entity.

3.3 **Integrity**

The PrCB and its personnel shall maintain integrity at all times. The PrCB shall implement adequate measures to ensure integrity.

3.4 **Impartiality**

- 3.4.1 The PrCB shall be impartial.
- 3.4.2 The PrCB shall be so structured and managed as to safeguard impartiality.



- 3.4.3 The PrCB and its personnel shall not engage in any activities that may conflict with their Impartiality.
- 3.4.4 The PrCB shall act impartially in relation to its applicants, candidates and certified persons.
- 3.4.5 The PrCB shall have a process to identify, analyze, evaluate, monitor, and document the threats to impartiality arising from its activities, including any conflicts arising from its relationships on an ongoing basis.
- a. This shall include those threats that may arise from its activities, or from its relationships, or from the relationships of its personnel. Whenever there are threats to impartiality, the PrCB shall document and demonstrate how it eliminates or minimizes such threats and document any residual risk. The demonstration shall cover all potential threats that are identified whether they arise from within the PrCB or from the activities of other persons, bodies or organizations.
 - b. Top management shall review any residual risk to determine if it is within the level of acceptable risk. Whenever a relationship poses an unacceptable threat to impartiality, then certification shall not be provided.
 - c. The risk assessment process shall include identification of and consultation with the appropriate interested parties, to advice on matters affecting impartiality including openness and public perception.

NOTE 1: Sources of threats to impartiality of the PrCB can be based on ownership, governance, management, personnel, shared resources, finances, contracts, training, marketing and payment of a sales commission or other inducement for the referral of new clients, etc.

NOTE 2: One way of fulfilling the consultation with the interested parties is by the use of an impartiality committee.

- 3.4.6 The PrCB shall not impart education and/or training in Cyber security domain within the same legal entity.
- 3.4.7 The PrCB shall have a process to eliminate or minimize risk to impartiality, if training/education of IT/ICS cyber security professional is carried out in a related body, which is linked to the PrCB by common ownership etc.
- 3.4.8 The PrCB shall have a process to ensure that the examiner is free of any conflict of interest with the candidate(s) by means of being an Instructor in the recent past. A separation of 2 years is considered acceptable for the purpose.
- 3.4.9 The PrCB policies and procedures shall ensure that it does not practice any form of hidden discrimination by speeding up or delaying the processing of applications.

3.5 Confidentiality

- 3.5.1 The PrCB shall ensure confidentiality of information obtained in the course of its certification activities by having a suitable system.
- 3.5.2 The PrCB Personnel, including any committee members, contractors, personnel of external bodies or individuals acting on the Certification Body's behalf, shall keep



confidential all information obtained or created during the performance of the Certification Body's activities. There shall be a mechanism such as obtaining signed confidentiality agreements, etc. for ensuring the same.

- 3.5.3 The PrCB shall use equipment, hardware, software and facilities that ensure the secure handling of confidential information (e.g. documents, records).
- 3.5.4 Whenever a confidential information is made available to other bodies (e.g., AB, agreement group of a peer assessment scheme), the PrCB shall inform its client of this action, in advance, through agreements, etc.
- 3.5.5 In case of transfer of certificate or application, if the client decides to move from one PrCB to another PrCB, the PrCB to which the client is now moving may ask the previous PrCB for information on the reasons for such movement, or the performance of the IT and ICS professional with respect to the certification requirements. The previous Certification Body shall be obliged to share this information within a reasonable time, not exceeding 15 days from the date of receipt of the request. Such information shall not be considered as confidential and the PrCB shall inform its client of this requirement, in advance, through agreements.

3.6 **Liability and Financing**

- 3.6.1 The PrCB shall also be able to demonstrate that it has evaluated the risks arising from its certification activities and that it has adequate arrangements (e.g., insurance or reserves) to cover liabilities arising from its operations in each of its fields of activities and the geographic areas in which it operates.
- 3.6.2 The PrCB shall demonstrate that it has a reasonable expectation of being able to provide and continue to provide the service in accordance with its contractual obligations. The PrCBs shall also be able to provide sufficient evidence to demonstrate its viability, e.g., management reports or minutes, annual reports, financial audit reports, financial plans, etc.
- 3.6.3 The means by which the PrCB obtains financial support should be such which allows the Certification Body to retain its impartiality.
- 3.6.4 In addition to the above, the PrCB shall also demonstrate initially and/or on an ongoing basis, that commercial, financial or other pressures do not compromise its impartiality.

4. **Technical Requirements**

4.1 **Personnel**

- 4.1.1 The PrCB shall have, as part of its own organization, personnel either employed or on contract, having sufficient competence for managing process of certification of cyber security professionals.
- 4.1.2 The PrCB shall have defined processes for selecting, training, and formally qualifying Scheme Manager, Examiners/ Interviewers, Exam Paper Setters, Invigilators and Decision Maker used in this activity (refer Annex A of this section).

4.2 **Competence**

- 4.2.1 The examiners used by the PrCBs shall have the following qualifications and experience:



- a. Any certified cyber security professional under this Scheme can be used as examiner for one level lower certification of the respective domain.
- b. The PrCB shall have a process of qualifying the examiners by a more senior professional of cyber security domain.
- c. The PrCB shall nominate a scheme manager for the management of (a) and (b).

4.2.2 Competence of Examiner of PrCB may be referred at Annex A of this section.

4.2.3 For any exemption from these requirements, the PrCBs shall approach the scheme manager.

5. **Other Resources**

5.1 The PrCB shall ensure adequate arrangements in the premises such as examination sites, computers and networks with IT security, power backup, ventilation, lighting and appropriate resources, e.g. for recording and storage of examination records.

5.2 The examination activity shall be recorded and the record retention time shall be a minimum of one complete cycle of certification (3 years). There shall also be a facility to watch the examination administration at the centre from remote location. The facility for remote monitoring shall be provided to the Scheme Manager the PrCB shall develop a procedure on the requirements for the individual test centres either under their direct or indirect control of the PrCB.

6. **Certification Process**

6.1 The PrCB shall manage the process of certifying cyber security professionals as per the documented 'Certification Process' prescribed under the Scheme.

6.2 The PrCB shall maintain records to demonstrate that the certification process is effectively implemented.

6.3 The PrCB shall ensure the requirements of the Scheme are met with, at every point in time. The PrCB shall certify cyber security professionals only under this Scheme and shall use the logo of the Scheme in the certificates issued to the certified cyber security professionals.

6.4 The PrCB shall have a written agreement along with the Code of Ethics and Conduct, with the certified persons on the use of the cyber security professional certificate.

6.5 The PrCB shall have a process to handle appeals by the candidates, against any of its decisions.

6.6 The PrCB shall have a process to handle complaints from users of the services of the certified cyber security professionals, or any other interested parties.

6.7 The PrCB shall comply with all the requirements as specified in "Certification Process for Certification of cyber security professionals".

7. **Publicly Available Information**

7.1 The PrCB shall maintain a website for providing information about the Scheme, and its certification activities under the Scheme.



- 7.2 The following information, with respect to personnel certification scheme, shall be made publicly available on the CB's website. The information provided shall be accurate, non-misleading and where relevant detailed enough for the reader to clearly understand.
- 7.2.1 The certification process, from application stage to the grant of certification, includes the assessment and examination process; the system for maintenance of certification, renewal, scope extension and reduction, suspension and withdrawal. The information shall also cover the terms and conditions of certification and the use of Certification Mark, as contained in the Certification Agreement.
- 7.2.2 Scheme specific rules and conditions for granting, maintaining, extending or reducing the scope of, suspending, withdrawing or refusing certification.
- 7.2.3 Requirements of cyber security professional Certification Scheme, including the cyber security professional certification criteria and application form, shall be available to the applicant. The PrCB may also provide any other guidance documents on the certification criteria for the benefit of the applicant, as long as they are not advisory/consultative in nature.
- 7.2.4 The PrCB shall make publicly available on its website, the information about applications registered and certifications granted, suspended or withdrawn.
- 7.2.5 On request from any party, the PrCB shall provide the means to confirm the validity of a given certification, and the provision for the same shall be made available on the website.
- 7.2.6 The PrCB shall maintain and make publicly available on its website, a directory of valid certifications.
- 7.2.7 A description of the rights and duties of applicants and certified professionals, including requirements, restrictions or limitations on the use of the PrCB's name and Certification Mark, and on the ways of referring to the certification granted.
- 7.2.8 In cyber security professional Scheme, the PrCB shall make publicly available its processes for handling appeals and complaints.
- 7.3 The PrCB shall have a procedure for updating of the information on its website. Any new updates received by the PrCB shall be updated within three working days of the event.
- 7.4 The PrCB shall list out the sources of its finances, especially if the PrCB is not listed as a company.
8. **Extraordinary Conditions or Local Emergencies**
- 8.1 In the events of hazardous weather, pandemic, or any other unforeseen emergencies, occurring on the day of an exam, the PrCB shall determine in such circumstances whether the cancellation of examination/assessment is required.
- 8.2 Every attempt shall be made to administer all exams as scheduled. The PrCB must have an incident management procedure to handle such situations.
9. **Safety and Security**



- 9.1 All exam materials shall be the property of PrCB, Scheme Owner or Scheme Manager. Removal of any material from the exam room by an unauthorized person, shall be prohibited.
- 9.2 The PrCB shall have defined policies and procedures for implementation of safety requirements for its operations, including applicable legal requirements, i.e., Fire NOC (No Objection Certificate), Lift permission etc.
- 9.3 The PrCB shall be responsible for providing secure systems, for conduct of examination and shall adhere to Information Security Management procedures and methods, defined by the PrCB.
- 9.4 The PrCB shall be responsible for guarding the Systems against virus, malware, spyware and spam infections using the latest Antivirus corporate/Enterprise edition suites, which include anti-malware, anti-spyware and anti-spam solution for the entire system. The PrCB shall maintain strict privacy and confidentiality of all the data it gets access to.
- 9.5 The PrCB shall provide the infrastructure required for conducting examination like the space, webcam in the centre, computers, servers, UPS, generators, LAN/WAN of required speed, routers, Network Management, Firewalls and proxy servers, internet connectivity (with required emergency backups) etc., as required by procedures of the PrCB.
- 9.6 The PrCB shall ensure data security, retain any data and/or records specified in the procedure, and transfer data relating to Candidate data files, Invigilator reports, and any other test-related files in a secure manner and in conformance with the PrCB procedures.
- 9.7 If invigilation through physical presence is not possible or desirable, Audio and Visual monitoring of candidates shall be carried out through a window, glass panel or via a video monitor. However, this shall be carried out only under the direction of the PrCB.
10. **Address, Name or Contact Information Changes**
 - 10.1 The Candidates and subsequent certified individuals, who have a change in their name, mailing address or contact information, must notify the PrCB in writing to ensure that all records, assessment reports and certificates are sent to their correct address, and are received in a timely manner.
 - 10.2 The PrCB shall verify applicable legal documents for any change in name of the candidate or certified professional, i.e., updated aadhaar card, driving license etc..
 - 10.3 The PrCB shall retain the copy of applicable documents for at least current and previous certification cycle and as per legal or contractual requirements.
 - 10.4 The PrCB shall share formal feedback/suggestions received on scheme requirements and implementation to QCI, as received from relevant interested parties.



Annexure A

Competence Requirements for Personnel Involved in Certification Process

1. Scheme Manager

S. No	Educational Qualification (recognised Institutes / University)	Total Experience in IT/ICS/Cybersecurity (including Professional experience + Consultancy experience) (A+B)	Training
1	Masters (recognised degree) OR	NA	16 hours training on the technical aspects of personnel certification scheme
2	Graduation or PG Diploma (recognised) OR	1 years	16 hours training on the technical aspects of personnel certification scheme
3	Diploma (recognised)	2 years	16 hours training on the technical aspects of the scheme

2. Exam Paper Setter

S. No	Educational Qualification (recognised Institutes/ University)	Total Experience in IT/ICS/Cybersecurity (including Professional experience, training, auditing consultancy)	Training
1	Masters (recognised degree) OR	10 years	24 hours training on personnel certification scheme (including psychometric techniques)
2	Graduation/ PG Diploma (recognised)	15 years	24 hours training on personnel certification scheme (including psychometric techniques)

3. Examiner(s)/ Interviewers:

S. No	Educational Qualification (recognised Institutes / University)	Total Experience in IT/ ICS Cyber security (including Professional experience, training, auditing consultancy)	Training
1	PhD. (Doctorate) OR	5 years	Knowledge of personnel certification scheme
2	Masters (recognised degree) OR	10 years	24 hours training on personnel certification scheme
3	Graduation/ PG Diploma (recognised)	12 years	24 hours training on personnel certification scheme



4. Invigilator(s):

S. No	Educational Qualification (recognised Institutes / University)	Total Experience in IT/ICS/Cybersecurity (including Professional experience + Consultancy experience) (A+B)	Training
1	Graduation	NA	8 hours training on proctoring physical or online exam.
2	Diploma (recognised)	5 years	8 hours training on personnel certification scheme

5. Decision Maker

S. No	Educational Qualification (recognised Institutes / University)	Total Experience in IT/ICS/Cybersecurity (including Professional experience + Consultancy experience) (A+B)	Training
1	Masters (recognised degree) OR	10 years	16 hours training on personnel certification scheme
2	Graduation/ PG Diploma (recognised) OR	12 years	16 hours training on personnel certification scheme
3	Diploma (recognised)	15 years	16 hours training on personnel certification scheme



SECTION 6

PROVISIONAL APPROVAL SYSTEM



1. Introduction

1.1 The conformity assessment framework for cyber security of critical sector entities has three provisions for conformity assessment bodies, which are:

1.1.1 Certification Bodies for Audit and Certification of CSMS of Critical Sector Entities.

1.1.2 Personnel Certification Bodies for certifying cyber security professionals.

1.1.3 Inspection Bodies for examining cyber security architecture and infrastructure.

1.2 The scheme for Certification of Persons (PrCBs) aims to attest cyber security professionals for their knowledge and skill in a particular domain.

1.3 The certification of personnel is operated by various bodies, operating certification of personnel scheme (herein referred as PrCBs) and seeking accreditation from NABCB to demonstrate their capabilities in this area or any other Accreditation Board that is a member of IAF having scope 'Cybersecurity'.

1.4 The PrCBs, in order to operate under the scheme, shall need to primarily comply with the requirements specified by the Accreditation Board (ABs) and the additional requirements prescribed in the Scheme.

1.5 In order to get accredited, a new PrCB is required to present at least two certified clients to the AB. This is required to demonstrate the capability and stability of operations, for assessing and managing the complete cycle of operations, including decision making.

1.6 To meet this requirement for acquiring accreditation, the PrCBs need to identify two clients that allow themselves to go through the process of certification.

1.7 Initially, the PrCBs that are yet to undergo an accreditation process for establishing their credibility, will not be preferred by cyber security professionals. This will discourage new PrCB entrants, such as Start-Ups, MSMEs etc. Hence, such PrCBs would not get applicants to offer as test cases to complete their accreditation process of witnessing.

1.8 Further, to launch the Scheme, it is necessary that some PrCBs are available at the initial phase to provide a basic level of credibility and boost their confidence.

1.9 Therefore, it is necessary to establish a procedure for the Provisional Approval of PrCBs under the Scheme, till their scope is validated and added in their accreditation or acquire formal accreditation from an Accreditation Board (AB), that is signatory to the International Accreditation Forum (IAF).

1.10 This document details out the requirements needed to be fulfilled by the PrCBs, desirous of operating under the Scheme and with pending status of their formal accreditation.

In order to acquire formal accreditation by an AB, the PrCBs would need to undergo two brief assessments, viz., Office Assessment and Witness Assessment, for an actual evaluation under the Scheme.



2. **Scope**

- 2.1 This document defines the process followed by a PrCB(s) for obtaining provisional approval in order to operate under the Scheme, or with pending formal accreditation for the Scheme, by the respective AB.
- 2.2 This approval holds validity for a period of one year, preferably within which the approved PrCB should obtain formal accreditation. The extension for provisional approval may be done as per the merit of the case, as considered by QCI.

3. **Criteria for Approval**

The PrCB(s) desirous of operating under this Scheme, shall be required to meet the criteria as prescribed in clauses 4 and 5 of this document.

4. **Administrative Requirements**

- 4.1 **Legal Entity:** The PrCB(s) shall be a legal entity or defined part of the same, such that it can be legally held responsible for all the conformity assessment activities undertaken by it. A governmental PrCB(s) is deemed to be a legal entity based on its governmental status. A PrCB(s), that is part of an organization involved in functions other than certification, shall be held separate and identifiable within that organization.
- 4.2 **Organizational Structure:** The PrCB(s) shall define and document the duties, responsibilities and reporting structure of its personnel and/or committees, and also declare its placement within the organization. If the PrCB is held as a defined part of a legal entity, documentation of the organizational structure shall include the line of authority and its relationship to others parts of the same legal entity.
- 4.3 **Integrity:** The PrCB(s) and its personnel shall maintain the integrity of the scheme at all times. The PrCB shall take adequate measures to ensure integrity is sustained.
- 4.4 **Impartiality:**
 - 4.4.1 The PrCB shall act impartially.
 - 4.4.2 The PrCB shall be structured and managed so as to safeguard impartiality.
 - 4.4.3 The PrCB and its personnel/staff shall not engage in any activity(s) that may be in conflict with impartiality.
 - 4.4.4 The PrCB shall require personnel involved in the certification process to sign a contract or other document(s) through which they shall commit and declare any prior and/or present association(s), on their own part or on the part of their employer.
 - 4.4.5 The PrCB and/or any other part of the same legal entity(s) shall not, under its organizational control:
 - a. be the designer, manufacturer, installer, distributor or maintainer of the attested activity(s);



b. offer or provide management system consultancy or internally provide audits to its clients, wherever the scheme requires an evaluation of the client's management system.

4.4.6 The PrCB shall ensure that the activities of discrete legal entities, with which the PrCB or the part of same legal entity has relationships, does not compromise the impartiality of the certified activities.

4.4.7 If discrete legal entity(s) offers conformity assessment services, the PrCBs' management personnel and personnel in the review and certification decision making process, shall not be involved in the activities of the separate legal entity..

4.4.8 The PrCB shall act impartially w.r.t. its applicants and the certified clients.

4.4.9 The PrCB shall establish and implement a documented procedure for analysing the threats against impartial conduct of the PrCB. The analysis shall be based on all potential sources which may arise during the PrCBs' activities (its own, of the related bodies and/or of employed personnel) and from its associated relationships (individuals/organizational).

4.4.10 The PrCB shall ensure that the conflict-of-interest analysis is carried out at least once a year, and whenever a significant change occurs in the PrCB's activities, such as changes in the organizational structure and business activities, or of the legal status and mergers with, or acquisitions of other organizations.

Note 1: A relationship that threatens the impartiality of the PrCB can be based on ownership, governance, management, personnel, shared resources, finances, contracts, marketing and payment of a sales commission or other inducement for the referral of new clients, etc.

Note 2: While carrying out the conflict-of-interest analysis the following risks, but is not limited to them, shall be considered:

- a. Self-interest threats: threats that arise from a person or body acting in their own interest. A concern related to certification, as a threat to impartiality, is financial self-interest.
- b. Self-review threats: threats that arise from a person or body reviewing the work done by themselves. The certification of a client whose product was designed, or who was provided service regarding internal evaluation by the PrCB or the personnel it employs, would be a self-review threat.
- c. Familiarity (or trust) threats: threats that arise from a person or body being too familiar with or trusting of another person, instead of seeking evaluation evidence. Repeat evaluation of a client by the same evaluator/auditor, over and over again may also present as a familiarity threat.
- d. Intimidation threats: threats that arise from a person or body having a perception of being coerced openly or secretly, such a threat to be replaced or reported to a supervisor.



- 4.4.11 If a relationship poses an unacceptable threat to impartiality, then certification shall not be provided. Some of these situations requiring prohibitions as mitigation measures have been described vide relevant clauses of the guidance standard. These shall be implemented together with the additional measure provided in this document.
- 4.4.12 Further, wherever risks to impartiality have been identified as a result of risk analysis (clause 4.4.9), the PrCB shall establish and implement a documented procedure for mitigation of threats against impartiality. These shall be through any of the following means of mitigation:
- The PrCB shall not use personnel for evaluation purposes if they have been employed by or are involved in consultancy / training work with the client, for a minimum of two years post the culmination of the employment / consultancy/ training work;
 - The PrCB shall not have any relationship with its clients other than that of a third party conformity assessment personnel;
 - The PrCB shall not impart education and/or training within the same legal entity;
 - The PrCB shall have a process to eliminate or minimize risks to impartiality whenever training /educational work is carried out in a related body which is linked to the PrCB by common ownership etc.

5. Liability and Financing

- 5.1 The PrCB shall evaluate its finances and sources of income, and demonstrate that initially and on an ongoing basis, impartiality is not compromised irrespective of commercial, financial or other pressures
- 5.2 The PrCB shall be able to demonstrate that it has evaluated the risks arising from its Certification/Inspection activities, and that it has adequate arrangements (e.g. insurance or reserves) to cover liabilities arising from its operations, for each of its fields of activities and the geographic areas it operates.

6. Publicly Available Information

- 6.1 The PrCB shall maintain a website for providing information about the Scheme and for its certification activities under the Scheme.
- 6.2 The PrCB shall maintain and make publicly available, the information describing its certification processes for granting, maintaining, extending, renewing, reducing, suspending or withdrawing Certification, and about the certification activities and geographical areas in which it operates.
- 6.3 The PrCB shall make publicly available the information about applications registered and Certifications granted, suspended or withdrawn.
- 6.4 The PrCB shall make publicly available its process for handling appeals and complaints.
- 6.5 Confidentiality: The PrCB shall ensure confidentiality of information, obtained in the course of its certification activities, through maintenance of a suitable system.



6.6 **Certification Agreement:** The PrCB shall have a legally enforceable agreement for the provision of certification activities to its client. In addition, the PrCB shall ensure its certification agreement requires the client to comply at least, with the specific requirements as prescribed in the relevant international standards and with the Scheme document.

6.7 **Responsibility for Decision on Certification:** The PrCB shall be responsible for, shall retain authority for, and shall not delegate, its decisions relating to issuance of statement of conformity, including the granting, maintaining, recertifying, expanding and reducing the scope of the Certification.

7. **Technical Requirements:** as mentioned in Requirements for PrCBs

8. **Personnel Records**

The PrCBs shall maintain up-to-date records, as per requirements of the Scheme document, of personnel involved in its consultancy/training activities.

9. **Conformity Assessment Process**

9.1 The PrCB shall manage the process of conformity assessment as per the document 'Certification Process' prescribed under the Scheme.

9.2 The PrCB shall maintain records to demonstrate that the certification process is effectively fulfilled.

9.3 The PrCB shall ensure the requirements of the Scheme are met at all times. The main difference between provisional approval and accreditation is that provisional approval compliances are looked at 'in-principle' level implementation (broad implementation with clear intent) of all the requirements, whereas during the time of accreditation 'audit in depth' process is followed. Irrespective of the status of approval, the process of certification of personnel adopted by the PrCB has the same level of rigor.

9.4 The PrCB shall certify only under the Scheme and shall use the logo of the Scheme in the letters issued to the manufacturer as per Section 7: Rules for the Use of Scheme Mark.

9.5 The PrCB shall make provision for the signing of an agreement with QCI in the prescribed format on the use of the Scheme / Certification Mark.

9.6 The PrCB shall have a process to handle appeals by the clients, against any of the PrCBs decision(s).

9.7 The PrCB shall have a process to handle complaints from the users of the services, of the PrCB or any other stake holder.

10. **Approval Process**

10.1 Application



- 10.1.1 Any organization interested in approval as a PrCB for the purpose of this Scheme may apply to QCI in the prescribed application format, along with the prescribed application fee. The applicant shall also enclose the required information and documents as specified in the application form.
- 10.1.2 The filled in application form for approval shall be duly signed by the CEO/authorized representative(s) of the organization seeking approval.
- 10.1.3 On receipt of the application form, it shall be scrutinised by the QCI, and those found complete in all respects will be processed further.

11. **Assessment Process**

- 11.1. On review of the application for completeness, an assessment team comprising a team leader and member(s)/technical expert(s) will be nominated by QCI, for the purpose of assessment at applicant's office and other locations, if required. Under normal circumstances, the assessment at Head Office will be for a total of two-man days. However, if the organization is already accredited to relevant ISO, the duration may be reduced.
- 11.2. The names of the members of the assessment team along with their CVs will be communicated to the applicant organization, giving it adequate time to raise any objection against the appointment of any of the team members, which will be dealt with by QCI on merits. All assessors/experts nominated by QCI shall have signed under takings regarding confidentiality and conflict of interest.
- 11.3. If necessary, QCI may decide based on the report of Office Assessment (OA) or otherwise, to undertake witness assessment(s) of actual evaluation or any part of the certification process by the applicant.
- 11.4. The assessment team leader shall provide an assessment plan to the applicant in advance of the assessment.
- 11.5. The date(s) of assessment shall be mutually agreed upon between the applicant and QCI assessment team.
- 11.6. The Office Assessment will begin with an opening meeting for explaining the purpose and scope of assessment, and the methodology of the assessment. The actual assessment process shall cover review of the documented system of the organization, to assess its adequacy in line with the assessment criteria as specified. It will also involve verification of the implementation of the system, including scrutiny of the records of personnel competence and other relevant records, and the demonstration of personnel competence through means like interviews, etc. In short, it will be an assessment for verifying technical competence of the applicant for operating under the Scheme.



- 11.7. At the end of the Office Assessment, through a formal closing meeting, all the non-conformities and concerns observed in the applicant's system as per the assessment criteria, and the assessment team's recommendation to QCI, shall be conveyed to the applicant.
- 11.8. Based on the report of assessment, and the action(s) taken by the applicant on the non-conformities/concerns, if any, QCI shall take a decision on whether to:
- 11.9. Under take Witness Assessments(s) (WA) of actual evaluation or any part of the certification process by the applicant prior to granting of provisional approval, or;
- 11.10. Granting provisional approval to the applicant as PrCB under the Scheme.

12. **Validity of Approval**

- 12.1 The approval shall be valid for a period of one year preferably.
- 12.2 The validity of the certificate issued by provisionally approved PrCB to certified candidates will be 3 years irrespective of whether they are provisionally approved or accredited.
- 12.3 During the validity of approval, QCI shall undertake at least one Witness Assessment to confirm the PrCB's competence. This may be waived if the organization is able to provide a Witness Assessment report from AB.
- 12.4 The PrCB shall obtain formal accreditation from an IAF accredited AB within one year of approval by QCI.
- 12.5 Based on the request of the PrCB and review of previous performance, it may be decided to extend the period of validity; in such a case, the PrCB shall be assessed covering both office and witnessing on-site, as decided by QCI, prior to such an extension.
- 12.6 The approval shall be subject to suspension/withdrawal with due notice of 15 days in the event of any non-compliance to the requirements of the Scheme.
- 12.7 The approved PrCB shall inform QCI without delay about any changes relevant to its approval, in any aspect of its status or operation relating to:
 - 12.7.1 Its legal, commercial, ownership or organizational status;
 - 12.7.2 The organization, top management and key personnel;
 - 12.7.3 Main policies, resources, premises and scope of approval, and;



12.7.4 Other such matters that may affect the ability of the PrCB to fulfil the requirements for approval.

12.7. QCI shall examine such information and decide on the issue on merits, with or without an on-site verification.

13. **Fee Structure**

The PrCB shall abide by the commercials as applicable.



SECTION 7

RULES FOR USE OF SCHEME MARK



1. Introduction

- 1.1 The Conformity Assessment Framework (CAF) for personnel certification comprises of PrCB on the lines of ISO/IEC:17024:2012.
- 1.2 The 'Scheme Mark' denotes the Mark that is assigned to the approved PrCBs.
- 1.3 The Mark is allowed to be used by certified personnel for the purposes of promotion and to display the mark in off- product(s), as prescribed in rules mentioned in the subsequent paras of this document.
- 1.4 Further, it is the collective responsibility of the NCIIPC, QCI and its constituent accreditation boards to keep an oversight on the use of Mark.
- 1.5 In turn the approved CABs will ensure that the entities who are offered conformity assessment services shall follow the rules for use of Certification Mark.

2. Purpose

The QCI and its constituent accredited organizations, and in the case of conformity assessment bodies, their attested clients, can benefit through visual identification of their status through the use of Scheme Mark. In doing so, the Mark Holders are provided guidance that shall include both individuals and organizations, for the purpose of displaying the Mark that 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 section is to establish rules for use of the Scheme Mark.
- 3.2 This document sets out the conditions that must be followed by PrCBs and certified cyber security professionals that are permitted to use the logo or symbols.
- 3.3 This document establishes the process to be adopted by the Scheme Manager for the grant of use of Scheme Mark to PrCBs and certified cyber security professionals.

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 scope of misuse with respect to Scheme requirements.

5. Prerequisites for Use of Scheme Mark

- 5.1 Organizations as Entities
 - 5.1.1 The Mark Holders approved under the Scheme are eligible to use Scheme Mark. They are required to submit an application to acquire authorisation for the Use of Certification Mark (refer Annex A of this section).



5.1.2 As per the contract between the Scheme Manager and the Mark Holder, the later shall be required to enter into a formal agreement with QCI for the use of Scheme Mark. This shall immediately follow after the grant of approval.

5.1.3 The PrCBs and certified cyber security professionals shall make provisions in their management system in order to institutionalise this requirement and be legally enforceable.

5.2 Individuals as Entities (cyber security professionals)

5.2.1 The cyber security professionals require a grant of certification for the requisite competence (ies) as stipulated by the PrCB and through established processes as mentioned in the Scheme.

5.2.2 The cyber security professionals are required to enter into a written agreement with the PrCB and shall be required to formally sign an agreement (refer Annex B of this section) with QCI for the use of Scheme Mark. This shall immediately follow after the grant of approval.

6. Oversight Responsibility

6.1 The QCI secretariat shall be held responsible to establish, implement and amend this procedure. The Mark Holder(s) is responsible to comply with the procedure, specifically to undertake surveillance or re-certification assessment. This shall be done with the oversight of NCIIPC.

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

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

7. Rules for Use of Scheme Mark

7.1 The Mark Holder requires total compliance with respect to the applicable criterias.

7.2 The Scheme Mark is allowed to be used only by approved conformity assessment bodies.

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

7.4 A Mark Holder subjected to important changes or overhauls and aiming to modify its original mandate post his/her secured approval, must apply de novo.

7.5 The Scheme Mark may be used in cases of any photographic reduction or enlargement and still hold it's validly. The colours of the Scheme Marks should remain the same as described below. Alternate colours for the same shall not be held valid.

7.6 For cases of photographic reduction and enlargement, sufficient care should be exercised to ensure that there is deviation in the aspect ratio and colour degradation/change.



- 7.7 The Mark Holder, upon suspension or withdrawal of its attestation, shall discontinue the use of Scheme Mark, in any form.
- 7.8 The Mark Holder, upon suspension or withdrawal of its attestation, shall discontinue the use of all advertising material with any reference to its attestation status.
- 7.9 In case the Scheme Mark is observed to be used in contravention to the specified conditions by a Mark Holder, suitable action(s) shall be taken by the approving body in accordance with the relevant requirements of Scheme, and with those specified in the documents “Scheme Attestation (Certification) Process” and “Requirements for Conformity Assessment Bodies”.
- 7.10 Depending upon the degree of violation, the 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(s) to address the wrong usage of the Scheme Mark, the conformity assessment body may suspend/withdraw their certification.
- 7.11 In case a Mark Holder’s certification is suspended; its attestation is cancelled, withdrawn or discontinued, it is the Mark Holder’s duty to discontinue the use of the Scheme Mark post the dated expiry from which the certificate stands suspended, cancelled, and withdrawn or discontinued. The conformity assessment bodies/QCI that have approved the Mark Holders needs to ensure compliance as stated above.
- 7.12 The Mark Holders shall sign a legally enforceable agreement with the Scheme Manager, QCI whereby it allows the use of Scheme Mark, after due compliance with the relevant conditions as described in Annex B of this section.
- 7.13 The Mark Holders shall be liable for an annual fee payment to QCI, through their operational entities for using the Scheme Mark, as prescribed from time to time. This payment shall be made to its approving Mark Holder for onward submission to QCI.
- 7.14 **Misuse scenarios:**
- 7.14.1 The Mark should not be used while making statement(s) related to out-of-scope entities.
- 7.14.2 The usage of NCIIPC’s, QCI’s and its constituent boards’ logos/Marks by the Mark Holder are not permitted. If required for temporary events such as collaborative training programs, etc. written permission needs to be sought from the respective organization.
- 7.14.3 The Mark Holder shall desist from misleading anyone; avoid positioning of incompatible marks that may devalue or degrade other Marks; use them illegally (they are protected trademarks); or use them in contravention to the recognised Scheme.
- 8. Conditions for use of Scheme Mark by Mark Holder Organizations (PrCBs)**
- Following conditions shall apply for use of Scheme Mark:
- 8.1 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.



8.2 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.

8.3 The Mark Holder shall not make any misleading claims with respect to the Scheme Mark.

8.4 The use of the Scheme Mark shall not be done in such a manner which brings disrepute to the Scheme Owner (NCIIPC) and Scheme Manager (QCI).

9. Conditions for Use of the Scheme Mark by Individuals (Cyber Security Professionals)

9.1 The Scheme Mark will only be displayed on the competency profile certificate(s) issued by a PrCB. The cyber security professionals will not use or display the Scheme Mark anywhere else.

9.2 Once certified, the cyber security professional shall abide by all clauses mentioned in Annex B) of this section, committing to the requirement of the Scheme through their approved PrCB.

9.3 Once the Mark Holder is certified by the QCI or QCI approved conformity assessment bodies, it shall require the cyber security professional to fill a duplicate contractual form / template, enclosed in Annex A of this section.

9.4 The PrCBs shall forward the filled contract form received from the certified cyber security professionals to QCI, for the purpose of signing and completing the contractual formalities. Along with the contract form, the relevant conformity assessment body shall also forward the details of the Mark Holder, covering the following information (as a minimum):

9.4.1 Name and address of the Mark Holder;

9.4.2 Legal entity Status (with evidence);

9.4.3 Names of the top management/ownership details;

9.4.4 Details of the Certification granted—number, validity etc.;

9.4.5 Scope of certification granted to the Mark Holder;

9.4.6 Any other significant detail(s) considered as relevant.

9.5 The cyber security professionals are required to submit an undertaking to their respective PrCBs for abiding by the Rules for Use of Scheme Mark.

9.6 The conformity assessment body shall also forward the copy to QCI of the draft certification document along with the details of the certified cyber security professionals, to whom it intends to issue to the Mark Holder, post the issuance of the certificate(s) to the successful candidates.

- 9.7 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.
- 9.8 The annual fee for use of Scheme Mark from the Mark Holder is to be submitted to QCI through the PrCB.
- 9.9 The conformity assessment body shall also make provision for informing QCI, about any changes in the certification status like suspension, withdrawal, etc.
- 9.10 The contract between QCI and the Mark Holder shall be valid as long as the later holds a valid certification under the Scheme or is advised otherwise.

10. Design of the Mark






- 10.1 Attestation of cyber security professionals:
 - 10.1.1 The Scheme Mark is only allowed to be used by the PrCBs while issuing the statement of conformance in regards with a specific competency profile issued to an individual cyber security professional.
 - 10.1.2 While creating professional profile for career growth, the certified professional may use the statement 'Certified competent in 'Capability Area' 'Expertise Level' under the Certification Scheme for Information Technology (IT) and Industrial Control System (ICS) cyber security professionals' without reproducing the logo.



■ C-100, M-0, Y-0, K-0	■ C-100, M-0, Y-0, K-0	■ C-34, M-18, Y-21, K-0
■ C-2, M-2, Y-29, K-0	■ C-100, M-100, Y-25, K-25	■ C-24, M-9, Y-9, K-0

- 10.1.3 While the PrCB will issue the above mentioned mark to certified cyber security professionals, the Scheme Manager shall issue the Scheme Mark mentioned below attesting its approval as a conformity assessment body under Conformity Assessment Framework for Cyber security of Critical Sector Entities. The approved PrCB shall get into an agreement with the Scheme Manager which will be similar to the Section 7: Rules for Use of Scheme Mark of the Certification Scheme for Cyber Security Management System (CSMS).



 C-100, M-0, Y-0, K-0	 C-100, M-0, Y-0, K-0	 C-35, M-12, Y-0, K-0
 C-2, M-2, Y-29, K-0	 C-24, M-9, Y-9, K-0	



Annexure A

Format for Application APPLICATION FOR PERMISSION TO USE THE SCHEME MARK

1	Name of the Cyber Security Professional	
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

SELF DECLARATION: (Cyber Security Professional to submit to PrCB/SO)

Certification Scheme for IT / ICS Cyber Security Professionals

1. I, _____, confirm that I will follow the rules and procedures prescribed by the Certification Scheme for Cyber Security Professionals. I understand that if I am found blatantly violating the rules and procedures at a later date, my certification can be suspended and withdrawn.
2. I confirm that I will follow the Code of Ethics pertaining to cyber security certified professional.
3. I have read and understood the Rules for Use of Scheme Mark and shall abide by it all the time. I will not misuse the same and avoid bringing any disrepute to either NCIIPC, QCI or to the Personnel Certification Body.
4. I view my knowledge, services and professional associations as being for the benefit of the people I serve and vow not to use them to secure unfair personal advantage.
5. Fees and financial arrangements, as with all contractual matters, are always discussed without hesitation or equivocation at the onset and are established in a straight forward professional manner.
6. I at times render service to individuals or groups in need without regard to financial remuneration.
7. I neither receive nor pay a commission for the referral of a private aspirant.
8. I conduct our fiscal affairs with due regard to recognized business and accounting procedures.
9. I am careful to represent facts truthfully to aspirants, referral sources and third-party payers regarding credentials and services rendered. I will correct any misrepresentation of our professional qualifications.
10. I will not malign colleagues or other professionals and will always abide by the confidentiality, integrity and data/information protection.
11. I will maintain highest level of integrity (Ethics) and reasoning ability using problem-solving approach as an Intelligence quotient.
12. All records kept on an aspirant are stored or disposed of in a manner that assures security and confidentiality.



13. I will treat all communications from aspirants with professional condence.
14. I will not disclose clients' confidences to anyone, except: as mandated by law.
15. I will not misrepresent our professional qualifications, affiliations and functions or falsely imply sponsorship or certification by any organization.
16. Advertisements, announcements, brochures, etc. promoting our services describe them with accuracy and dignity. These promotional materials are devoid of exaggerated claims.
17. I will not make public statements, advertisements, etc. which contain any of the following:
 1. A false, fraudulent, misleading, deceptive or unfair statement.
 2. A false representation of a fact, or a statement that may mislead or deceive because it is removed from its original context or makes only a partial disclosure of relevant facts.
 3. A statement implying unusual, unique or one-of-a-kind abilities, including misrepresentation through sensationalism, exaggeration or superficiality.
 4. A statement concerning the comparable desirability of services offered by ourselves and others.

I confirm that I have read and understood the document forming part of this declaration and will be abiding the same by letter and spirit.

Signature of the candidate

Application number

Date