Conformity Assessment Framework (CAF) for Cyber Security of Critical Sector Entities (CSEs) - Frequently Asked Questions (FAQs)

Section I| Overview & Applicability

Q1: What is the QCI–NCIIPC Conformity Assessment Framework (*CAF), and why is it developed?*

The CAF for Cyber Security of Critical Sector Entities is designed and developed jointly by the National Critical Information Infrastructure Protection Centre (NCIIPC) and the Quality Council of India (QCI) to create a comprehensive national framework and mechanism to secure the critical information infrastructure (CII) of CSEs from cyber threats. The CAF will help establish a robust ecosystem for CSEs, NCIIPC, regulators and other bodies to holistically address the cybersecurity aspects connected with people, processes, technology and governance within and across the CSEs.

Q2: Which sectors or organisations does the CAF apply to?

The CAF is primarily targeted for entities in India's critical sectors, viz, Power & Energy, Transport, Government, BFSI, Telecom, Strategic & Public Enterprises, and Healthcare. Organisations having critical information CII would significantly benefit from adopting the CAF voluntarily. Appropriate authorities, in future, may also mandate CSEs of specified critical sectors to conform to the CAF.

The CAF is however not meant for CSEs only but can also be adopted by other organisations to enhance their cyber resilience.

Q3: How does the QCI-NCIIPC CAF compare with other country-specific frameworks (e.g., US NIST, UK NCSC, Singapore's CSA)?

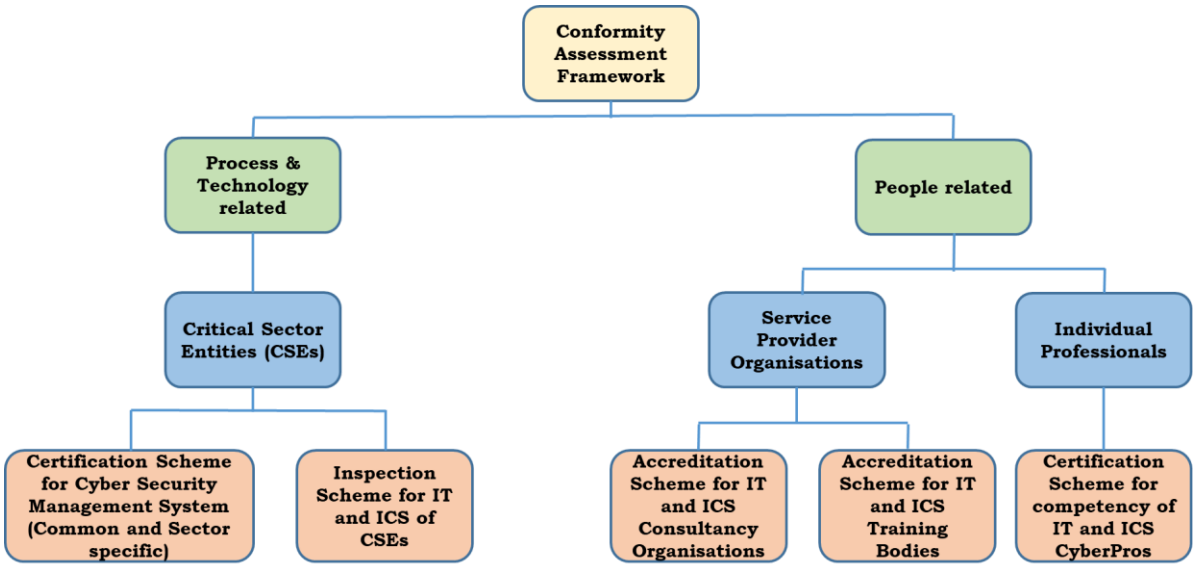
The QCI-NCIIPC CAF consolidates the best practices from multiple global standards (ISO 27000 series, IEC 62443, NIST, CIS, etc) and the Indian laws, regulations and guidelines (IT Act 2000, guidelines from NCIIPC, CEA, etc). The QCI-NCIIPC CAF is developed through multi-stakeholder consultation and is tailored to specifically address the Indian CII environment, ICS/ OT complexities, and national security priorities. It is aligned with the national legal and regulatory mandates and the National Cybersecurity Reference Framework (NCRF), just like other country-specific frameworks, which incorporate their local laws, regulation and industrial nuances.

Q4: What roles do NCIIPC and QCI each play in the CAF?

Broadly, NCIIPC is the Scheme Owner, providing overarching direction and alignment of the CAF to the cybersecurity requirements of critical sectors and CSEs. QCI, India's National Accreditation Body, is the Scheme Manager responsible for accrediting Conformity Assessment Bodies (CABs), handling day-to-day operations and ensuring compliance with the scheme's standards.

Q5: Can you briefly describe the overall structure, objectives and expected outcomes of the QCI-NCIIPC CAF?

A structural view of the CAF for cybersecurity of CSEs is given below:



The objectives of the Scheme are described below:

- **Certification Scheme for Cyber Security Management System (CSMS)**: Establish a uniform approach for the certification of CSMS of CSEs at three levels. Define the key cybersecurity controls and processes of the CSMS and describe the methods by which conformance to the CSMS shall be demonstrated and evaluated for certification.
- **Inspection Scheme for IT and Industrial Control Systems**: Establish a uniform approach for periodic inspection of IT and ICS of CSEs. Define the key cybersecurity controls and processes for cyber resilient systems and describe the activities and outcomes of inspection.
- **Personnel Certification Scheme for IT and ICS Cyber Security Professionals**: Provide a framework for objectively attesting and certifying IT and ICS Cyber Security Professionals for their expertise and competence in different cybersecurity domains that are relevant the critical sector entities and various other organisations.
- **Accreditation Scheme for IT and ICS Training Bodies**: Provide a framework to accredit Training Bodies (TBs) that have sufficient infrastructure and competent human resources to train individual professionals and/or CSEs in different cybersecurity domains.
- **Accreditation Scheme for IT and ICS Consultancy Organisations**: Provide a framework to accredit Consultancy Organisations (COs) that are technically competent and have necessary knowledge, skills, expertise and processes in place for different work heads required by the CSEs and other organisations. The work heads defined under the scheme cover the entire gamut of cybersecurity work required by CSEs.

The Quality Council of India, through National Accreditation Board for Certification Bodies (NABCB) and National Accreditation Board for Education and Training (NABET) will accredit the undermentioned bodies, who will further carry out the certification of CSEs and individuals:

- **Certification Bodies (CBs)** having sufficient infrastructure and competent human resources to audit and certify the CSMS of CSEs.

- **Inspection Bodies (IBs)** having sufficient infrastructure and competent human resources to inspect the CII and other IT/ ICS of CSEs.
- **Certification Bodies for Persons (PrCBs)** having sufficient infrastructure and competent human resources to test, attest and certify the competence of individual IT and ICS cybersecurity professionals in different cybersecurity domains.
- **Training Bodies** with expertise and competence in different cybersecurity domains, to train and develop IT and ICS knowledge, skills and expertise.
- **Consultancy Organisations** with expertise and competence in different work heads, to deliver the required work to CSEs and other organisations.

Q6: How does a CSE or any other organisation adopt the QCI-NCIIPC CAF?

The Scheme documents provide all the required information for organisations wanting to adopt the QCI-NCIIPC CAF. Organisations are also advised to peruse the standards and guidelines listed in Annexure 1 for additional guidance. Answers to specific queries related to the Scheme may also be sought from QCI, who would give it in the form of FAQs and other publicly available documents.

Section II| Certification Scheme for Cyber Security Management System (CSMS)

Q1: What are BTC, STC, and ATC — why three levels?

The Technical Criteria has been developed with three tiers of conformance:

- **Basic Technical Criteria (Level 1)**, referred to as BTC (Level 1) is a horizontal criteria that covers the common cyber security requirements for all critical sector entities and other organisations. This level is foundational in nature and common across all Critical Sector Entities (CSEs).
- **Supplementary Technical Criteria (Level 2)**, referred to as STC (Level 2) is a semi horizontal criteria that covers the cyber security requirements relevant and appropriate to critical sector entities of the Power sector.
- **Additional Technical Criteria (Level 3)**, referred to as ATC (Level 3) is a vertical criteria that addresses the cyber security requirements for specific classes of industrial control systems of critical sector entities of the Power sector.

The three tiers of conformance enables Power Sector CSEs to implement a cybersecurity management system that covers their generic IT, OT/ICS and CII.

Q2: How does the BTC, STC and ATC compare with ISO 27001 and IEC 62443 certifications?

BTC (Level 1) is based on ISO 27001:2022 with some additional requirements. Annexure A of the Scheme document provides a mapping Between BTC (Level 1) and other referenced standards/ guidelines.

STC (Level 2) is based on IS/ISO/IEC 27019:2017 and enhances Level 1 by incorporating Power sector specific requirements from IS/ISO/IEC 27019:2017 and IEC 62443 series of standards that are relevant for CSEs of the Power Sector.

ATC (Level 3) is conceptually akin to IEC 62443 Part 3 and has requirements that are relevant and appropriate for conformity assessment of critical industrial control systems of CSEs of the Power Sector. The requirements are derived from a combination of functional requirements and risk assessments and align with the IEC 62443 series of standards and NIST SP 800-82r3 which specifically address the security of control systems.

Q3: The STC and ATC are specific to Power Sector. What about STC and ATC for other sectors?

The Power sector was chosen for STC and ATC because of the thrust given by the Ministry of Power, CEA and NCIIPC for enhancing cybersecurity in Power sector entities. A lot of work was already being done with regard to IS/ISO/IEC 27019:2017 and IEC 62443 series of standards, and the same could be leveraged for the STC and ATC through the Power Sector representatives and other technical experts in the Technical Committee (TC).

STC (Level 2) and ATC (Level 3) for other sectors can be similarly developed if the need for the same is identified by the regulators/ national bodies. The Technical Committee would be specifically constituted to have appropriate sectoral representatives and technical experts to provide oversight on the scheme development.

Q4: Do I need to implement all three levels (BTC, STC, ATC)?

Broadly, all CSEs would need to implement BTC (Level 1), to be in conformance with the requirements of ISMS that is mandated by IT (NCIIPC) Rules, 2018. Appropriate authorities will provide necessary direction on the implementation of STC and ATC.

The implementation is cumulative — an organization must first implement BTC, then add STC and ATC if relevant.

Section III| Inspection Scheme

Q1: What is the relation between CAF Certification and Inspection?

Broadly, CAF certification checks a CSE's ISMS, whose processes are defined through the cybersecurity management system. On the other hand, inspection technically examines the cybersecurity of a CSE's IT/ ICS infrastructure and systems.

While CSMS certification and Inspection are independent of one another, the CSMS and inspection criteria have a strong correlation, with each inspection control supporting a control defined in CSMS. Requirements mandated in the Inspection Scheme complement the requirements specified in BTC (Level 1), STC (Level 2) and ATC (Level 3).

Q2: Can you describe the objectives of the CAF Inspection Scheme for better understanding?

System vulnerabilities and unused services increase the attack surface of a system, creating potential entry points for attackers. An assurance that critical systems of CSEs are hardened and fortified against cyber-attacks can be achieved through their inspection by technical experts using their professional judgment and objectivity.

The Inspection Scheme is designed to provide assurance of hardened and cyber-secure IT/ ICS systems through mechanisms such as technical examination of their design/ architecture/

threat modelling documents, physical examination of the deployed and running systems, assessment and testing of the in-use asset inventory (hardware, software, firmware, OS, etc.) to determine their conformity with specified security benchmarks, vulnerability scanning and penetration testing of defence-in-depth implementation.

Inspection or examination of a system is done to validate the technical implementation of 'safeguards' and controls that establish a baseline for cybersecurity protection and hardened cyber defences. Inspection activities validate that the configurations of software and hardware adhere to industry-recommended benchmarks and the cybersecurity safeguards prescribed in the Inspection Criteria are effectively implemented in the operational systems.

Q3: How does an IB carry out inspection?

The IBs use Inspection Criteria of the Inspection Scheme as reference for carrying out inspection. These criteria are based on 18 controls from CIS v8.0 for IT infrastructure and 20 controls from CIS v7.0 for ICS infrastructure. These controls are to be validated by the inspection team using vulnerability scanning, penetration testing tools, scenario creations and other techniques focusing on infrastructure with less emphasis on process auditing. Some of these activities may be required to be jointly undertaken by the CISO and inspection team.

Q4: Why are CIS cybersecurity controls chosen for Inspection Criteria?

The rationale for selecting CIS cybersecurity controls for Inspection Criteria is that the CIS controls are more prescriptive and pragmatic and have a wider industry acceptance. They offer a prioritised set of actions that collectively form a defence-in-depth set of best practices to help mitigate the most common attacks on IT and ICS systems and networks. Further, these controls share insight into attacks and attackers, identify root causes, and translate that into classes of defensive actions.

Q5: When should a CSE typically go for an inspection?

Inspection of cybersecurity of operational critical systems should typically be done when the 'system of interest' is commissioned, periodically and whenever there are significant changes in the system architecture or implementation. Inspection may be carried out by in-house or external teams or by inspectors from independent Inspection Bodies (IBs). IBs provide a quantitative feel of the degree of the system hardened. This lead to better confidence on the achievement of the goal of secure system.

Q6: Does the Inspection Scheme recognise the constraints of OT/ ICS?

ICS systems rely heavily on a combination of open and proprietary technologies provided by OEM products, systems, and services. Asset owners generally have an agreement with OEMs/ SP/ SI for after-sales support across the operation phase. These include configuration setting, system hardening, providing patches, port setting and penetration testing as they demand extensive domain knowledge, and technical insights and may impact ICS operations. These agreements often impose restrictions on ICS asset owners for what adjustments they can make to ICS without voiding the warranty. Therefore, these agreements must be considered when determining how to implement safeguards to harden ICS systems and solutions.

Q7: Is inspection mandatory, and how often must it be done?

Yes, inspection is mandatory under the Scheme. Regular inspection of CII of CSEs is strongly recommended. The frequency may vary based on risk level, sector regulations, or severity of findings in previous inspections (e.g., annually or every two years).

Q8: Who conducts these inspections?

Accredited Inspection Bodies (IBs) under QCI.

CSEs may also carry out internal inspections through their own teams or third-parties, who have ICS/ OT domain expertise and technical competence.

Section IV| Consultancy, Training, and Personnel Certification

Q1: We already use external consultants. Why do we need accredited Consultancy Organisations (COs)?

Accredited COs are vetted by QCI for technical competence, impartiality, and alignment with the CAF / synchronisation with national cyber security requirements as prescribed by NCIIPC, CERT-In and NSCS. This ensures you get consultants with recognized ICS/OT expertise, not just generic cybersecurity. It reduces the risk of substandard advice or conflicts of interest.

Q2: Why does the CAF accredit Training Bodies (TBs)?

Training is crucial in bridging the knowledge and skill gap, especially for ICS/ OT. Accredited TBs provide curricula aligned to a CSE's cybersecurity domains and competency profiles. It also supports preparing for Personnel Certification, if desired.

Q3: What are the benefits of the Personnel Certification Scheme?

Please refer to annexures C, D and E of Section 3 of the scheme document, wherein the applicability of the Scheme for individuals and organisations are described.

Section V| Implementation & Operations

Q1: How do we get started with the CAF if we have limited security maturity?

Begin with a BTC (Level 1) gap analysis—this sets a baseline. If you're in the power sector or similarly regulated, incorporate the STC. If you have advanced ICS systems with special demands, consider ATC. Engage an accredited consultant (CO) or your internal team to design an implementation roadmap.

Q2: How do we find accredited CBs, IBs, COs, or TBs?

QCI maintains official directories of accredited bodies on its website or through published listings. Always verify the accreditation scope matches your sector (power vs. BFSI, etc.) and the needed ICS domain.

Q3: What if my organization is already certified to international frameworks (like ISO 27001 or IEC 62443) or follows NIST CSF?

It is recommended that CSEs should develop a roadmap for adoption of QCI-NCIIPC CAF, since it incorporates India-specific elements. QCI accredited CBs provide sufficient considerations to already accredited / certified entities by if they are a part of IAF/MLA ecosystem which may lead to reduction in audit intensity.

Annexure A

Standards and Guidelines

For CSEs and other Organisations

Note: Indian Standards (IS) are available at reasonable prices on Bureau of Indian Standards (BIS) website):

- IS/ISO/IEC 27001:2022 (mandatory for CSEs)
- IS/ISO/IEC 27002:2022 (mandatory for CSEs)
- IS/ISO/IEC 27000 (recommended)
- IS/ISO/IEC 27003 (recommended)
- IS/ISO/IEC 27004 (recommended)
- IS/ISO/IEC 27005 (recommended)
- IS/ISO/IEC 27007 (recommended)
- IS/ISO/IEC TS 27008:2019 (recommended)
- IS/ISO/IEC 27017:2015, Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services (recommended)
- NIST SP 800-82r3, Guide to Operational Technology (OT) Security (mandatory for CSEs of Power Sector)
- IS/ISO/IEC 31000:2018 (recommended)
- ISO/IEC TR 27016 (recommended)
- IS/ISO/IEC 27035-2:2023, Information technology - Security techniques Information security incident management (recommended)
- Sector-specific standards: ISO/IEC 27011 for telecommunications organizations, ISO/IEC 27019 for power & energy, ISO 27799 for health (optional)
- NIST Cybersecurity framework equivalent in ISO/IEC TS 27110:2021 (optional)
- Maturity models ISO/IEC 33000 (optional)
- IEC/ISA 62443-2-1, Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program (recommended for CSEs of Power sector)
- IEC 62443-3-3, Industrial communication networks – Network and system security – Part 3-3: System security requirements and security assurance levels (recommended for CSEs of Power sector)

- IEC 62443-3-2, Industrial communication networks – Network and system security – Part 3-2: Target security assurance levels for zones and conduits (recommended for CSEs of Power sector)
- IEC/ISA 62443-1-1, Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models (recommended for CSEs of Power sector)
- IEC/TR 62443-2-3, Industrial communication networks – Network and system security – Part 2-3: Patch management in the IACS environment (recommended for CSEs of Power sector)
- IEC/TR 62443-3-1, Industrial communication networks – Network and system security – Part 3-1: Security technologies for industrial automation and control systems (recommended for CSEs of Power sector)

For CBs and CSMS auditors:

- ISO/IEC 17000, Conformity assessment — Vocabulary and general principles
- ISO/IEC 17020:2012, Conformity assessment — Requirements for the operation of various types of bodies performing inspection
- ISO/IEC 17021-1:2015, Conformity assessment — Requirements for bodies providing audit and certification of management systems
- IS/ISO/IEC 27006-1:2024, Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 17025:2017, General requirements for the competence of testing and calibration laboratories
- ISO 17065:2012, Conformity assessment — Requirements for bodies certifying products, processes and services
- IS/ISO/IEC 19011:2018, Guidance on the management of audit programmes (mandatory for auditors)
- IS/ISO/IEC 27007:2020, Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing (mandatory for auditors)
- IS/ISO/IEC TS 27008:2019, Information technology — Security techniques — Guidelines for the assessment of information security controls (mandatory for auditors)
- IS/ISO/IEC 27017:2015, Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services (mandatory for auditors)

For IBs and inspectors:

- Center for Internet Security (CIS) - Controls and Benchmarks (v8.0) for IT infrastructure, released in May 2021.

- Center for Internet Security (CIS) - Controls and Benchmarks (v7.0) for ICS infrastructure. Informative References
- NIST 800-115 - Technical Guide to Information Security Testing and Assessment
- NIST 800-171 - Guidelines for Protecting Sensitive Information
- NIST 800-167 - Guide to Application Whitelisting
- NIST 800-41 - Guidelines on Firewalls and Firewall Policy
- NIST 800-53 - Security and Privacy Controls for Information Systems and Organizations
- NIST 800-128 - Guide for Security-Focused Configuration Management of Information Systems
- NIST 800-123 - Guide to General Server Security
- NIST 800-124 - Guidelines for Managing the Security of Mobile Devices in the Enterprise